WHITE PAPER

Managed Security Services Models: How They Work

Table of Contents

Executive Summary

In 2017, cyber attackers compromised over one billion accounts and records. According to Gartner, cybercrime costs will reach $2 trillion USD by 2019 and cybersecurity spending will reach **$1 trillion USD** by 2018.

The security landscape is becoming more complex and threats more pervasive and hostile. Mobility, bring your own device (BYOD), virtualization, multi-cloud, and social media are all vulnerable entry points into an organization and can pose risks if they are not properly managed. Due to the vast channels by which enterprises are vulnerable and can be attacked, as well as the impact of recent breaches in the news, security is at the forefront of board discussions.

Most organizations are primarily focused on keeping their systems operating at optimum performance, which consumes most of their IT department's resources. Not only do they lack the technology and security expertise to develop and maintain an effective security stance, they lack the budget and the time required to remain up-to-date on the numerous threats facing their organization.

With growing threats, tight budgets, increased regulatory pressure, and the need for premium security expertise, many organizations are turning to managed security services to bridge the gap, augment IT teams, and provide around-the-clock security system monitoring and management.

As organizations are realizing that challenges like premium skills shortages, tighter budgets, data proliferation, technology sprawl, and the rise in hostile threats necessitate partnering with external experts in response to changes in the industry, the market for managed security services is rapidly accelerating and maturing.

In a recent survey by 451 Research of 301 U.S. IT security professionals, 87% reported planning to migrate to a security-as-a-service (SaaS) model within the next year. A separate survey of in-house IT security professionals from February 2017 reported that 86% of IT security professionals either already partner or plan to partner with an MSSP to handle many of the Security Operations Center (SOC) responsibilities to monitor, analyze and respond to security incidents.

Source: The 5 Benefits of a Managed Security System, Nov. 17, Hitachi-Systems-Security.com

This paper describes managed security services models, how they work, and the benefits of engaging a provider to proactively monitor and manage security systems.

Mastering the Managed Security Services Market

Today's CIOs and CSOs face expectations, opportunities, and challenges that have grown tremendously over the last decade. In conjunction with emerging technologies such as DevOps, Public, Private and Hybrid Cloud, is the challenge of managing people, process and compliance. Wrapped around all of this is the concept of security. What "security" means for an organization has changed dramatically over the last several years.

The complexity of security and compliance programs have made it difficult for organizations to implement and maintain sufficient security capabilities. CIOs and CSOs have become overwhelmed with the pace of the regulatory and technology changes, all while balancing end user productivity data access to the associated security risk. The threat of a breach and the organizational impact is ever-booming. All these needs must be addressed while ensuring compliance within tight budgets and tighter timelines.

A solution that organizations are increasingly adopting is partnering with a Managed Security Service Provider (MSSP) to augment their security teams with the right people, processes and technologies to address gaps in their security program and secure their critical systems and data across the extended IT ecosystem.

How MSSPs Work?

Managed Security Services (MSS) is an ever-evolving and industry-driven approach to implementing, monitoring and managing an organization's ever-changing security needs. The services may be delivered in-house, through staff augmentation, outsourced to a service provider or a blended approach depending on the specific gaps or opportunities the organization wants to address in information system security.

An MSSP functions as an extension of the client's security organization, offering a multitude of services from the operational day-to-day security tasks of running security tools, as well as, alert response to the other side of the spectrum in executive level strategic security advisory services.

Integration with the MSSP

The keys to successfully selecting and integrating with an MSSP is to start with understanding the needs of the security program and breaking down the requirements into a matrix. The matrix should consist of current and future security technologies or services required, which of those items will be serviced in-house short term and long term, and an assessment of how well the current items are serviced as a metric to judge performance. Items that are serviced in-house with poor marks may be more immediate candidates for moving to a MSSP. Security services or tools that have yet to be or are not fully implemented to sufficiently realize the ROI or proper risk mitigation may be a great candidate for movement to an experienced service provider.

One of the most overlooked items when choosing a MSSP is understanding how integrated the relationship will be with the provider. If the organization is simply shifting a few routine tasks to a service provider, then the relationship is primarily governed by SLAs and a regular touch point. If the engagement is meant to be more integrated with the organization, then success will require effort and collaboration from all parties. The future is a more integrated approach to security service providers as industry specialization continues to outpace the ability of many organizations to change. The recommendations for MSSP integration are as follows:

1. Ensure the details of the services and technologies are defined and clearly communicated and create a responsibility matrix that the client and service provider organization agree upon. Gaps in the understanding of responsibility is a vulnerability often overlooked on new contracts.

2. Get to know the MSSP relationship manager and leadership. Ensure the personality and communication style is a fit for your account.

3. Maintain a clear escalation contact sheet and process available from the MSSP and one available to the MSSP of your internal contacts. When issues arise, minutes matter.

4. Appoint a relationship point of contact from the client organization that integrates well with the internal project management, IT, and security organizations as a conduit for a unified message and direction to the MSSP.

5. Establish the communication cadence and what reports or data points are expected from the MSSP in providing the right degree of transparency as to the service performance.

6. Integrate in-house security engineering and architects with the MSSP teams to discuss upcoming organizational needs and initiatives. Utilize face- to-face or video sessions as much as possible to build a virtual team.

7. Much like the internal IT or security teams need lead times and proper planning for success, the MSSP needs the same. Ensure that there is an integration step with the internal project plans to update the MSSP of changes or new integrations to reduce the likelihood of rushed delivery and to allow for proper planning.

8. For new products or service needs, the MSSP may be able to fulfill the requirement from their existing portfolio or provide guidance based upon their industry experience.

9. When selecting a new product for implementation, verify the experience the MSSP has in advance of the procurement. Organizations that select a product or service that is not the primary skill set of the MSSP may receive adequate instead of exceptional service.

Much like you would do for your own organization, keep in mind the skillset and experience of the MSSP when selecting products or services.

10. Incentivize the security team members for the mutual success of projects or services in which they are integrated with the MSSP. This reduces the instances of finger pointing and promotes team collaboration.

11. When working with strategic advisory, prepare to explain the needs of the organization as well as, documented and perceived security issues the organization is facing.

12. When working with the MSSP for board presentations, include any questions or data points specifically requested by the board as well as, include a small background summary of the board members, so the team can create reports or slides that cater to the individual board.

Security Advisory Services

Security Advisory Security Services include anything from risk assessments, program creation or evaluation, board presentation preparation, security leadership mentoring, executive security incident preparation, to senior security staff augmentation. In this scenario, a third-party service provider completes security functions that the organization may not be able complete on its own or wishes to bring in an external resource with an expansive background. Contracts are typically time and materials with billable hours for overage. Many times these types of services show their ROI by accelerating the maturity of the client security program and provide a second point of view for the CIO or CSO.

Services can include:

- Security Program Strategy Creation or Review
- Organizational Security Incident Response Planning
- Board Presentation Preparation
- Virtual CISO Services
- Security Control Framework Creation or Compliance
- Security Audits & Audit Support
- Security Risk Assessments
- Security Policies & Procedures
- Security Leadership Monitoring & Advisory
- Industry Change Trends & Analysis
- Cyber Security Insurance Advisory

Security service providers with advisory services are usually flexible and will tailor service deliverables to meet the changing business and security requirements of the organization.

Managed Security Services

Managed Security Services are more tactical than advisory Services. MSSPs maintain advanced security technologies and services that have been tested across many organizations, handling a variety of business requirements and threats.

More advanced service providers can integrate various products and services into a comprehensive service offering that can provide a rich flow of security information and reporting. Oftentimes, this information can be analyzed by the client or MSSP Security Information & Event Manager (SIEM).

Services offered by MSSPs continue to evolve and may include:

- Security Operations Monitoring
- Security Incident Response, Investigation & Forensics
- Security Information & Event Management (SIEM) as a Service
- Endpoint Detection & Response
- Data Loss Prevention
- Denial of Service Protection
- Mobile Device Management
- Multi-factor Authentication
- Web Application Firewalls
- Vulnerability Scans & Management
- Firewall Management & Compliance Reporting
- Intrusion Prevention System (IPS) management
- Email Security
- Web Access Security Services
- Multi-Cloud Enabled Security Services
- Configuration Baseline & Management
- File or System Integrity Monitoring
- System Controls Compliance Monitoring & Reporting
- System & Application Patch Management
- Network or Application Penetration Tests
- Security Training, Testing & Reviews
- Identity Access Management
- Privileged Access Management
- Cloud Access Security Brokers (CASB)

Managed Security Services Benefits

There are a number of benefits of managed security services models. Figure 1 outlines value-based benefits.

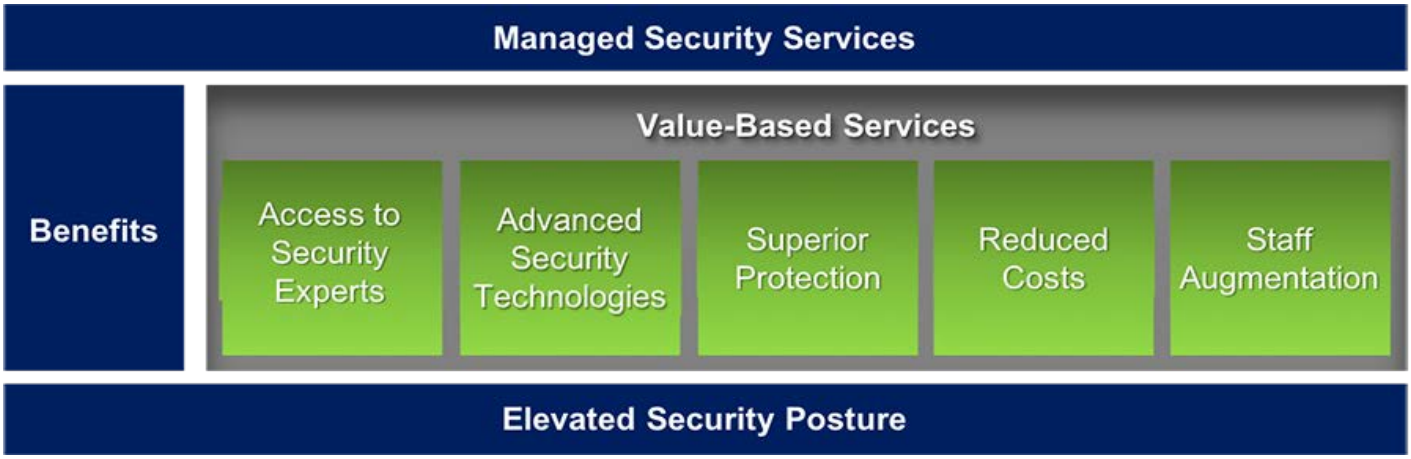

Figure 1

• **Access to Security Experts.** Access to skilled resources without having to spend on continuously hiring and training IT security staff. MSSPs have highly skilled security professionals who keep up-to-date on the latest threats and how to remediate them. Quality MSSPs provide assistance to businesses to not only meet compliance needs, but also to tailor their cybersecurity program to the unique needs and risks specific to each industry.

• **Advanced Security Technologies.** MSSPs maintain advanced security technologies that have been tested across many organizations, handling a variety of threats as they continue to evolve.

• **Superior Protection**. MSSP experts can take companies beyond the security basics by providing in-depth security for advanced security requirements, like threat analysis and remediation, BYOD protection and advanced anti-malware.

• **Reduced Costs.** MSSPs allow businesses to replace large capital expenditures associated with investing in new cybersecurity tools and capabilities with predictable, ongoing operational costs.

• **Staff Augmentation.** Security is a business issue and it must be managed so that the business and its executives can maintain a laser focus on the company's mission. The organization exists to serve customers, protect and engage its employees, and deliver value to its shareholders. Engaging an MSSP allows organizations to focus on strategic initiatives.

Managed Security Services Checklist

There a number of factors involved when choosing an MSSP.

- **Expertise.** Does the MSSP have the expertise to meet my company's security requirements? Ensure that the provider has the talent, experience and capabilities to deliver exceptional service. A good MSSP should have experts in various security and protection areas. Is there a technical team that regularly reviews industry standards?

- **Technology.** What types of technology does the MSSP use to protect my infrastructure against traditional and advanced threats? How does the MSSP handle scanning, encryption and centralized logging and reporting? What level of flexibility within the technology is available? Does the MSSP deploy security using virtualized security solutions like virtual firewalls/IPS?

- **Compliance.** Can the MSSP support your compliance requirements? Do they understand the requirements for the various industry and regulatory controls applicable to your organization?

- **Cost.** How much will it cost? Will my business see the value provided by the MSSP? Cost should not be the sole deciding factor in selecting an MSSP, as the cost of the services is only part in the security risk calculation.

- **Scalability.** Can the managed security service solutions scale with your business? The cost of an MSSP SLA should include monitoring, management, and reporting.

Finally, when selecting an MSSP, organizations must ensure that the MSSP will be a strategic partner. An MSSP is hired to protect IT infrastructures and critical data. Ensure that they are in it for the long haul and have the required capabilities.

Choose an MSSP who will be a trusted security advisor.

The Right Managed Security Services Provider

Managed Security Services Providers are not created equal. So, finding one to work with can be painful, even more painful if it's the wrong one. With more than 17 years of providing critical IT managed services, Secure-24 has worked with some of the world's largest organizations and delivered innovative services to increase the protection of their data, brands and reputations.

The right managed security services provider will enable organizations to:

- Align Security Policies with Business Strategy. Develop a security plan to manage risk, support compliance, and protect against threats.

- Maximize IT Productivity. IT teams can focus on strategic initiatives and other business critical projects.

- Manage Costs. Organizations can shift from a CAPEX to an OPEX model with predictable costs. MSSPs can help also reduce the resources dedicated to security monitoring and management.

- Optimize Network Reliability. Security professionals provide around the clock monitoring and and quick remediation of security incidents to minimize disruptions and the impact of attacks on the network.

Conclusion

Managed Security Services Providers are and will continue to play a significant role in the security landscape. The question isn't if there will be a security breach, rather, it's when. The ultimate question remains: do organizations have the proactive monitoring and advanced technologies to secure information and data systems?

Through advanced, integrated technologies, unparalleled threat detection intelligence, and security expertise MSSPs can help enterprises mature their security programs to protect mission-critical systems and data.

Disclaimer. The following is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Secure-24 services remains at the sole discretion of Secure-24.

About Secure-24

Secure-24 has 18+ years of experience delivering mission critical application hosting, comprehensive managed IT, and cloud services to enterprises worldwide. Secure-24's focus on superior service, support, governance and compliance has driven industry-leading client satisfaction rates.

Secure-24 is SAP-certified in cloud and infrastructure, hosting, and SAP HANA operations, a Microsoft Fold Partner, and an Oracle Gold Partner managing Oracle E-Business Suite, PeopleSoft, JD Edwards and Hyperion applications across all industries for businesses of every size.

Secure-24 specializes in successful outcomes. By making every client's IT, cloud and security requirements work seamlessly together, managing all systems in concert and treating each client like they are our only client, Secure-24 stands alone in the industry as an independent Managed Cloud and Security Services provider.