Managed Network Security Services in the Cloud

Dr. N.K. Joshi
Director,
Modi Institute of Management & Technology, Kota

Kamal Kulshreshtha
Associate Professor, Dept. of Computer Applications,
Modi Institute of Management & Technology, Kota

***Abstract* - Traditionally, the local area network (LAN) was viewed as a trusted network. Perimeter protection came in the form of a corporate firewall that was viewed as the cornerstone of protection from a threat that was deemed to be largely external. A growing number of organizations are partially or completely outsourcing the security management function to third parties, typically known as Managed Security Service Providers (MSSPs). Managed Security Service Provider (MSSP) networks are a form of collaboration where several firms share resources such as diagnostics, prevention tools, and policies to provide security for their computer networks. While decisions to outsource security operations of an organization may seem counterintuitive, there are potential benefits from joining a MSSP network due to pooling of risk and access to more security-enabling resources and expertise. We provide structural results that explain the reasons for firms to join a MSSP network. We also characterize the growth of MSSP network size under different forms of ownership. This illustrate the need for initial investment in MSSP networks to overcome initial stalling effect and illustrate that while need for initial investment may increase the optimal network size.**

Keywords- Information security, Managed security services, Managed security services provider, Outsourcing, Network Effects, Network growth, Network ownership structure, Distributed denial of service, Risk management

I. INTRODUCTION

A growing number of organizations are partially or completely outsourcing the security management function to third parties, typically known as Managed Security Service Providers (MSSPs). They engage MSSPs due to increasingly sophisticated threats, cost pressures, and absence of internal expertise. The services that MSSPs provide present additional risks ORGANIZATIONs are required to manage.

Traditionally, the local area network (LAN) was viewed as a trusted network. Perimeter protection came in the form of a corporate firewall that was viewed as the cornerstone of protection from a threat that was deemed to be largely external. Coupled with an ever-increasing web presence, many businesses have seen the need to implement some form of intrusion detection to protect vital information assets, as well as their reputation. The proliferation of virtual private networks or VPNs resulted in an easy method of bypassing this protection.

The purpose of this is to identify the risks associated with the MSSP engagement and offer guidance to assist organizations in mitigating these risks. Organizations should pay particular attention to risk management issues that are heightened when serviced by MSSPs.

This concept can be vividly illustrated in the enterprise network domain. To improve responsiveness and build stronger customer relationships, most organizations have opened their networks to direct access by remote employees, business partners, customers and other third parties. The resulting porosity of the network perimeter has created ample opportunity for security threats to penetrate the innermost regions of the enterprise, exposing vital IT resources to damage and destruction.

Furthermore, as organizations have become more reliant on external Internet connectivity for day-to-day business affairs, they are susceptible to considerable financial loss when that connectivity is reduced or lost. Distributed denial of service (DDoS) attacks or worm outbreaks that affect network infrastructure for any length of time can have potentially devastating results on the business.

Outsourcing of technology-related services may improve quality, reduce costs, strengthen controls, and achieve any of the objectives listed previously. Ultimately, the decision to outsource should fit into the institution's overall strategic plan and corporate objectives.

The time and resources devoted to managing outsourcing relationships should be based on the risk the relationship presents to the institution. Risk management is the process of identifying, measuring, monitoring, and managing risk. Risk exists whether the institution maintains information and technology services internally or elects to outsource them. Regardless of which alternative they choose, management is responsible for managing risk in all outsourcing relationships. Accordingly, institutions should establish and maintain an effective risk management process for initiating and overseeing all outsourced operations.

To combat the ever-escalating danger posed by network security threats, forward-thinking organizations have two options: invest significantly in the people, processes and technology required to maintain world-class, 24/7 network security operations, or outsource the function to the growing number of highly effective managed security services providers (MSSPs).

In computing, managed security services (MSS) are network security services that have been outsourced to a service provider. A company providing such a service is a managed security service provider (MSSP) also Managed security services (MSS) is a systematic approach to managing an organization's security needs. The services

may be conducted in house or outsourced to a service provider that oversees other companies' network and information system security. Functions of a managed security service include round-the-clock monitoring and management of intrusion detection systems and firewalls, overseeing patch management and upgrades, performing security assessments and security audits, and responding to emergencies. There are products available from a number of vendors to help organize and guide the procedures involved. This diverts the burden of performing the chores manually, which can be considerable, away from administrators.

Following are some of the many types of security-related services offered by MSSPs:

- *Network Boundary Protection*

Using technology such as firewalls and virtual private networks (VPNs), the MSSP protects the organization's network perimeter. The MSSP should provide device monitoring of connections to external third parties such as Internet Service Providers.

- *Management of Intrusion Detection and Prevention for Networks and Hosts*

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are automated services that can detect patterns in network traffic and may take action according to a rule set or pattern definition database.

- *Event Log Management and Alerting*

Event log management and alerting is conducted to monitor event logs generated by network devices or computer systems to centralize, filter, and provide management reports on material activity. Alerts can be set for highly sensitive events or activities.

- *Anti-virus and Web Content Filtering Services*

Managed antivirus protection provides organizations with malware protection that helps safeguard ORGANIZATIONs from new threats. The malware definitions are updated frequently to help recognize the new threats.

- *Patch Management and Security Software Management*

MSSPs can identify and manage network security related software systems and components requiring regular security updates; conduct compatibility testing before deployment; deploy the updates uniformly; and provide reporting on the status and effectiveness of the security software as implemented.

- *Security Incident Response and Management*

MSSPs can assist an organization in building an incident response team or providing a turnkey incident response in the event of a breach.

- *Data Leak Prevention*

MSSPs can help identify all methods of data ingress and egress, and establish systems that monitor and enforce appropriate controls.

- *Secure Messaging*

MSSPs can provide services to ensure the security of messages into and out of the organization.

- *Information Security Consulting Services*

Security consulting by MSSPs may include risk assessment, vulnerability assessment testing, penetration testing, compliance tools, education and training, and attestation services.

II. NETWORK OUTSOURCING IS THE SECTOR'S FASTEST-GROWING SEGMENT

For an expanding range of IT functions, outsourcing has become the strategic direction of choice, allowing companies to focus more on business opportunity and less on risk. The combined infrastructure outsourcing segments (data center, desktop and network outsourcing) equal more than 80 percent of total IT outsourcing spending. Network outsourcing remains the fastest-growing segment, with an 12.5 percent CAGR between 2011 and 2013. Dollar-wise, the network outsourcing market has been projected to reach a value of $600 billion by 2014, according to Gartner analysts. Network security is a rapidly growing outsourcing category.

It comprises two major types of service provider offerings:

III. MANAGED SERVICES "IN CLOUD"

Remotely managed and monitored security services that do not depend on customer premises equipment (CPE); the "cloud" represents the telecommunications providers' network. In the cloud services can replace or augment CPE devices to block ports and protocols or to remove spam or viruses from network traffic.

In this managed service can uniquely offer "clean bandwidth" that has been purged of security threats such as DDoS attacks, worms, viruses, botnets and other malware.

The managed security services (MSS) market of cloud-based services will grow by 67% in 2014 and is expected to reach $1200 million by 2015… Cloud-based services offer the best protection against distributed denial of service (DoS) attacks, which are also the most prevalent internet-originated type of attack."

IV. CPE-BASED MANAGED SERVICES

A security offering for which the provider remotely manages the customers' on-premise equipment, located at

the network's edge, and assumes responsibility for associated aspects of network security.

Both network-based and edge-based security technologies can co-exist. Both these are required to holistically and comprehensively address security threats. The most security-conscious organizations are also supplementing their edge-based security infrastructure with in-the-cloud managed network security services, providing for extra protection.

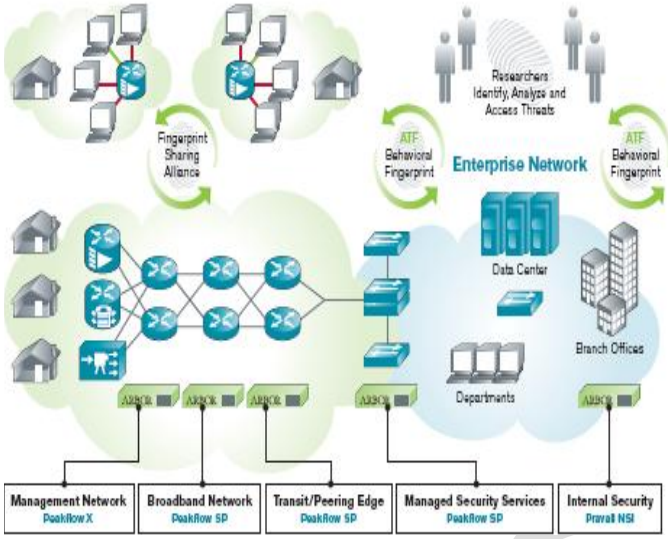

Figure 1: MSSP Deployment Core-to-Core

V. MSSPS EFFECTIVELY ADDRESS USHROOMING SECURITY CHALLENGES

As networks themselves grow larger and more complex, outsourced security services from MSSPs are attractive for several reasons.

- The costs of improving from computer crime continue to escalate. For example, based on the findings of its annual computer security survey, the U.S. FBI estimated that computer crime cost U.S. businesses $500 billion in 2013. Sixty-four percent of the 2,066 organizations surveyed suffered a financial loss from computer security incidents. They spent nearly $15 million to deal with virus-type incidents and $9 million on network intrusions.
- Security threats are non-stop and only increase in frequency and malice.
- Some threats can only be addressed in-the-cloud by providers. These include DDoS attacks and botnets, which flood up stream links to enterprises. And they can only be resolved in-the-cloud and not at the enterprise edge.

Because service providers own and manage the network infrastructure, they are uniquely positioned to offer in-the-cloud security services.

Cloud-based security services can reduce the number of low-level attacks and enable an enterprise to improve the performance of web-based commerce while focusing its efforts on mitigating more serious security threats.

- MSSPs provide far greater capabilities, more efficiently, than a single enterprise can. The benefits of network outsourcing are well-established-lower costs, reduced complexity in the customer enterprise, technology scalability, broad capabilities and risk off-load-and certainly apply to in-the-cloud managed security services.

VI. THE INDUSTRY'S CHOICE FOR IN-THE-CLOUD MANAGED SECURITY

Hardware manufacturing companies offer a unique approach to helping service providers maximize the business value they deliver to enterprise customers with the MSS hardware, a market-proven solution for providing security to the core and performance to the edge. MSS hardware is deployed in the backbones of every major service provider and multi-service operator (MSO) network around the globe.

VII. THE BUSINESS CASE FOR IN-THE-CLOUD MANAGED NETWORK SECURITY

Outsourced network security services are already a popular choice for enterprises around the world. According to the 2013 Global Security Survey conducted by CXO Media and PricewaterhouseCoopers, participating enterprises are already outsourcing key activities.

These key activities include:

- Firewall monitoring: 32%
- Vulnerability scanning: 26%
- Network firewalls: 24%
- Intrusion detection: 18%
- Network security monitoring: 16%
- Security event monitoring: 15%
- Rogue technology detection: 7%

Figure 2: Key activities Included in managed security services.

Clearly, there is significant opportunity for enterprises to reap the benefits of outsourced detection of rogue

technology (worms, viruses, botnets, etc.), which in-the-cloud services from MSSPs essentially provide.

As more and more enterprises transition from in-house monitoring and management of network-based threats, they will find many service providers delivering network-based managed service offerings built on MSS hardware. These service offerings provide fully scalable, proactive detection and mitigation capabilities to respond to attacks before they impact enterprise networks.

VII. THE BENEFITS OF IN-THE-CLOUD MANAGED SECURITY SERVICES

When enterprises choose in-the-cloud managed security services from providers such as those listed above, they can expect to receive numerous significant benefits, such as:

- Cost savings in many areas of operational and capital expenditure. This encompasses labor, equipment and software, facilities and other infrastructure costs. By leveraging the resources available from MSSP providers, enterprises are able to concentrate their valuable resources on core competencies.
- Improved performance of network resources, as in-the-cloud managed services deliver greater network reliability and integrity. As a result, QoS improves, and enterprises can more consistently meet internal service level agreements (SLAs).
- Higher levels of network security, which, in addition to enabling better network performance. This builds a greater sense of security and trust among all users.
- Managed DoS Services Expertise in a complex and constantly changing domain. MSSPs have the critical mass of resources to invest in in-the-cloud security services, focusing large amounts of human and monetary capital to develop world-class offerings. Through this process, providers gain extraordinary levels of security knowledge, leveraging cumulative learning to enhance the economies of scale gained from serving many enterprise customers.

Figure 3: Services offered/provided By MSSP.

Finally, the growing popularity of outsourced network security services has helped the MSSP industry as a whole to mature quickly. Providers have addressed issues that may be cause for concern. They have:

- Overcome a history of service delivery failures at certain high-profile security service providers
- Dealt with today's regulatory environment, which requires greater levels of due diligence
- Built customer confidence in their service delivery to assuage concerns over loss of control
- Used the proper processes and technology to ensure the utmost confidentiality, as customers routinely send proprietary network information outside the enterprise

XI. CONCLUSION

From its origins in relatively peripheral operations such as data center management, outsourcing has arguably become the enterprise IT industry's most profound trend of the last decade, moving up the "food chain" to highly mission-critical activities such as network security. Managed security services represent growing revenue. Most MSSP operate in multivendor environment.

In this paper we examine the economic rationale for MSSP networks, i.e., to provide an economic rationale for why firms may choose to outsource security.

Outsourcing, particularly the outsourcing of high-risk network security monitoring and threat mitigation, offers enterprises a solid roster of business benefits:

- Cost savings in many areas of operational and capital expenditure
- Improved performance of network resources, as in-the-cloud managed network solutions deliver greater network reliability and integrity
- Higher levels of network security, as significantly more resources are dedicated to an enterprise's needs
- Expertise in a complex and constantly changing domain

The hardware solutions are the choice for MSSPs and their customers who want to ensure security to the core and performance to the edge. Managed security offerings are among the industry's most powerful and present a strong complement to the internal network security capabilities. It delivers market-leading performance in a wide range of security services, from network-based DDoS detection and mitigation to worm detection and reporting. When customers can outsource not only their network security activities, but associated risk and anxiety as well, creating a true silver lining in the stormy world of enterprise network management.

Organization's challenges in dealing with high profile network security breaches, changing technology, malware, system maintenance costs, complexity, and uncertainty surrounding network security have resulted in an increased use of MSSPs. In addition, organizations can have high levels of risk exposure in the event that an MSSP cannot comply with service level agreements.

Confidentiality agreements should be drafted with MSSPs. From the time that discussions are first initiated, the MSSP is privy to confidential information that should not be disclosed. Drafting such an agreement ensures that both parties will arrive at acceptable solutions to security concerns.

REFERENCES

[1] Gartner Group, "Information Security in an E-Business World: Coping With the Threats."
[2] As cited in "Networks move out," Infoconomy.
[3] Business Benefits for Service Providers and Enterprises by Arbor Networks, Inc.
[4] Allen, J., D. Gabbard, C. May, "Outsourcing Managed Security Services".
[5] Bensen, S.M. and J. Farrell, "Choosing How to Compete: Strategies and Tactics in Standardization", Journal of Economic Perspectives.
[6] Definition adapted from "'In the Cloud' Security Services Will Change Providers' Landscape," Kelly M. Kav anagh, et al, Gartner
[7] Camp, L.J., and C. Wolfram, "Pricing Security", CERT Information Survivability Workshop, Boston.
[8] Campbell, K., L. Gordon, M. Loeb, L. Zhou "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", Journal of Computer Security.
[9] "Managed Security Service Market Continues Strong Growth," Yankee Group, Andy Efstathiou.
[10] Carbal, L. M., D. J. Salant, G. A. Woroch, "Monopoly Pricing with Network Externalities," International Journal of Industrial Organization, 199-214.
[11] Cavusoglu, H., B. Mishra, S. Raghunathan "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", Int. Journal of Electronic Commerce, 70-104.
[12] Computerwire, news reports (online database).
[13] Cowen, Tyler, "Public Goods and Externalities". The Concise Encyclopedia of Economics.
[14] Dejesus, Edmund X. "Managing Managed Security". http://www.infosecuritymag.com/articles/january01/cover.shtml
[15] Gaspar, Suzanne. "Security Concerns Dominate NW500 Survey. " http://www.nwfusion.com/research/2001/0507feat2.html?&_ref=650835007
[16] Davidson, Stephanie and Friedman, Rich. "Special Report: Outsourcing Update." http://www.itworld.com/Career/1875/ITW0228outsourrcing/
[17] Messmer, Ellen and Pappalardo, Denise. "Demise of Pilot Seen As Blow To Outsourcing." http://www.nwfusion.com/news/2001/0507pilotcrash.html
[18] IBM Managed Security Service Provider, http://www-935.ibm.com/services/in/en/it-services/managed-security-services.html.
[19] http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/appendix-d-managed-security-service-providers.aspx
[20] http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf