The IT Security Enforcer’s Advisory on Managed Security Services Models and Execution
The IT Security Enforcer’s Advisory on Managed Security Services Models and Execution

Security is about protection, and in the enterprise IT environment, that means protection of a burgeoning array of physical and digital objects. Most objects, or property, within an enterprise can also be defined as assets, making IT security at its most basic level about maintaining the health of a business’s balance sheet. That commercial and operational significance should inform how managed security services (MSS) are developed and delivered to enterprises. Solutions need to address not only individual objects/assets but also the overall wellbeing of the business.

Today’s enterprises operate in a highly heterogeneous, virtualized technology environment, where easy access to both information and tools encourages the proliferation of new devices and services. Sanctioned and unsanctioned “bring-your-own-device” (BYOD) as well as “Shadow IT” deployments for departmental solutions contribute to this amorphous landscape. For IT security, management needs to be agile and look well beyond traditional concepts of perimeter protection and assess the specific risks to enterprise data, devices, users, and applications—in addition to enterprise networks—within this dynamic and shifting hybrid environment.

Table 1: Enterprise IT and Information Assets

<table>
<thead>
<tr>
<th>Assets</th>
<th>Examples</th>
<th>Vulnerabilities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Financial, employee, customer info</td>
<td><strong>Hardware and software</strong></td>
<td><strong>Sabotage</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access and authorization</td>
<td><strong>Espionage</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application data</td>
<td><strong>Theft</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User data (passwords, personal data, social networks)</td>
<td><strong>Vandalism</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network traffic</td>
<td><strong>Ransom</strong></td>
</tr>
<tr>
<td>Application</td>
<td>CRM, ERP, CMS, email</td>
<td><strong>Hardware and software</strong></td>
<td><strong>Sabotage</strong></td>
</tr>
<tr>
<td>Device</td>
<td>Server, appliance, PC, tablet, smartphone</td>
<td>Access and authorization</td>
<td><strong>Espionage</strong></td>
</tr>
<tr>
<td>User</td>
<td>Employee, customer, supplier, partner</td>
<td>Application data</td>
<td><strong>Theft</strong></td>
</tr>
<tr>
<td>Network</td>
<td>LAN, WAN, Internet</td>
<td>User data (passwords, personal data, social networks)</td>
<td><strong>Vandalism</strong></td>
</tr>
<tr>
<td>Service</td>
<td>Internet, cloud</td>
<td>Network traffic</td>
<td><strong>Ransom</strong></td>
</tr>
</tbody>
</table>

- **Data** is the most fundamental enterprise asset; all businesses have it and it interacts with all the other types of enterprise asset. Unlike devices or networks, for example, it does not come with any of its own security features.
Managed Security Services Models and Execution

Applications differ between and within different enterprises, but exhibit similar vulnerabilities in terms of exposure to operating systems, hardware and networks, as well as the integrity of the data they generate and the code they run on.

Devices are similarly diverse within a given enterprise, but fall into common classes of user and system hardware. System devices tend to share the same vulnerabilities as networks and services, while the threats to user devices often involve user-specific data and applications. Devices can and do come with at least some integrated security features—for example, biometric authentication, or anti-virus software, or wireless encryption for a Wi-Fi router.

Users are perhaps the most variable of enterprise assets, both within and across different organizations. And it is their myriad individual uses of IT—their accounts, passwords, authorizations, personal data, and custom applications and interfaces—that are liable to threats.

Networks, which host enterprise environments made up of all of the above assets, have traditionally been a logical place to focus enterprise security, with the hope that protecting the whole will provide safety to the parts. Firewalls, unified threat management (UTM), and incident detection/protection services (IDS/IPS) all help secure the enterprise perimeter, working with routers to filter, block, and mitigate threats.

Services introduce vulnerabilities to other parts of the hybrid IT environment navigated and consumed by enterprises. Securing access to Internet and cloud services can mitigate some threats, but not all. Some of those security features come with the service, and some do not.

Added together, these elements of the hybrid IT environment represent a significant challenge to each business in protecting its assets against threats carried out in various emerging forms like phishing, distributed denial of service (DDoS), malware, or botnet attacks. They give both enterprise IT managers and their managed security service providers (MSSPs) an exceedingly complex task in their pursuit of cyber defense, making agility perhaps the most important ingredient in addressing it.

With the landscape changing much faster than any one tool, appliance, or service can be deployed, it is essential to avoid the obvious allure of the “big fix”. To do so, organizations should move toward a resilient approach, building security in and around each core element of the enterprise IT system. Meanwhile, the cost and expertise required to build and maintain internal security architectures and teams requiring constant upgrading and strengthening is driving many enterprises to seek partners for advanced managed security services. Working together, the enterprise and its MSSP partner can cooperate within a flexible framework and strategy, combining best of breed tools with proactive and reactive defense based on a shared, agile cyber defense strategy. Enterprises can access the resilient threat defense needed under a security-as-a-service consumption model.

Working together, the enterprise and its MSSP partner can cooperate within a flexible framework and strategy, combining best of breed tools with proactive and reactive defense.
Securing the Extended Enterprise

Getting there means deploying, integrating, and rationalizing a variety of traditional and advanced security tools and technologies. Most large enterprises have a range of solutions built up over several product generations to secure the wide area network (WAN), local area networks (LANs), and desktops.

Traditional Security Methods

Firewalls are installed on network perimeters and configured to block unauthorized traffic. Enterprises tend to have a mix of firewall solutions deployed to filter network packets and application layer traffic going in and out of the secure environment. Managed firewalls offering ongoing monitoring, maintenance, upgrades, and remediation are common, often incorporating IDS/IPS, identity management integration, and web application firewalls (WAF) for filtering HTTP traffic of specific web applications.

Enterprises tend to have a mix of firewall solutions deployed to filter network packets and application layer traffic going in and out of the secure environment.

Encryption solutions are implemented to secure data and documents, authentication for access and authorization, and network traffic. Encryption is often a component of a communications service, such as IP VPN, secure email gateway, or secure socket layer (SSL) for securing web browser access.

Anti-malware solutions are deployed on both enterprise networks and clients, ranging from desktop anti-virus to server-based email scanning, spam blocking, and content filtering. Anti-malware features are found within unified threat management (UTM) solutions and services which bundle firewall and IDS/IPS with gateway-level anti-malware features, VPN, load balancing, and/or data loss prevention (DLP) features.

Identity and access management (IAM) systems are used to safeguard and control user identities and their permissions for accessing IT and information systems, applications, and resources. Key features include single-sign-on (SSO) for authorizing access across multiple resources, and multi-factor authentication to protect against lost/stolen credentials.

Advanced Security Methods

In recent years, advanced security solutions and methods have been sought by the enterprise to provide more adaptive protection against threats as a result of growing use of applications in the cloud.
Cyber security is increasingly being used to describe solutions that focus less on the protection of individual assets or components and more on taking a comprehensive proactive approach against known and unknown threats. There is a human element (security analysts) alongside newer technologies, including threat intelligence and analytics platforms.

Cloud computing is rapidly transforming the way IT infrastructure and applications are deployed and consumed, with virtual networked assets exposed to threats well outside of the traditional enterprise environment. Because of these factors and the advanced threats faced by the increasingly digital enterprise, IT organizations and their partners are shifting their security strategies away from prioritizing standalone technology tools such as firewalls and anti-virus software, and more toward agile solutions developed around overall security methods and processes.

Managed Security Services for Cyber Defense

To be sure, enterprises can and do rely on MSSPs to manage ad hoc pieces of the traditional and more advanced security puzzle. For example, a new security appliance or software is installed (perhaps with the help of an MSSP acting as integrator), but soon after, the enterprise realizes it lacks the resources to manage and maintain it, or to leverage its benefits beyond the bare minimum. As a result, many large organizations not only have a “hodgepodge” of security tools installed but also an unstructured and inefficient stable of managed services contracts all working independently of each other.

In some cases, having a partner on which to rely for essential operations and maintenance will satisfy the needs of an otherwise proactive, well-staffed, and strategically-driven IT security organization. With the desire (and the resources) to own security responsibility internally, this kind of organization can make even a patchwork of various solutions work. Partners may be chosen for their specialist capabilities, or they may be engaged to ensure security controls and policies are in place which the internal team can then use as a baseline. MSSPs can also be engaged for incident response or post-breach forensics and mitigation.

But in other cases, enterprises seek an MSSP that is able to take on more than just managing a device or a specific task or a set of policies, or to help out tactically in response to specific incident. Whether it is called security as a service, end-to-end managed security, or managed cyber defense, strategic partners can and are being leveraged to take a holistic approach that extends to ownership of the function of security systems, security policies, and security incidents and events. The driver for these enterprises is often an internal skills gap and the resulting lack of in-house resources to manage security end to end.
At the same time, enterprises increasingly acknowledge the logic of adopting a security as a service model which guarantees, in theory, as-needed provision of skilled talent and expertise and full partner responsibility for systems, policies, and controls, with dynamically upgraded solutions that keep pace with increasing sophistication of both security tools and threats. For these organizations, there is a strong sense of security—in the general sense—when a trusted partner steps up to take responsibility no matter what happens within the broad guidelines of its remit. If cyber defense is the goal—that is, provision of an overall set of resources to protect the enterprise from cyber threats no matter where or how they manifest themselves—MSSPs and security as a service are a logical way to reach it.

Engaging the Managed Security Service Provider

As already mentioned, traditional MSSP service packages often center around a specific function, policy, tool, or technology—for example, managed authentication or managed firewall services—with function-specific packaging in the form of delivery, customer support, and service levels.

Table 2: Examples of Traditional MSSP Service Models/Bundles

<table>
<thead>
<tr>
<th>Service</th>
<th>Components</th>
<th>Options</th>
</tr>
</thead>
</table>
| Managed Firewall         | End-to-end management and monitoring of platforms located at the customer premises or in a hosted (single-tenant) or cloud (multi-tenant) deployment model. | • Standard, Select and Premium service levels  
|                          |                                                                             | • Firewall optimization, with advanced analysis of firewall rules and helping to extend security, performance and compliance enforcement |
| Managed Identity         | Integration and management of authentication solutions (software, hardware, or web tokens); managed digital certificate services | • Cloud authentication, leveraging corporate directory for secure cloud app access           |
| Endpoint Protection      | Managed protection of mobile and other devices (smartphones, tablets, PCs, Wi-Fi__33 routers, VPN clients) | • Per-device license and/or management fees  
|                          |                                                                             | • Can be bundled with mobile device management, application management services          |
| Data Leakage Protection  | Solutions for protecting enterprise data from leaking outside of the internal IT environment. | • Project-based consulting and integration  
|                          |                                                                             | • Solutions for network perimeter, database, application data leakage; on-premise or as a service“ |

These examples illustrate both how MSS services are defined, and also how they are valued. The enterprise contracts a provider to deliver a specific capability, tool, or expertise, within an agreed-upon framework based on
Managed Security Services Models and Execution

the organization’s landscape and requirements, and, ultimately, what the MSSP is able to guarantee.

Advanced managed security services, by contrast, are designed not around management of an individual tool or function, but rather a process for defending against a variety of threats. Customers aren’t outsourcing system operations, they are subscribing to delivery of a defined level of protection.

Table 3: Examples of Advanced MSSP Service Models/Bundles

<table>
<thead>
<tr>
<th>Service</th>
<th>Components</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Management</td>
<td>Software license-based, with optional components including appliances, standard support services (included in license first year, chargeable thereafter)</td>
<td>• Premium level support</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Flexible pricing of license based on a daily average of messages per second (MPS)</td>
</tr>
<tr>
<td>Threat Monitoring</td>
<td>Scalable per-device pricing</td>
<td>• Based on specific requirements ranging from simple (end-point nodes) to complex (web application firewalls) or any tailored mix</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Per-day consultancy</td>
<td>• Service levels (time to respond, time to resolve)</td>
</tr>
<tr>
<td>Managed SIEM/Analytics</td>
<td>Managed or cloud-hosted threat intelligence/analytics platform, supported by security analyst teams</td>
<td>• Often packaged as part of a “CyberSOC” solution inclusive of anti-DDoS, APT (advanced persistent threat), IDS/IPS services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Threat analytics for automated aggregation, analysis and reporting</td>
</tr>
</tbody>
</table>

Best Practices in MSSP Engagement

For basic managed security services, following such service definitions and delivery frameworks is sufficient for the enterprise organization that prefers to (and is able to) handle overall responsibility for threat protection and security controls with third-party help for specific management tasks. In these cases, common measures for SLA measurement and enforcement are enough, because the enterprise is consuming the MSS as a component within its own operational ecosystem.

With advanced security services, it is not so simple to work within traditional engagement models. Multiple technologies and solutions (e.g., DDoS protection, threat management, cloud security, threat intelligence) may be included in an integrated package. Even separately, advanced security services introduce complexities that, while enabling a very powerful solution, are no longer black-and-white when it comes to measuring service benchmarks.
Managed Security Services Models and Execution

April 2017

While a large part of managed security services are still SOC-centric—that is, focused on monitoring and managing tools and devices in a dedicated enterprise security operations center (SOC)—models are necessarily evolving within the context of the cloud. Fewer elements are under the direct control of the enterprise or provider, and threats are apparent beyond the traditional enterprise perimeter. In this environment, the importance of developing a shared strategy with the MSSP can help the enterprise meet the challenges of environmental change.

**Challenge: How to Develop a Security Strategy Roadmap for Scale**

A strong and trusted provider should be able to outline the process of how new capabilities will be integrated.

Constant change is one of the biggest challenges to all IT environments—and with security especially—due to the uncontrolled and largely external nature of the threat landscape. When engaging an MSSP for individual advanced solutions, or in an overall security as a service or cyber defense model, those changes and challenges must be shared.

In collaboration with its provider, the enterprise must work out in advance how and when upgrades and improvements will be onboarded, how system interoperability will be solved, and how knowledge will be transferred. A strong and trusted provider should be able to outline the process of how new capabilities will be integrated (along with expected improvements in delivery), for example, through new automated processes.

This can be achieved following an initial audit of the enterprise environment, agreeing on the parameters of its current threat landscape and combining it with a forward-looking view based on the MSSP’s roadmap. In addition to the overall responsibility taken for systems, processes, and policies, the MSSP can extend that responsibility to include market intelligence, providing assessments of the latest vendor technology assessments as they emerge, and providing regular briefings to enterprise management on what to expect in the coming quarter and year. This proactive, advisory component to an MSSP engagement will go a long way toward proving the provider’s shared commitment, enhancing overall trust.

**Challenge: Data Residency and Data Flows**

IT organizations and MSSPs use various methods to provide security for enterprise data in storage and in transit. With the growth in adoption of cloud computing and increasing concerns over data privacy and regulatory compliance, control over data flows and data residency is an issue for which enterprises can seek solutions from service partners. As more and more IT workloads become virtualized, cloud service providers are delivering geo-specific hosting to ensure data sovereignty—where required—is enforced. Even when such compliance is not
explicitly required, vulnerability based on unclear, changing, or pending legislation and regulation means that businesses are erring on the side of caution.

Providing security for such deployments can become challenging. Key components of MSSP portfolios are often delivered from a centralized global SOC. Regionals capabilities—and regional SOCs—are increasingly required to maintain the integrity of legal data residency. Partnering with an MSSP with regional SOCs capable of providing compliant solutions with local knowledge and support can help overcome these challenges. As part of their selection process, enterprises can look for regional security certifications and compliance along with the global, technical credentials that MSSPs may offer.

**Challenge: Affirming Service Levels**

Service level agreements (SLAs) form an important part of any managed services contract, but they can also fail to achieve the overall objective of the relationship. Because not all circumstances are under the service provider’s control, no MSSP can offer 100% protection and/or remediation against all enterprise threats. And when metrics fall short, contractual penalties are usually no substitute for loss of data, intellectual property, or productivity.

That said, SLAs remain a fundamental building block for the MSS engagement, and enterprises should make sure there is complete transparency regarding definitions of metrics, reporting, and responsibilities arising from the results of regular reporting. For example, an MSSP dutifully reporting monthly security incidents falling from a typical average of thousands to zero in the last month may be adhering to its agreed reporting SLA. The fact that the last month’s report showed zero incidents because the provider’s systems failed may not be captured or communicated because the defined SLA does not require it. That is not the sort of SLA affirmation an enterprise should accept.

Advanced services require advanced SLAs, enabling reporting that not only encourages proactive service and communication, but also empowers the enterprise to monitor how the MSSP and its platform are performing in real time, against confirmed metrics. In this sense, the enterprise needs to be able to “watch the watchers” in order to go beyond arbitrary enforcement to shared performance management.

This can be achieved two ways: 1) through the same regular briefings communicating advice and market intelligence, enterprises can also receive interactive reporting—allowing them to hold the MSSP’s “feet to the fire” on SLAs; 2) through platform visibility via service dashboards, bringing together self-service controls with an enterprise view of the SOC management console and real-time reports on service delivery for defined services (e.g., DDoS, SIEM, UTM, etc.). In this way, enterprises won’t be inundated with potentially meaningless reports but can seek real-time insights on service delivery when required.
Conclusions and Recommendations

Each enterprise is different, but every enterprise needs increasing levels of IT and cyber security, and managed services are increasingly offering solutions for basic and advanced services. Enterprises should embark on MSSP engagements with the goal of forging a stronger framework for protecting enterprise assets by enlisting a trusted partner.

Enhance Protection of Enterprise Assets with MSSP Engagement

Enterprises should not focus too much on device-specific or service monitoring. Internal reporting exercises can devolve into rote busywork that misses the point of security processes and controls. Managing security should not mean managing a sensor or log file—it should mean protecting the enterprise’s IT assets. As such, enterprises should plan for the evolution of security controls toward increased MSSP engagement.

Partnership Approach

By engaging more closely with the MSSP—from initial auditing, to collaborative planning, to forging strategy—enterprises can ensure that their providers perceive their own role as the trusted partner they require. Sharing responsibility for strategy, monitoring, management, and mediation guarantees a stronger and more relevant solution.

Documentation, Reporting, and Remediation Controls

Sharing responsibility, however, does not take the MSSP off the hook. Closer engagement from the client side only makes documentation and reporting more meaningful. Care should be taken from the beginning to define the reporting process, but also all associated processes. What is the point of reporting an event without explaining its context? What is the point of identifying a problem without immediately seeking a solution? Service reporting must extend to frameworks for escalation and remediation, all with the shared goal of full protecting IT assets.

*Care should be taken from the beginning to define the reporting process, but also all associated processes.*
Perpetual Review

MSSP engagements should also include a formal mechanism for ongoing or perpetual review of defined processes and the overall engagement. This is additional to the regular interactive briefings MSSPs should be providing for meaningful communication of performance and roadmap. At a more strategic level, management stakeholders from client and provider need to make sure the engagement is working at optimum levels. This process will further strengthen a relationship that should already be very close, but too often is kept at arm’s length.