Stratecast Partners *A Division of* **FROST & SULLIVAN**

Why Enterprises Outsource Network Security

Executive Summary

Network security as a topic is continuously in the business headlines and, increasingly, discussed in boardrooms. Furthermore, for a growing number of enterprises, improving network security and complying with layers of security regulations form an inescapable mandate but a mandate without crystal clear directions or an endless checkbook.

Faced with these realities, enterprises should apply due diligence into evaluating all its options. One of those options is an outsourcing relationship with a credible Managed Security Services Provider (MSSP).

At minimum, outsourcing of network security can overcome many of the constraints enterprises face in addressing network security alone. Those constraints include:

➢ Lack of adequate expertise and professional processes

➢ Time for security improvement is short

➢ Maximizing return on previous security investments

➢ Having firm assurance that tangible improvement in network protection will be accomplished

➢ Building a close and continuous alignment of network security and business objectives

Even though outsourcing security can assist in overcoming these constraints, many enterprises still do not pursue this path because they perceive cost-savings to be limited. Unfortunately, many cost-related decisions are too narrow in scope and are solely based on one's perspective of near-term direct costs and miss the bigger picture of near and long-term cost avoidance and a full accounting of the benefits received. Consequently, despite the fact that it may be a better option, outsourcing may be prematurely discarded. Only when comprehensive business cost and benefit analysis on outsourcing is completed does an enterprise gain a full appreciation of the full value a MSSP relationship can offer.

As part of this study, we detail the costs incurred in delivering competent and dependable network security to your organization. We also describe how the two structural and correlated characteristics of the MSSP business model result in higher levels of economic benefits and security effectiveness for the enterprise than possible through an in-house approach. Those two characteristics of the MSSP business model include:

1. Shared resources and economies of scale, and

2. Proficiencies.

We conclude our study with a review of VeriSign, a major provider of security infrastructure and services. Extensive and competent visibility into looming security threats, multiple levels of experience, and dedication to customers positions VeriSign as top contender for your security outsourcing business.

Introduction

Increasing expenditures on network security is a reality for many enterprises. However, accepting increases without first conducting the same rigorous evaluation that is applied to other business expenditures is a sub-standard practice. While it would seem unfathomable that any enterprise would accept increases in security expenditures without first conducting a cost-benefit analysis, this sub-standard practice does occur for enterprises who fail to quantify the full cost of deploying and managing network security.

Although no two enterprises are exactly the same in terms of network resources to protect and the value each enterprise assigns to security, network security costs do fall into two similar categories for all enterprises: technology and expertise. Only when a full understanding of what security technology can and cannot accomplish is combined with the advantages of various means to best leverage the security technology does the cost-benefit analysis become an effective decision-making tool.

In this report, we will describe why managed security services, a partial or full alternative to in-house management, should be considered by enterprises as an effective means to improve security cost management while also improving network security. We will begin our analysis with context on why network security is becoming increasingly strategic for enterprises. Following this context, we will describe the reasons why enterprises are outsourcing the management of security. The next section provides the rationale for choosing a Managed Security Services Provider (MSSP). Last, we will conclude with an assessment of VeriSign, an international provider of managed security services.

Trends in Enterprise Networks and Security

There are three concurrent trends that are placing network security as an increasingly strategic imperative for enterprises. They are:

1. Enterprise networks are becoming more open,

2. Security threats are advancing in speed, sophistication, and potency, and

3. The penalties for inadequate network protection are rising.

Each of these trends will be discussed in sequence.

1. Enterprise networks are becoming more open

A combination of technology push and productivity pull is compelling enterprises to open their networks to a broadening range of users, access devices, and access methods. For example, expanding availability of affordable wired broadband access, WLAN access points (public hotspots and corporate wireless LANs), and higher speed mobile wireless networks in addition to continuous advancements in miniaturization and performance of mobile devices (e.g., laptops, PDAs, and smartphones) have greatly reduced the technology hurdles for network-connected users to virtualize the office environment anywhere. In fact, these

advances represent a critical stepping-stone for enterprises in improving their market competitiveness by providing network connectivity and flexibility for all potential users of networked resources (workers, business affiliates, and customers).

However, unless robust controls are established and continuously managed, the risk to the enterprise network and sensitive corporate information intensifies to the point that enterprises must respond by restricting the more open access they need to support their business objectives. As a result, enterprises forego a portion of the productivity improvements these technologies could enable.

2. Security threats are advancing in speed, sophistication, and potency

With almost daily occurrence, news stories report new attacks or security breaches of an enterprise network. On a more individual basis, few laptop and desktop users can claim they have never been infected or at minimum inconvenienced by a virus or worm. Concurrently, business use of traditional security technologies (e.g., firewalls, anti-virus filtering, intrusion detection, and VPNs) is becoming commonplace and adoption of newer security technologies (e.g., behavioral-based traffic filtering) is on the rise. Therefore, the logical conclusion is that the malicious elements are advancing at a faster pace than enterprises can address their network vulnerabilities. There are several reasons for this:

- **The hacker community operates more like an efficient organization than distributed and disconnected pockets of individuals -** Hacking tools and shared experiences are readily available for hackers to quickly improve their skills. Consequently, the time window from recognition of software vulnerabilities to actual attacks is shortening.

- **Attackers are skirting traditional network-layer parameter defenses and exploiting application-layer vulnerabilities -** Even so, traditional attack methods are not becoming dormant so retiring traditional defenses is not practical. As a result, enterprises incrementally supplement their security infrastructure on an as needed basis, too often after experiencing a material attack.

- **Attack originations are not limited to external, unauthorized users -** Attacks and misuse of network access by LAN-connected users can be equally if not more disruptive than external attacks because the user has the benefit of insider information. Frequency of attacks is also a problem; according to the annual FBI/CSI surveys insider security breaches consistently occur with greater frequency than external-based attacks.

- **A new breed of sophisticated, methodical, and well-financed attackers are changing the complexion of the hacker community -** The malicious and fame-seeking hackers are now supplemented with attackers with fortune aspirations perpetrated through acts of extortion and information theft.

3. The penalties for inadequate network protection are rising

There are several points that support this statement as outlined below:

- **Network disruption and/or performance degradation (e.g., slow response times) attributable to an attack reduces an enterprise's return on investment**

in business applications and network infrastructure - Simply stated, investments in applications and network infrastructure were made to support business objectives. If attackers compromise the reliability of the network and subsequently user access to applications and application responsiveness, the enterprise is not receiving the full benefits anticipated in these investments.

- **Penalties for non-compliance in regulatory requirements, industry standards, and internal corporate policies keep rising too -** While monetary penalties are the most quantifiable, they are not the only penalties that are incurred. Recovery from negative publicity and damage to business and customer relationships is costly as non-compliance events seize the time, talent, and motivation of corporate resources that would otherwise be directed toward meeting business objectives. Other related expenditures associated with meeting compliance include:

    - Staying current on compliance requirements and translating those requirements into effective device and process-level instructions requires an additional knowledge set.

    - Monitoring, reporting, and improving actual compliance level is a continuous operation. Furthermore, a stable level of compliance, not an average with considerable variation, is required. Even a temporary reduction in security posture represents a window of opportunity for a devastating event and/or penalty.

- **Proliferation in security point product adds to management cost through complexity -** In addition, protection gaps can exist through sub-optimal cross-vendor device interoperability.

- **In consideration of network openness and device mobility, the potential of re-infection by worms and viruses is present -** Without thorough remediation or quarantining of infected devices and subsequent scanning of all accessing devices, the potential for re-infection exists resulting in additional cycles of detection of infected devices and remediation.

Enterprise Reasons for Outsourcing Security

In consideration of the trends previously outlined – network openness, advancing security threats, and the penalties for inadequate security – we believe that the time is right for enterprises to seriously consider partial to complete outsourcing of their network security. In making this transition, we believe enterprises will benefit through a more economical and effective approach to protecting their network and the resources hosted within. We will describe in greater detail how economic and effectiveness benefits are generated in the next section. Before doing so, it is important to recognize the constraints enterprises face in attempting to address these three trends exclusively with in-house personnel.

- **A lack of adequate expertise and professional processes** – Absent adequate resources, an enterprise's ability to protect its network from the evolving nature of security threats is a growing a challenge. Moreover for most enterprises, the cost to acquire and retain the talent needed to build an in-house dedicated and professional security practice is prohibitive.

- **Time for security improvement is short** – Even if the enterprise has the expertise, it may not have the scale to improve their security infrastructure in a desirable length of time. Furthermore, creating the scale would be a misdirection of corporate effort if the necessary scale to improve security were materially more than what is needed to manage the upgraded security infrastructure going forward.

- **Must maximize return on previous security investments** – For many enterprises, their security infrastructure is an accumulation of years of incremental investments in point security solutions and/or the result of acquisitions of other companies. However, starting with a clean slate to improve the network security infrastructure is not a practical option. Alternatively, constructing a plan on how to improve the enterprise security environment by leveraging existing infrastructure and supplementing with targeted investments requires a broader range of security expertise than most enterprises can claim to have.

- **Firm assurances of tangible improvement in network protection are needed** – Correlated with the previous point, assurances are required in making any new security investments. Layering on additional devices without the means to measure improvement is an incomplete approach to advancing network security. Building the monitoring, measurement, and reporting capabilities necessary to demonstrate improvement is a complex task.

- **Security must be aligned with business objectives** – Excessive levels or over-reactionary security responses can come at the price of restraining the enterprise's ability to meet its business objectives. Alternatively, security must be applied in a measured fashion to continuous balance business needs and network protection.

Managed Security Services Deliver Economic and Effectiveness Benefits

There are two structural and correlated characteristics of the MSSP business model that creates a more economical and effective security delivery model than an enterprise's exclusive reliance on in-house resources. They are:

1. Shared resources and economies of scale, and

2. Proficiencies.

1. Shared resources and economies of scale

The one-to-many attribute of managed services (i.e., one resource – person, process, or platforms - serves multiple customers) creates a lower cost per customer for the MSSP than the cost structure of an enterprise with in-house security resources. In addition, the larger operational scale of MSSPs (i.e., economies of scale) relative to most enterprises also contributes to a lower per customer cost base. Elements of the MSSP service delivery model where this is present include the following:

    a. Security personnel

    b. Infrastructure, process, and procedure investments supporting:

        i. Security information and event management

        ii. Regulatory and industry compliance assessment and reporting

   iii. Security device evaluations

   iv. Security device implementation

   v. Continuous management and maintenance

   vi. Help Desk support

  c. Volume purchasing agreements

2. Proficiencies

There are two contributors to a MSSP's proficiency advantage over enterprises: (A) operational efficiencies and (B) operational effectiveness. Each of these is described below:

A. Operational Efficiencies

Through operational efficiencies, the MSSP can typically close windows of vulnerabilities and complete security operations faster than most enterprises. This is attributable to MSSPs maintaining a larger number of available resources and established processes to serve its enterprise customers. With a larger base of available resources, the MSSP delivers to its customers shorter execution times (i.e., a turnkey-like operation) in both single vendor and multiple vendor operations than is possible from enterprises with more limited in-house resources. Furthermore, similar operations that the MSSP conducts for multiple enterprises leads to experience-based time efficiencies. Part of this efficiency gain is through streamlining and another part is through learned and shared experiences. By encountering a diversity of customer situations, the MSSP can re-use what is learned from one customer to the next and, through this process, avoid unnecessary time in re-creating solutions or work-arounds for each customer. Essentially, the MSSP builds a library of experiences to utilize in serving its customers.

B. Operational Effectiveness

Operational effectiveness of a MSSP creates a more direct path to security improvements. This is visible in two areas.

- Because the MSSP has the objective to serve the customer, not a security vendor, highly effective MSSPs will view the enterprise's security environment holistically, not as discrete security products or services. With this holistic rather than a piece-parts perspective, improvements in an enterprise's security infrastructure will be more robust as they follow a comprehensive plan, rather than a more limited treatment of the latest security concern.

- Similar to the point made under operational efficiencies, experience gained through repeatable operations conducted for multiple enterprises leads to a widening knowledge base. Consequentially, the MSSP is better equipped to complete the security operations with greater assurances that they will have the intended effect and will have minimal disruption to the enterprise's business.

Quantifying MSSP Affordability

In this section we will assign reasonable costs to the two security service delivery elements where a MSSP model saves over enterprise in-house management. From this assignment, a comprehensive accounting of the costs enterprises encounter in managing their security in-house is presented. However, due to enterprises' varied circumstances (e.g., network size and complexity, local personnel costs, regulatory and industry requirements, protection quality sought, and technologies deployed), there is no universal cost equation. Nevertheless, the size and scale of these costs illustrated below plus the higher level of risk avoidance a MSSP provides strongly supports the argument that a MSSP engagement is very compelling from both economic and reliability perspectives.

The following table lists the costs an enterprise would incur in-house for the same functions that a MSSP has a cost advantage through sharing resources over multiple customers and economies of scale. Since many of these functions require security technicians time, we expressed those cost based on a Full-Time Equivalent cost of $136,000 annually. Please note, we also expressed some functions based on an hourly rate of $65. In doing so, an implicit assumption is made that the security technician is already employed AND available; an assumption that is frequently not met.

Elements of Security Delivery	Cost Descriptions
Security Technicians	Annual salary and benefits of a moderately experienced security manager: $120,000.
	Hiring expenses (advertising, resume reviews, background checks, and interviewing): additional 10% of employee compensation with three years expected tenure.
	Basic training (varies by experience but an essential investment due to the dynamic nature of security threats and technologies): additional 10% of employee compensation.
	Full Time Equivalent cost base of $136,000 annually.
	Size of the organization, diversity of security equipment (technology and vendors), and quality of network protection sought directly impacts size and composition of the security staff. For a bare minimum of security oversight, a ratio of one full-time equivalent (FTE) to every 200 employees is reasonable. As will be described in subsequent cost elements, this cost element escalates quickly.
	Other cost considerations:
	For smaller enterprises where security knowledge is concentrated with fewer, the risk to maintaining a steady state of network protection exists as the result of departures (i.e., one person is the sole keeper of an inordinate amount of knowledge).
	Lacking a career path for security professionals is an indirect contributor to employee churn in this occupation. Consequently, hiring and training expenses rise with churn levels.
Security information	The flow of information from a single piece of security equipment designed to detect anomalous and suspicious traffic can be immense and multiplies in volume

7

Elements of Security Delivery	Cost Descriptions
and event management	with the number of security devices. Collection, filtering, correlation analysis, and event prioritization and alerting are functions that require specialized systems and expertise. Without this investment, the enterprise will not gain the full protection designed into the enterprise's investments in security hardware and software.
	The cost of these systems to conduct what is commonly termed Security Information Management (SIM) and/or Security Event Management (SEM) are significant, easily exceeding $150,000 in the first year of operation and $30,000 annually in subsequent years.
	Personnel costs further add to the complete cost. Dedicated 24 x 7 support requires a minimum of four or more full-time equivalent security technicians with appropriate training for a cost of $578,000 annually. Depending on network complexity, system implementation, and recurring tuning can consume an additional 300 hours for initial set-up and 50 hours monthly thereafter for a cost of $19,500 initially and $3,300 monthly.
Regulatory and industry compliance management	With the rise in mandatory regulatory and industry compliance, enterprises must expand their knowledge base and capabilities to accomplish the following: (1) understand compliance issues thoroughly, (2) measure compliance attainment accurately and continuously, and (3) develop and execute on plans to improve compliance attainment. Because each enterprise and enterprise networks are unique and regulations vary by industry, there is no universal cost figure that can be developed. Nevertheless, consultant engagements directed toward compliance management is becoming more common and entail consultant-level fees, fees that exceed those of a security technicians FTE. In addition, IT consultants that focus exclusively on compliance issues estimate the financial benefits of labor cost savings of compliance management and fine avoidance they provide for a 100-person firm commonly exceed $20,000 annually.
Security device evaluations	In the competitive network security industry and with the evolution of security threats, introductions of new security technologies and products are inevitable. For the enterprises serious about making knowledgeable purchasing decisions, objective testing of new products is recommended. However, objective product testing can add up quickly based on depth and duration of the testing.
	Starting fees from an independent testing lab are approximately $10,000 per week.
Security device implementa-tion	Whenever new security equipment is to be deployed into the enterprise network, security technician's time is required for installation, configuration of the new equipment and potentially other components within the enterprise network, and policy creation. Security staff's knowledge and experience with the security technology and vendor's management system will have a bearing on the time required to successfully complete these tasks. Training may also be required.
	For new security technologies or vendors where additional product training is required, three weeks minimum of dedicated effort is not uncommon resulting in an additional cost of $7,800. This cost includes an underlying assumption that the security technician(s) is available to be relieved from his/her current tasks to dedicate time to learn a new technology and become fluent in a new management system potentially from a new vendor. In addition, the on-going duties of the newly trained security technicians are now expanded unless there are other

Elements of Security Delivery	Cost Descriptions
	technicians available to pick up the old duties. Consequently, new security technologies and/or security vendors could require the enterprise to step-up the size of its security staff and budget at an annual FTE rate of $136,000.
Continuous maintenance and management	Device-level health monitoring, installation of software updates, vulnerability assessments, and testing are essential activities in ensure security equipment is operating at peak effectiveness. Even if conservatively estimated at two hours per month per device, the annual cost per device is $1,600 for maintenance and management assuming all of these activities are completed remotely (no technician visits). Non-remote servicing, equipment sophistication, and diversity of vendor equipment used will cause this per device cost to rise.
Help Desk	The 24 x 7 pervasiveness of an enterprise network requires the same of network security. Consequently, around-the-clock and, for global operating enterprises, multiple language help desk support is essential. For all but the very largest multi-national corporations, staffing such a need is difficult to accomplish efficiently, that is, ensuring all staff members are fully utilized throughout their work assignments. The ability to serve multiple enterprises with the same help desk resources by a MSSP can provide this desirable efficiency. In general, the cost savings in staffing is calculable by comparing the cost of MSSP help desk support to the savings gained in reducing or avoiding increases in enterprise help desk staffing.

Another consideration in this evaluation is the quality and diversity of support. As the enterprises diversify their security vendor and technology selections, the MSSP has the diversity and availability of knowledgeable help desk staff to immediately support this circumstance. As a result, enterprises can minimize help desk staff growth and immediately support the deployment of new security products and technologies. Conversely, inadequate or delayed availability of help desk support negatively impacts an enterprise's efforts to improve its security infrastructure and avoid adverse impact to end-users. |
| **Proficiency** | As previously described operational efficiency and effectiveness are the two components of the higher levels of proficiency a MSSP delivers to enterprises. For the enterprises, the costs savings are visible in:

• Faster completion times of security-related tasks,

• Avoidance of redundant task and/or re-work, and

• Faster time to security improvement and reduction in security vulnerabilities.

Cost assignment to the first two is fairly straightforward. The third, however, is not due to the differences enterprises associate with the value of security and the unpredictability on the impact of an attack or intrusion that is now blocked through improved security.

With the faster completion times of a MSSP, the enterprise would need to increase security staff levels, training, and processes in an attempt to replicate the MSSP time efficiency. In general terms, a one-for-one relationship can be used. That is, to reduce completing times by a certain percentage, say 20%, would require a similar increase in in-house security expenditures. In addition, if the enterprises need for |

Elements of Security Delivery	Cost Descriptions
	faster completion times is more associated with specific projects than a permanent overall improvement, leveraging the immediate availability of a MSSP's more extensive resource base results in an even more economical approach.
	Re-work of security tasks (e.g., remediation of a second occurrence of a worm infection or re-installing a software update) can quickly consume existing security staff time and reduce concentration on other activities the staff is required to address. In addition, the closing of security vulnerabilities is delayed. Similar to efficiency, the cost calculation is similar. If the enterprise has a 10% level of re-work with its security tasks, 10% additional resources are required versus employment of a MSSP.

Economic Crossover to Outsourcing Security

Because enterprise network and security situations differ widely, there is no single method to compare the cost of outsourcing to in-house management. However, by comparing the number of security devices the enterprise's in-house staff can manage versus the number a MSSP would manage for the same annual expense provides an effective test on whether a MSSP engagement is worth pursuing.[1] Essentially, if the number of security devices that the in-house staff can **effectively** manage is less than the cost to outsource, a MSSP engagement is worthy of a serious evaluation. As the tables below demonstrate for firewalls and IDS/IPS devices, an enterprise in-house security staff would need to be highly proficient to manage as many of their enterprise's security devices as effectively as a MSSP.

Dynamic Firewalls (five or more rule changes in a month)

Number of enterprise firewalls	Number of firewalls a full time in-house security technician or two half time technicians would need to manage to be cost equivalent to a MSSP engagement	
	Full time responsibility	**Half time responsibility**
1 – 5	11	5 - 6
6 – 20	14	7
21 – 100	17	8 - 9
Over 100	23	11 - 12

A similar comparison can be produced for the management of IDS/IPS devices. An important distinction between IDS/IPS and firewall management is that IDS/IPS devices capture and report data on potentially threatening network traffic. Conversely, firewalls report a considerably smaller range of data related to threatening traffic that was blocked. Therefore, managing IDS/IPS devices is a highly data intensive activity that requires both device/policy tuning to filter out spurious data and expert evaluation of the remaining data to determine the next course of action (e.g., policy change). Consequently, the attention to

---

[1] Comparison based on a full-time equivalent expense for an in-house security technician of $136,000.

managing IDS/IPS devices regardless of whether this activity is done with in-house staff or through a MSSP is higher on a per device basis than managing firewalls. The comparison shown in the table below reflects this dynamic.

IDS/IPS Devices

Number of enterprise firewalls	Number of firewalls a full time in-house security technician or two half time technicians would need to manage to be cost equivalent to a MSSP engagement	
	Full-time responsibility	Half-time responsibility
1 – 5	9	4 - 5
6 – 20	12	6
21 – 100	15	7 - 8
Over 100	19	9 - 10

It should be noted, that the charts above assume that all the firewalls are all of similar manufacture. However, as mentioned earlier, most large environments are heterogeneous. The different technologies in such an environment require even greater head count and training in order to maintain sufficient expertise. One last point regarding this cost comparison is that it is only a baseline comparison reflecting only a portion of the cost elements of security delivery – just the cost of security technicians. The costs associated with the other elements of security delivery outlined in the previous report section are not fully captured.

Why to Select VeriSign as Your MSSP

Selecting the right MSSP is a critical decision for any enterprise. This criticality stems from the strategic tasks entrusted to the MSSP, which are: (1) helping to protect the enterprise network and stored information, and (2) advising the enterprise on when and how to alter its security infrastructure (e.g., policies and technologies). This first task is straightforward; MSSPs represent an alternative to in-house security for the two overarching reasons outlined earlier in this report – affordability and proficiency. Additional context, however, is necessary to fully appreciate the second.

For the vast majority of enterprises, MSSP engagements demand collaboration with the enterprise security organization. It is unlikely that any enterprise will completely relinquish total responsibility for securing its network to a third party. Intuitively, the enterprise's security organization has a primary responsibility to the enterprise of maintaining a balance between the cost and restrictions network protection entails and advancing business objectives that are tied to the use of the enterprise network resources. Therefore, proactive, reliable, and prioritized advice from the MSSP on when and how the enterprise should alter its security infrastructure is an invaluable tool in maintaining this balance. Without high-quality advice, excessive and/or untimely expenditures on security and unnecessary user disruption and inconvenience in use of network resources can occur.

To effectively address both of these strategic tasks, MSSPs need to score high in the attributes of visibility, experience, and dedication. VeriSign, as described below, is well positioned in all three.

- **Extensive Visibility Matched with Intelligent Data Processing** – Network security is a data intensive operation with relevant flows of information emanating from several sources. Broad visibility into a range of information sources with systematic processes to filter, correlate, and analyze is essential for a MSSP to advise its customers effectively on emerging threats and the ability of their security infrastructure to combat them. As a pioneer and major provider of DNS (processing 128 billion queries daily), VeriSign has around-the-clock access to sources of *state of the Internet* information that are unavailable to other MSSPs. In addition, VeriSign gathers event information from all its managed security services customers (750 million events daily) collected on-site through VeriSign's non-intrusive Security Defense Appliances. To translate this vast amount of data into useful and actionable information, VeriSign has multiple resources employed to continuously assess, report, and advise. Beyond the significant security expertise within VeriSign, the company also relies on best of breed tools. These include the TeraGuard architecture, and three critical components, the Security Defense Appliance deployed on the customer premise, VeriSign Correlation, and the MSS Customer Portal. The VeriSign Correlation Engine operates as a clearinghouse for conducting more detailed analysis across all the information sources. Output from the Correlation Engine is customized and presented through a Web portal to VeriSign's customers from which they can better understand and drill-down on the security state of the Internet and their network. Combined with VeriSign's in-house security experts, prioritized and detailed alerts and security recommendations are developed for each enterprise customer.

- **Experience at Multiple Levels** – Time, resources, and breath of security technology and vendor coverage are all attributes in an assessment of a MSSP's experience level and ability to serve a diverse range of enterprises. VeriSign is not a new provider of managed security services; the company has been provider directly, not as a minor sideline business, for five years. VeriSign's customer base reflects this experience. The company serves companies of all sizes (from the largest enterprises in the world to local credit unions) in the most demanding security-conscious environments such as federal agencies, financial institutions, health-care organizations, telecommunications carriers, and online retailers.

  In addition to the company's extensive information sources and systems, VeriSign has a strong organization of hundreds of security professionals and five security operation centers to serve its growing base of more than 800 managed security services customers. To gain a perspective on VeriSign's seasoned professionalism, 100% of the company's security consultants have earned some level of security industry accreditations (including Certified Information Systems Security Professional distinction) and 90% have three or more industry certifications and average ten years of experience in enterprise information security.

  Last, to serve the vendor heterogeneous networks of enterprises, in-depth knowledge and support of leading security device vendors is essential. VeriSign has significant

experience supporting market leading security technologies and products from Check Point, Cisco, Enterasys, ISS, Juniper, and Secure Computing and can provide objective advice to its customers on which to deploy in their networks.

- **Dedication and Stability** – A decision on which MSSP provider to select is a decision to be made for the long-term. Oscillating between a MSSP engagement and in-house staff or switching from one MSSP to another result in cost inefficiencies driven by transaction costs, disruption to the natural benefit flow of a continuous professional relationship, and reduction in network protection can occur. Therefore, enterprises should gather various indictors of MSSP dedication level. Investments in systems and security personnel are two indicators. Another is involvement in the security industry, which VeriSign is very active in standards formation (e.g., Open Authentication) and in sharing its knowledge and insights at industry conferences. Customer retention and contract expansion are other important indicators as they provide tangible evidence of enterprise satisfaction with past service and confidence that the MSSP will deliver same if not better service in the new contract period. VeriSign's customer retention level among large, stable enterprises (not involved in a merger and acquisition, or a business failure) is nearly 100%. Last, financial stability is important as it can point to ability to continue to maintain and improve the systems and personnel to support customers. As of October 2005, VeriSign had a market value of $1.2 billion and is a diversified, publicly traded provider of critical infrastructure services for the Internet and telecommunications networks. Noteworthy company attributes include: more than 4,000 enterprise customers, 93% of Fortune 500 companies use VeriSign SSL certificates, and VeriSign's DNS registry service, which currently includes over 40 million domain names, highlights the company's attention to dependability with 100% uptime over a ten year period. From a financial perspective, the company's performance as measured by revenue, operating income, and net income has shown solid growth in 2004 and 2005. In addition, VeriSign is not saddled with onerous debt levels. Consequently, profitability and low debt levels contribute to company-level flexibility in making continuous investments to better serve its customers and strengthen its competitiveness in the security industry.

Conclusion

In this study, we detailed how managed security services deliver a combination of affordability and proficiency to enterprises. Those reasons notwithstanding, enterprise adoption of managed security services does vary. Even so, enterprises that have adopted a managed security service approach share one to several common attributes in which they rate moderate to high. Those attributes include the following:

- ✓ Network geographic reach and complexity,
- ✓ Sensitivity of information stored and accessed,
- ✓ Dynamic nature of your network, user communities, and applications,
- ✓ Openness of your network to extranet partners and customers,
- ✓ Diversity of security technologies and vendor products deployed or in need of being deployed, and

13

✓ Regulatory and industry compliance requirements, current or upcoming.

In addition, the following catalysts stimulate enterprise consideration of outsourcing security and developing a MSSP relationship:

✓ Recently suffered a damaging attack,

✓ Seeking to manage security expenditures more effectively,

✓ Hiring and retaining qualified security staff has been problematic,

✓ Need to heighten protection levels in a short period, and

✓ Inherited a network that lacks a recently completed in-depth security vulnerability assessment.

If any or all of these attributes apply to your enterprise moderately or highly or one or more of the catalyst reflect your situation, then the next logic step is to evaluate MSSPs to determine which is the best fit for your needs. As outlined in the previous section, VeriSign has the qualities of a premier MSSP and worthy of your consideration.

Michael Suby
Research Program Manager
Stratecast Partners (a division of Frost & Sullivan)
msuby@stratecast.com