
Why Outsource to a Managed Security Service Provider (MSSP)?

Mike Johnson
CTO



Introduction

Computer security breaches are reported in the media everyday, littering newspapers, TV and other news outlets with reports of the consequences of poor IT Security. Unfortunately, identity thefts, computer break-ins, and web page defacements occur every hour of every day.

The role of protecting computer networks from hackers has never been more difficult. Threats range from unsophisticated hackers that know only how to execute a prepackaged program to more malicious hackers targeting companies for intellectual property, credit card data, or simply to cause downtime. Defending a network from such tactics takes planning, extensive expertise, and specialized tools. Often corporate IT departments are ill equipped to handle these evolving threats.

A Managed Security Services Provider (MSSP) handles only security issues and allows your IT staff to focus on tasks more in line with your core business. It is no wonder then that more and more companies are choosing to outsource their security management – either in whole or in part. The goal of this whitepaper is to help you understand exactly what a MSSP does, and the benefits companies can experience by working with an external security partner.

Market Demand

Too often, IT professionals hear statements from prospective clients such as “We’re secure, we have a firewall.” While the presence of a firewall is certainly a good thing, it does not necessarily create a secure network. A firewall is only a layer of security on one network entry point. And when ignored, a firewall can rapidly lose its effectiveness. It only takes one open hole for a hacker to gain entry into your network, which can lead to the loss of all your company’s proprietary and confidential information.

As a security provider, we often find that when companies install a firewall or security device they have the best of intentions. Then, after a period of time, they begin to overlook it as the day-to-day demands of their position encroach on their security tasks. After a while, they don’t perform the necessary maintenance on it, nor do they proactively monitor and manage it. Firewalls are left for months or even years without proper backups, security patches, or log review.

With the layoffs that have plagued many companies over the past few years, IT departments are overworked and understaffed. Naturally the highest priority is put on keeping the network running. It is understandable why proactive tasks such as network security and log review are given a lower priority.

To make matters worse, threats – and the technology to combat these threats – are constantly evolving. Most companies’ IT Staffs have trouble just keeping up with the latest vulnerability announcements, much less staying current with the latest technological advances from the security community.

The result is that companies often end up throwing money at a problem by purchasing more and more security devices. Sometimes this works, but more often the effort is misdirected and results in at best more network devices for an overworked staff to manage and at worst a complete waste of time and money.

A MSSP can solve this problem by reducing the demands placed on your IT staff and providing focused, actionable information about security events.

What Does a MSSP Do?

Functions of a MSSP can vary widely. Sometimes a so-called MSSP does little more than monitor security devices. The other extreme is those that provide turn-key management – so much so that the client is often not allowed direct access to the devices or even given possession of passwords. In the middle are those providers that offer a balance of management and monitoring to suit your needs, while still providing you with the level of control that you desire. A MSSP should, at minimum, provide the following services:

Log/Alert Review Regular review of security logs and alerts is critical to determine an organization's risk level. A MSSP will typically have tools to do this that will sift through vast amounts of information and pull out only the relevant pieces, thus avoiding a common problem in log analysis: information overload.

Reporting A MSSP should provide you with regular reports detailing any activity that requires action on your part, as well as any actions they took (security updates, rule changes, etc.).

Backups Critical security files, such as firewall, IDS, and router configurations should be backed up by the MSSP on a regular schedule.

Upgrades/Maintenance A MSSP should provide regular upgrades and maintenance, such as log rotation and rule cleanup, to your security devices.

Ruleset Changes A MSSP will interface with your security device to provide any rule changes that you require, or that are dictated by security events.

Monitoring Proactive monitoring of your security devices should be included with any service provided by a MSSP. In addition to simple up/down status, a MSSP should automatically check variables important for that specific device, such as processor utilization, disk space, or critical processes.

Portal Portals have become the gold standard for MSSPs. Every provider seems to tout the features of their portal as the most important feature of the service. Though this is overstating things a bit, a portal does have an important place in relationship with a MSSP: real time access to data. Via the portal, you should be able to access any information about your security devices that you would reasonably want to know.

Support A MSSP will provide a consistent support structure, and will be readily available in the event of a question or problem.

Benefits to Working with a MSSP

We've discussed what a MSSP is, and what a MSSP does, but what exactly are the benefits that a company would experience if they chose to work with a MSSP? This section explains some of the more commonly cited benefits.

Security Expertise Most small- and medium-sized companies do not have a security expert in house and rely on external assistance to make sure security is given the priority it deserves. Larger companies may have security expertise in house, however these persons often get sidetracked with day-to-day issues and security is moved to the back burner. MSSPs offer significant value in either scenario by providing security experts with one focus: keeping your information protected from all threats.

Specialized Tools A MSSP will have customized software to assist with security event notification and review. This will allow the MSSP to review data and respond to an event more quickly than a corporate IT department.

Cost Savings Security experts require a broad range of knowledge and experience. Because of this, such experts are difficult to find and expensive to hire. Continued training adds ongoing expenses. And if you want more than one resource, you must cross train others within your organization or hire more than one expert. Both options are often cost prohibitive. Companies can hire a MSSP for 20–30% the cost of a full time security administrator, and by doing so gain access to an entire security team.

Shared Knowledge Since MSSPs provide security services to multiple companies, knowledge from one client is commonly transferred to others. For example, if a bug or threat is discovered at one client's site a MSSP will be aware of that issue and proactively address it at other clients' sites before it becomes service affecting. All clients benefit from the experiences of any one client.

Trending Due to the amount of security data that is processed on a day-to-day basis, a MSSP can spot security trends far more quickly than the average corporate IT manager, who does not have the benefit of reviewing dozens or hundreds of disparate security devices. For example, a MSSP may discover an increase in attacks directed at a certain port, or attacks from a certain IP range. In either case, customers can be notified and secured before they experience the threat firsthand.

Reports & Security Documentation MSSPs typically provide reports and documentation regarding security incidents, actions taken, updates applied, potential threats, and more. These reports usually make it easier to show the value of security to non-technical staff. Further, the documentation often satisfies audit requirements needed by corporate policy or regulations.

Dependable Support Relationship A MSSP will provide ongoing security support structure that is unrelated to turnover or change in your workplace. And, since you are contracting with a company rather than relying on one person, your access to support will be more dependable.

Security Enhanced Procedures Security requires attention to detail in order to provide data confidentially, integrity and accessibility. Because of this, MSSPs have more stringent procedures and controls in place than their clients otherwise would.

Monitoring/Portal MSSPs will monitor your security devices and provide appropriate information via a portal. Not only are your critical devices being monitored 24/7, which

most companies are not doing at all, you have access to data you otherwise wouldn't have via a portal. Typical data delivered by MSSPs' portals include statistics about the health of your security devices and real-time information regarding security-specific events.

Free up internal resources When trying to adequately address IT Security with in-house personnel, managers quickly realize how time-consuming this venture can be. IT Security is a topic that requires deep expertise. In house personnel inevitably find that they are distracted from their core duties: keeping the computer network healthy and functioning correctly. By partnering with a MSSP, companies can eliminate this drain on overworked resources.

Reduce Potential for Incidents By proactively monitoring logs, looking for suspicious traffic, and applying security patches, a MSSP will reduce an organization's chances of an IT security incident.

Objectivity, Independence A MSSP is by nature a third party. Thus, they have no stake in the impact of any information provided or deficiencies found. In addition to being good business practice, this independence is often specified in regulations or called for by corporate auditors.

Peace of Mind Perhaps the biggest benefit of all is, by knowing that security professionals are proactively handling your IT security, a major source of worry is removed. This benefit can't be quantified. Its effect on the bottom line can't be measured. But it is most often cited by our clients as the number one benefit they experience by outsourcing their security management.

Summary

Outsourcing certain IT security functions is a growing trend in corporate America. Now that most companies of any size have a firewall and/or other security devices in place, many are beginning to realize that the complexities of IT Security are too much for them to handle internally. This partially explains the success of MSSPs.

The other factor leading to the rise in popularity of MSSPs is the fact that they cost-effectively enhance a company's security posture by proactively addressing deficiencies. Many companies believe they are being proactive today with their IT security, but few are going to the extent that can be reached less expensively by partnering with a MSSP.

By working with a MSSP companies can increase security, reduce strain on internal resources, and more effectively manage corporate risk.

For more information on MSSPs, please reference Webfargo Data Security's 3rd whitepaper in this series entitled "How to Select a Managed Security Service Provider," which can be found at www.webfargo.com/library.