Global Information Assurance Certification Paper

A Fundamental and Essential look into Managed Security Services

By: Kevin Warda

SANS (GSEC) Practical Assignment Version 1.4c – Option 1
March 28, 2005

This paper will cover the ideology and benefits of Managed Security Services. It will discuss the motivation and framework, as well as the services of most Managed Security Providers (**MSSPs**). It will also take a look into the new services of today. Overall, the paper will highlight the crucial demand for companies to utilize managed security services now, and well into the future.

What is MSS?

You see the acronym; you hear the buzz. But what exactly *is* **MSS** and what can it do for you? MSS stands for Managed Security Services. It is a way of outsourcing your critical network security functions to a dedicated highly trained staff, devoted to monitoring and managing your infrastructure 24 hours a day, 7 days a week, 365 days a year.

Most companies now a days, big and small, use a layered security approach to their corporations infrastructure. “Layered Security” is a way of placing multiple barriers between the perimeter and the core of a company’s infrastructure. It is analogous to a mid-evil castle or fortress. In those days there were many hurdles and obstacles between the enforcing army and the core of a country’s castle or fortress…the King himself. In most cases an opposing army would first have to climb a very steep hill in difficult terrain to even attempt breaching the gates of the castle. Once the army reaches the castle, they would have to cross a moat that surrounded the perimeter. If the army made it across the moat they still would have to break down the gates to get inside. Once inside, the King’s defenders who are standing on guard would notice the breach and attack the opposing army. Even still there might be many corridors, walls, locks, and protection between the courtyard and where the King is actually being held.

In today’s world of Information technology the model of layered security holds true. An opposing army (hacker) tries to obtain trade secrets (the King) of a very reputable company. The scenario is the same, although the means are different. In this case the layers of security are a non-visible, natted, perimeter firewall (castle on a very steep hill), a restrictive and secure firewall policy (a surrounding moat and castle gates), an intrusion detection system (castle guards), and internal firewalls, or routers with separate network segments

(secure path to the King's holding place).

As described above, layered security is a necessity in securing anything that is of great importance. Whether it be top-secret government documents, or the secret formula to Coke ®, there must be barriers and practices put in to place to protect this vital information. Protecting these assets can be a very daunting task. Most companies do not have the money, equipment, resources, or expertise to effectively and efficiently protect what is most dear to their corporation.

Enter MSS, Managed Security Services. As defined above, this is a dedicated staff that is skilled and trained to do one thing - Protect your King!

What sources are saying about MSS?

"The market for Managed Security Services is rapidly growing. According to the Gartner Group, Managed Security Services (MSS) are expected to grow at a 20% compound annual growth rate, reaching over $1.5 billion in 2006. This remarkable rate of growth makes MSS "the" fastest growing segment of security services. "Gartner believes that the majority of enterprises that outsource the monitoring and management of perimeter security will increase their security level at equal or reduced cost to internal efforts. Enterprises should focus internal security resources on internal security issues and architectures, and outsource
repetitive, external-facing tasks to managed security service providers." - John Pescatore and Kelly Kavanagh, Gartner North American MSSP Magic Quadrant 2H02"

Since no one can fully eliminate accidental or intentional incidents, many MSSPs institute an avoidance program. Parameters and practices are put in place so that the MSSP's endeavor is to mitigate risk to the fullest extent possible. A good MSSP should protect the availability, integrity and confidentiality of business assets that are critical in today's internetworked economy. It should include a robust information protection program that addresses avoidance, assurance, detection and recovery, to ensure information, computing and telecommunications assets are not compromised. Therefore a company needs an offering that facilitates the complete lifecycle incident management service, combining prevention and assurance with rapid detection and response.

Author and information security expert, Peter Stephenson, developed the Intrusion Management Model below:

Definition:
Limiting the possibility of a successful intrusion through effective preventative, quality management and detective processes, and facilitating successful investigation of an intrusion should one occur.

Four Layers:

1. *Avoidance*
2. *Assurance*
3. *Detection*
4. *Recovery*

The Intrusion Management Process:

- AVOIDANCE: Using policies, procedures and tools such as firewalls, and access control to avoid threats against information assets.
- ASSURANCE: Vulnerability testing and system audits ensure compliance with policies.
- DETECTION: Real-time logging and interception of intrusion or abuse attempts.
- RECOVERY: Restoring the affected system or device to its pre-compromise condition with as little loss of information assets as practical.
- INVESTIGATION: Tracing intrusions and abuses in a manner that facilitates appropriate responses.

CIA – The Three Bedrock Principles of Security

Confidentiality:
Confidentiality is the principle of keeping your private information and documentation just that - private.
It is very important with banking institutions or E-commerce sites. With this type of organization, there is a very large amount of credit card numbers and other personal information that needs to be protected and kept confidential. Think of the repercussions of a drug being made public prior to its official release date - All of the time and money of research and development would go down the drain. The possibility of an individual's health records becoming public domain can also have very serious ramifications if they were compromised in any way. All of this type of information needs to be protected from prying eyes, whether the prohibited view ability is out of curiosity or malicious intent. For most people and companies alike, there is very high regard to ones privacy. An MSSP that shares in this philosophy and has practices in place to keep it that way are invaluable to corporations where this is a priority.

Integrity:
Integrity is the principle of having all of your private information, documents, data, and the like, remain authentic, accurate and unaltered. A well-known integrity attack that happens all too frequently is known as a "web defacement". This takes place when the homepage, or front door of a corporation's website is compromised and is changed to display a message that is usually derogatory towards the victim's corporation, or is simply used as a banner for a political statement. In either case, the Integrity of the company's website has been compromised. Thus, the face of the company has changed. This is a very bad reflection on the company who has been victimized, and its security posture. The embarrassment and repercussions of such an act can cause a lack of trust in that company by its vendors and shareholders. Thus the ramifications to such an event can be catastrophic to the corporation's bottom line.

Availability:
Availability is the principle of having all of your public and private information that you deem accessible, *stays* accessible at all times.
A common type of attack that compromises availability is known as a "DoS attack", or Denial of Service attack. The attack does what the name suggests, and denies service to the trusted entity that is trying to access the information that is allowed to them. There are many examples of Denial of Service attacks. If the website of an e-commerce site is down due to a DoS attack, it disables users from shopping at that store, and debilitates the business of that vendor.

On February 7, 2000, at 10:20 AM PST, the well-known Search Portal "Yahoo.com" became frantic when they found that their systems were being flooded by false requests from hundreds of hosts around the Internet. What became clear over the following hours was that the site had been a victim of a Distributed DoS attack. Yahoo's US-based services were almost entirely inaccessible until services were restored about 3 hours later. By one report, 41% of their international services were unavailable too, making this the biggest DoS attack anyone had seen to date. Over the next few days, additional attacks were launched against other major Web sites, among them included: MSN, Amazon.com, eBay.com, Buy.com ZDNet.com, E-Trade.com, and CNN.com. According to the Yankee Group, estimated costs of the attack totaled $1.2 billion cumulative and the attack on Amazon alone cost between $200,000 and $300,000 per hour. Losses of customer goodwill, corporate reputation and public trust may have been even greater.

What are the benefits of MSS?

Personnel:
Analysts not only need to be very skilled technically, but they also need to be highly trained in the areas of customer service. This staff is responsible for

monitoring, managing, and maintaining hundreds, and sometimes thousands of devices 24 hours a day 7 days a week 365 days a year. They are most likely certified in multiple areas of security as well, which enables them to be proficient in many disciplines of security, as well as knowledgeable with many different types of devices. These devices also range from Vendor to Vendor, so security analysts need to be multi-lingual in terms of flavors of Operating Systems, environments, and syntax. A lot is expected out of today's skilled security analyst. Attracting and retaining this critical staff is a huge challenge. Therefore it is best to let the job of acquiring such individuals rest on MSSPs and not your organization.

Time:

We've heard it before; "Time is money" - and for most companies today, it is a precious commodity. Most staff at organizations work a typical 9 to 5 work day, 5 days a week. So out of 168 hours a week, 40 of them are used to manage your network and its security functions. So who's watching your network the other 128 hours? No one is right? The problem with that scenario is that "Hackers" don't sleep! They know that the most opportune time to attempt an attack on your infrastructure is during those 128 hours - the time that most likely … no one is watching. This also applies to holidays. They know that while most people are mowing down on turkey, they can be hard at work scanning your network, looking for vulnerabilities. It is simply impossible for the typical organization to have the resources and finances to be able to be present 24 hours a day 7 days a week 365 days a year. MSSPs are designed to be able to offer this type of coverage. They also have the skilled staff that is very efficient in the practices of managing and monitoring, which require the expertise to parse through large amounts of logs and quickly identify false alarms. Therefore this enables them to deliver prompt and reliable service to provide attractive Service Level Agreements (SLAs) to prospective customers.

Facilities:

Another big appeal to utilizing Managed Security Services are the facilities offered by MSSPs. Most providers offer state-of-the-art, secure, certified Security Operations Centers (SOCs) in multiple locations. They typically offer best-in-class hardware and software solutions that are designed to keep customers' networks secure. Most organizations merely do not have the room, or the money, to provide such a luxury.

Compliance:

Compliance with the many security related laws and regulations today can be a daunting task for any business. Most MSSPs can offer extensive knowledge in the area of legal requirements and industry standards. It is their job to do the research, and to have the know-how when it comes to security related requirements that are specific to one's organization. They also need to have the

knowledge and expertise to keep managed devices hardened and patched. This includes upgrading devices to current industry standards, to keep them from possible malicious activity, and to further reduce the risk of new threats to their infrastructure. Some MSSPs provide expert analysis and correlation of global security threats from around the world. And even still, some also provide audit services to ensure customers remain in compliance on an ongoing basis.

Cost:

The cost reduction that companies can take advantage of by outsourcing their security functions can be dramatic. This is one of the biggest benefits that a company can experience when outsourcing their security related needs. One of the main reasons why this is true, is because it basically covers every area of concern when considering a Managed Security approach:

- It costs money to hire, train, and maintain a skilled security staff
- It costs money to build, deploy and maintain a state-of-the art Security Operations Center with the hardware and advanced technology it requires.
- It costs money to have personnel "on-the-clock" 24 hours a day 7 days a week 365 days a year including holidays.
- It costs money to keep up with the latest and greatest security related laws and regulations, threats and vulnerabilities and provide on-going patch
- management.

Another huge cost savings that has not been mentioned is known as "Risk Transfer". The financial losses that can take place from a security breakdown caused by an inexperienced in-house staff member can be catastrophic. So rather than assuming all of the risk/liability themselves, many companies are sharing the responsibility with Managed Security Services Providers, and reaping a number of business advantages in return. To some companies, this alone is the price of admission for choosing to use outsourced Managed Security Services.

What types of Services does Managed Security offer?

Managed Firewall:

In today's world, it is practically a necessity for a company to have a form of perimeter defense in their network infrastructure. Imagine a castle without fortified walls, or a safe at a bank without a metal door and lock. In the physical world it seems obvious to have doors and locks in place to facilitate a secure perimeter around areas that we deem prohibitive without explicit permission to

access. Well, in the world of Information, the same concepts hold true. A good firewall product with a hardened, restrictive and secure policy in place will considerably cut down on your company's exposure and vulnerability to attacks. It is considered the first line of defense for corporate networks, and acts as the gatekeeper to your critical information assets. These devices control the flow of information to and from your corporate network, and because of this, it must hold many rules that allow or disallow access to anyone and everyone that is behind this perimeter. This can be a very tedious and time-consuming task for a network admin to address. For example: sometimes an individual gets fired from the company, or someone new is hired in. The access requirements involved in both cases needs to be modified in all places where it applies. It most cases that access also includes the firewall policy. A new device and/or a new service to an existing device is deployed and this connectivity traverses through the firewall. Again firewall polices need to be tweaked. And with a very large corporation with many of these practices happening on a daily basis to an already huge firewall policy, the task can be overwhelming and almost impossible for a network administrator that already has a hundred other things on her plate. This is why deploying and maintaining these critical security devices requires specialized expertise, 24X7 monitoring and continuous management to ensure they protect your enterprise as your business needs change and security threats evolve in complexity. Unfortunately, most security organizations face serious resource constraints, both budgetary and time, making it impossible for them to acquire this specialization in-house.

Some of the firewall vendors that currently exist today include: Check Point, Cisco, Juniper, WatchGuard, ISS, and SonicWALL.

Managed Intrusion Detection:

An intrusion detection device is like a smoke detector, or a security camera. In most cases it cannot stop the intrusion, but alerts who is watching or listening that a breach of access has taken place. This layer of security is found everywhere, to banks, retail stores, and even your own home. As important as it is to have these devices in the physical world, it is just as important to have them in your corporate network. Now imagine if the smoke alarm was only turned on during the day, or the security cameras were only monitored during business hours. You would see quite clearly that the value of this layer of security would be dramatically decreased. That is why it is so important to have 24x7 monitoring of host-based, and network-based sensors. Unfortunately, proper intrusion detection management including policy tuning and keeping up-to-date signatures of the latest and greatest attacks, is a resource-intensive activity that most organizations cannot afford to do. And with the increasing complexity of today's business technologies, it is not an easy task to adequately monitor an organization's systems for interruptions or intruder penetrations. It is often difficult to determine if an anomaly is the result of a serious intrusion, or simply a coincidence, or what we would call a false positive. It takes a skilled

individual to determine what is a real attack versus what is normal network activity. And the vast amount of data that must be processed to identify these problems makes monitoring virtually impossible for an organization's internal staff.

Some of the intrusion detection vendors that currently exist today include: ISS, eEye Digital Security, Cisco, Computer Associates, and Snort.

Vulnerability Assessment:

Vulnerability Assessment takes a more proactive security approach. The vigilant organization constantly re-evaluates its security policies to ensure change has not weakened or nullified its ability to secure business-critical assets. Therefore it practices the performing of multiple and periodic scans on its corporate network. These scans can provide a wealth of valuable information about the level of exposure to threats. Vulnerability scans are an essential component in an effective information security program, although most companies do not have the staff with the expertise, experience and focus necessary to efficiently conduct vulnerability scans and interpret the results. That is why it is essential to have a dedicated team of experts to accurately assess the network vulnerabilities that affect a corporation, and to do so using state-of-the-art tools and techniques with minimum risk and disruption to the business and its daily functions.

Some of the vulnerability assessment vendors that currently exist today include: ISS, Network Associates, eEye Digital Security, and PredatorWatch.

Managed AntiVirus:

Viruses, Worms and Trojans can be a major problem for most companies today. The spreading of a virus, the self-replication of a worm, and the deception of a Trojan, can all lead to major losses to a corporation’s infrastructure. Without a form of antivirus on your network today, you are almost begging to have your systems compromised by a malicious application. Even with the most robust perimeter defenses, an unsuspecting trusted user can plug his laptop into your network, only to infect the network with the latest virus he picked up the night before while web surfing at home. Companies now a days need to have some sort of an antivirus solution integrated into their security functions. However, the task of managing antivirus software on all of your workstations throughout your entire company is nearly impossible. You would need a managed antivirus approach. From a technical standpoint, when it is said that your antivirus is "managed", it means that your workstations all obtain their configuration and virus definitions from a parent server. This antivirus server performs actions transparent to the end user, and usually does so on a regular predetermined schedule. Most managed antivirus solutions perform a daily scan of all workstations at 3:00AM. The administrator can change this time, but it is usually

most preferred by companies, due to the fact that their staff is at home sleeping. In this way the scans are less obtrusive on the end user. The antivirus parent server also has an update schedule where it receives its definitions from the vendor's servers. This enables the entire antivirus solution to be completely transparent, and as up-to-date as possible. From an administration standpoint, managed antivirus provided by an MSSP takes it one step further. They are able to integrate this service in conjunction with others that they already provide. Many firewall vendors today, such as Check Point, allow for seamless integration with antivirus products and their firewall products. This allows antivirus checking to be performed at the perimeter or on the DMZ, allowing the traffic to be scanned for viruses BEFORE it has a chance to enter your network and hit your mail server. The management of such solutions can all be addressed by MSSPs, allowing you to worry about your business, and not the latest virus to hit the Internet.

Current antivirus vendors include: Symantec, McAfee, Trend Micro, and Panda Software.

Managed Content Filtering:

In today's business society, more and more employees are connected to the outside world via the Internet. The importance of protecting your organization from the misuse of the Internet has never been more apparent than now. The repercussions of allowing employees to surf non-work related sites on the web, and download inappropriate material, can cause many problems in your organization. There are potential lawsuits, possible compromising of sensitive data, or the potential of a denial of service to your operations. The two latter can be caused by accidentally downloading a malicious app (virus) that are typically found at inappropriate websites. A company not only needs to have a strict security policy when it comes to employee Internet usage, but it also needs to be enforced as well. Having a content filtering solution in place within your organization protects you from the pitfalls that come with employees overstepping these boundaries. Most of these content-filtering applications provide a comprehensive library of URLs categorized by the type of content. They also have the ability to filter by a Keyword list as well. These applications usually are applied to dedicated hardware that sit within the perimeter or DMZ of your network's infrastructure. In the same way as antivirus, these applications also have seamless integration with your corporate firewall. Check Point FW1-VPN1 software for instance, has built in controls and settings for many best of breed content filtering applications. Again, this makes the management of this service an interchangeable capability for an MSSP. The MSSP can, and in most cases do, manage the hardware and the software of both content filtering and antivirus solutions.

Current content filtering vendors include: Surf Control, Websense, Aladdin Knowledge Systems, and Finjan Software.

What is the future of MSS?

The concept and practice of Managed Security Services is one that manages and mitigates Risk. Sometimes an intruder gets through the barriers of security that an MSSP manages and has in place to protect an organization. Any losses that the organization receives due to the attack are not the responsibility of the MSSP. The organization and the MSSP have an agreement, that its services will minimize the Risk, that is the sum of the Threats and the Vulnerabilities to their organization, as much as technically and humanly possible. No MSSP can fully guarantee protection……although there is one.

One company can be classified as being the Next Generation of Managed Security Services. That company is ISS (Internet Security Systems). They are providing a new standard of accountability, whereas they are actually *guaranteeing* protection against Internet threats. Currently, they are the only MSSP in the industry offering a guaranteed protection solution. How can they do this you ask? They provide a solution that goes beyond simple event monitoring and device management, by offering a money-back guaranteed performance-based Service Level Agreement (SLA). They are also providing the industry's only Managed Security Services protection warranty, providing customers with a $50,000 cash payment in the event of a security incident. This ensures 100% accountable, reliable protection.

With all of the successful attacks that a typical organization experiences on a day-to-day basis, how can an MSSP afford to provide such a service as a money back guarantee? The answer ISS has come up with is to address this concern, is **"Intrusion Prevention"**.

Intrusion Prevention takes a preemptive approach to security. It is the next level to Intrusion Detection and Firewall perimeter defense. The devices in an Intrusion Prevention system are able to detect and block malicious activity, using sophisticated network analysis techniques and attack signatures. They have the ability to take action against attacks, such as worm outbreaks or malicious insider activity, and help to reduce the impact of fast moving or difficult to detect threats. One device that has had recent success in this department is the Proventia® devices by ISS (Internet Security Systems). This suite of products offers a turnkey solution to layered security. It has the capabilities to offer firewall, intrusion detection, intrusion prevention, antivirus, and content filtering, all in one hardware appliance. In turn this device can not only detect attacks, but can stop them before any damage can occur to your infrastructure. It also has the capabilities of doing vulnerability assessments on the fly. It detects when a new device has entered the network and performs active and passive scanning that gives you a real-time picture of your security

risks.

Here is a quote from ISS regarding their Proventia® product line:

"UNIFIED, END-TO-END INTERNET SECURITY
Proventia leverages a single, powerful engine to drive a complete family of advanced security products. The Proventia product family includes advanced intrusion prevention, firewall, VPN, vulnerability assessment, antivirus, mail security and Web filtering. Plus, it provides end-to-end coverage for networks, servers, desktops, wireless points and remote points. All of the security applications in the Proventia product family can be easily managed from anywhere, via the SiteProtector™ centralized management system. Unified management and a common protection engine across Proventia products enable ISS to provide preemptive, ahead-of-the-threat protection quickly and easily."

Another step toward next-generation managed security solutions is a service that provides current daily threat information that is tailored to a particular organization and its business needs. MSSPs taking that service even another step further is having a team of experts in-house that provide the threat analysis. Again, ISS is that MSSP currently providing both aspects mentioned. They have a team of experts that gather up-to-the-minute information regarding the latest Internet threats from thousands of sources around the world called "X-Force". With that information they have created a service named "XFTAS (X-Force Threat Analysis Service)". The service provides current and forecast threat information, personalized and up-to-date expert analysis and correlation of global security threats, and daily vulnerability and alert notifications. Everything mentioned is provided via a web portal that is accessible via "two factor" authentication 24/7/365.

Some of the MSSPs that currently exist today include: Counterpane Internet Security, ISS (Internet Security Systems), NetSec, TruSecure, Ubizen, and LURHQ.

Conclusion:

In the ever changing world of Information Technology, the faster the changes take place, the greater the threats will become. Hence, Information Security has never been more important than it is today, and it will only become more important in the future. A company needs to consider security needs to their

network as a first priority. With that being said, the best option today for securing your infrastructure is through outsourcing. While outsourcing functions of a business (in general) is advantageous in many ways, outsourcing security functions has now become vital.

The benefits of Managed Security are a huge plus to any company today. But with the new services that MSSPs are offering and will start to offer well into the future, the managed security solution has gone way past being a luxury, and has now become a necessity.

Your King is important. The last thing you want, is to hear your hacker adversaries saying..."Check Mate!"

References:

- Stephenson, Peter. Investigating Computer-Related Crime. Boca Raton: CRC Press LLC, 2000

- SANS Institute. Track 1 - SANS Security Essentials. Volume 1.2 Defense In-Depth. SANS Press, January, 2004.

- SANS Institute. "The February 2000 DDoS Attacks". Track 1 - SANS Security Essentials. Volume 1.3 Internet Security Technologies. SANS Press, Jan, 2004: 58

- Stephen, Justin. The Changing Face of Distributed Denial of Service Mitigation. August 16, 2001. URL: http://www.sans.org/rr/whitepapers/threats/462.php (March 28, 2005)

- LURHQ. "Managed Security Services". ©1996-2003 LURHQ Corporation. URL: http://www.lurhq.com/managed_security_services.html (March 28, 2005)

- LURHQ. "Partners". ©1996-2003 LURHQ Corporation. URL: http://www.lurhq.com/partners.html (March 28, 2005)

- ISS (Internet Security Systems). "Managed Protection". Atlanta: ©2004

Internet Security Systems Inc. URL: http://www.iss.net/products_services/managed_services/managed_protection.php (March 28, 2005)

- ISS (Internet Security Systems). "X-Force Threat Analysis Service". Atlanta: ©2004 Internet Security Systems Inc. URL: http://xforce.iss.net/xftas/ (March 28, 2005)

- ISS (Internet Security Systems). "The Proventia® Product Family". Atlanta: ©2004 Internet Security Systems Inc. URL: http://documents.iss.net/literature/proventia/Proventia_Platform_Brochure.pdf (March 28, 2005)