The growth of the Internet and of e-businesses has increased the vulnerability of corporate systems to external attack. Sreedharan Sreekumar discusses an increasingly common approach to managing this problem.

Why does an Organization engage Managed Security Services?

Security needs of network-based systems have never been higher.

In a “2000 Computer Crime and Security Survey,” conducted by the Computer Security Institute in partnership with the Federal Bureau of Investigation, ninety percent of the survey respondents stated that they had detected computer security breaches in the past year. The advent of networked information-based businesses based on the Internet and their deployment of e-business applications has heightened the vulnerability of systems to security breaches. However, the demand for security has been outstripping the ability to provide it. The almost critical shortage of security-knowledgeable system and network administrators combined with the difficulty of staying on top of security issues can hinder the implementation of even basic security precautions. That is where Managed Security Services (MSS) can make sense although trusting computer security to outsiders might initially seem to many as being counter-intuitive.

Some organisations (referred to as “service users” in the remainder of this article) with established security programs prefer to outsource only the key aspects of their e-security infrastructure, firewalls and intrusion detection. This enables them to release technical resources for more complex or security-sensitive projects, such as web access control, security policy management, directory services or PKI. But there are other organisations that either lack the expertise to tackle the myriad security issues facing today’s enterprise or have difficulty recruiting security experts, let alone training and retaining them; they are therefore turning to global security providers to manage many key aspects of their e-security infrastructure.

The obvious benefits for service users is that Managed Security Services Providers (referred to as “security providers” in the rest of this article) have insight into security situations based on extensive experience across a range of organisations and business types. They are better positioned to recognize and respond to the symptoms of developing situations because in all likelihood they encounter them more often. For instance, if they observe an attack on one of their clients, they can move to protect all of their clients from the same attack before it spreads to others. So outsourcing security not only offers economies of scale but also economies of skill. Also, many security providers have special Security Operations Centers (SOC) with state-of-the-art infrastructure managed by trained personnel. Running part of a service user’s operation from such sites elevates its security to a higher plane. Further, by outsourcing, say, their intrusion detection services, the service user can implement best practices for IT security without having to support that expertise in-house. Other service users turn to security providers for a simpler reason: They cannot keep up with all their pressing security issues with in-

---

1 Public Key Infrastructure
house staff alone. They may be too large and too distributed geographically to assign in-house IT staff to everything related to security.

But what in the world is Managed Security Services?

The concept of “managed security” means different things to different people primarily because there is a wide variety of companies involved in this area. Security providers are an eclectic, no-one-size-fits-all group of companies that have a mixture of backgrounds. Many of them were spun off from security consulting or networking firms. Some are a result of partnership between either Internet Service Providers or Application Service Providers with security product OEMs2 to offer value added security services. Yet others have a service infrastructure provider background where they manage raw Internet bandwidth and prepare customer-targeted data for processing. Also several security software manufacturers have launched managed services arms to complement their product offerings. In addition to the variety of backgrounds of security providers, maintaining security entails several functions and hence security providers offer a wide range of services. Some of these services are:

**Firewall Management** The service provider monitors the availability and health of the firewall system on a 24x7 basis and responds, as agreed to, in case of failure. Recommendations on software updates to maintain the security posture will also be made by the service provider.

**Intrusion Detection** The service provider monitors network traffic around the clock to detect intrusions or network misuse. The service provider’s team of security experts works closely with the service user to define proper security responses and escalation procedures for all types of security events. The service may also include secure Web access to intrusion detection security events, logs, summary reports, and statistics to better manage the service user’s network and to back up critical data for disaster recovery efforts.

**Management of Virtual Private Networks (VPNs)** Monitoring, managing and support of VPNs3 by a service provider allows organizations to effectively obtain secure, cost-effective, and reliable communications over the Internet without the required investment in hardware, software, and training. The security provider’s site-to-gateway VPN and gateway-to-gateway capabilities allow for the authentication of remote users while providing instant access to corporate information over the Internet by establishing a VPN between their systems and the corporate firewall. In addition there could be the ability for administrators to receive secure Web access to VPN usage logs, summary reports, and statistics.

**Content Monitoring** Protects users and networks from Internet-based viruses and hackers by scanning and cleansing e-mail attachments, file transfers, and Web traffic as well as keyword-based filtering of inappropriate e-mail or Web pages.

**The Strategic Role of Auditing in Managed Security Services**

So what should the role of audit be in all of this? Selection of the service provider is extremely critical not only because it is such a daunting task but also because the first undertaking of the selected security provider is usually to conduct a vulnerability assessment of the service users’ network to help locate unprotected resources and focus security risks. This assessment will include a vulnerability scan, which attempts to uncover security risks before hackers do. The security provider may also conduct interviews with each department to identify specific needs, requirements and may also address expectations for a new security policy. The close scrutiny required by this process affords the security provider intimate knowledge of the client’s network infrastructure. In addition, the written agreement with the service provider and the management of that agreement are also equally important. Therefore when auditing a managed security service agreement, the following issues must be addressed by the auditor.

**1 Selection of Service Provider**

The auditor must examine whether the following aspects were looked into at the time of selection of the security provider.

1. Was the service provider asked about NOC staff qualifications and experience and whether the service provider hires employees who are certified to manage the solutions they sell? Do they conduct background checks on their own employees?
2. The auditor must examine whether the service user had obtained a client list and checked references: does the service provider have a successful history of dealing with similar organizations?
3. What security measures have been taken by the security provider to secure their applications, their backend systems? If an SOC goes down, is there a backup available?
4. The availability of auditing tools and techniques with the service provider is also important. Does the service provider keeps secure logs, proper audit trails and submits itself to internal audits on a regular, at least quarterly, basis and in addition conducts an independent architecture review by outside experts?
5. Audit must examine if the service provider is ready for incident response. Is there a set of clearly documented procedures that show that the service provider is ready to handle everything from a minor network glitch to a major denial of service attack? There should also be clearly defined notification mechanisms to let the service user know that something happened and how it was handled.

---

1 Original Equipment Manufacturers
2 Virtual Private Network is the extension of an enterprise’s private network across a public network like the Internet.
II Agreement with Service Provider

The Auditor should consider such things as:

1. Existence of a formal agreement between the service provider and the service user.
2. Inclusion of a clause, which states that the service provider is obligated to comply with acts and regulations pertaining to the functions it should undertake on behalf of the service user.
3. Existence of Service Level Agreement (SLA) with performance monitoring procedures. This usually is the single most element in any MSS contract. The SLA defines the role of the service provider and the service user. It should be ensured that SLAs contain adequate response time and escalation processes.
4. Inclusion in the contract of forensic services, to collect and preserve data and evidence of security problems after a network intrusion. This evidence is critical for criminal prosecution of hackers, and to design measures on how to prevent it or reduce the impact to an acceptable level the next time.
5. Adherence to the service user’s security policies.
6. Stipulation in the outsourcing agreement that activities performed by the service provider are subject to controls and audits as if they were performed by the service user itself.
7. The extent to which the agreement provides for the audit of the service provider, and whether this provision is adequate. This includes assessing the potential reliance on any IS audit work carried out by either the service provider’s internal auditors or an independent third party contracted by the service provider.

III Management of Agreement with Service Provider

The auditor should verify that:

1. The service user has the capacity and competence to follow up and review the services provided.
2. The service provider conducts tests to prove the installed solution is really enforcing the service users security policy. Ensure that the service provider repeats vulnerability assessment and reviews the security policy on a regular basis.
3. The recommendations of the service provider in the initial vulnerability assessment have been implemented. Too often do service users believe that their signature on the agreement with the service provider will guarantee their security.
4. Where SLAs are not being met, the service user has sought remedy and corrective actions have been considered to achieve the agreed service level.

About the Author

S. Sreekumar, CIA, CISSP, CISA, CFE, CQA
Sree began his audit career with the Indian Audit and Accounts Department where he worked for 14 years. Between 1993 and 1998 he was Director, EDP, in the office of the Comptroller and Auditor General of India. Sree is presently a senior auditor with the International Monetary Fund based in Washington D.C. He can be contacted at Ssreedharan@imf.org.

*Defined minimum performance measures at or above which the service delivered is considered acceptable.*