The Extended Enterprise: Manage Complexity, Cost and Compliance

Adapted from Worldwide and U.S. Security Services 2009-2012 Forecast and Analysis: Economic Crisis Impact Update by Irida Xheneti, IDC #216111

Introduction

Today’s business operating environment across all industries has become a challenging and competitive arena. As organizations strive to grow and capture market share, they use a variety of business models and solutions to successfully achieve their business objectives. For example, organizations add more employees or expand their partner and supplier ecosystem as well as their customer base. They also rely on technology advancement to enable their business to run more efficiently and more securely to increase the productivity of their employees and enable more efficient collaboration with partners, suppliers, and customers.

As the technology arena evolves with the introduction of mobile devices, IP communication, wireless networks, virtualization, cloud computing and green IT initiatives, and many other technologies, organizations are looking for cost-efficient means to deploy, integrate, and manage these technologies securely. While an open IT infrastructure and innovative technologies enable companies to increase productivity and revenue, they also open the door to a plethora of security threats and vulnerabilities, business disruption, and security infrastructure challenges such as data breaches, data loss, noncompliance, decreased customer confidence, and many more. The threat landscape becomes more complex, especially during a downturn in the economy, when security breaches increase while organizations look to cut costs and remain secure and compliant with industry regulations. Furthermore, internal and external pressures continue to rise as a result of the high stakes between new technology investments and the risk that security threats pose to organizations.

To address these security concerns, organizations require a proactive risk management strategy that enables them to identify and prioritize the most critical assets that need to be secured and allows them to verify that proprietary data is not leaving the network perimeter. In addition, organizations need a secure and cost-effective way to manage their networks, systems, and applications, as well as their information assets, while staying focused on their primary business. Furthermore, security processes require constant review as well as policy enforcement, given the volume and severity of external threats such as viruses, spam, denial of services, and internal threats such as data leakage and new emerging vulnerabilities from the deployment of new technologies.
Given these dynamics, organizations are constantly under internal and external pressures to manage the complexities of their IT infrastructure, reduce cost and ensure the integrity and security of their IT infrastructure, and meet compliance regulations while remaining competitive in a difficult economic environment. These responsibilities certainly make for a daunting task—especially when there is a lack of in-house IT security expertise and the cost of hiring the talent to perform these tasks becomes outrageously expensive—and they are not the best use of internal resources for both small and large organizations. Ultimately, as these costs increase, managed security services allow an organization to focus on its primary business and outsource security management to a trusted service provider.

This Executive Brief examines the challenges organizations face in terms of security and discusses how organizations can deploy managed security services to alleviate those challenges.

**Managed security services: To outsource or not to outsource security operations—that is the question**

Among the many critical challenges that IT executives face, enterprise security has always given many pause. Not long ago, major threats to confidential information and the IT infrastructure consisted of an occasional virus, worm, or a clever intruder, and it was relatively easy to check off the enterprise security box and continue further down the list. However, today's threats and vulnerabilities have been transformed into sophisticated silent attacks with much higher business stakes. Given this evolving threat and business landscape, the inevitable question arises: Can an organization manage IT security on its own? Not surprisingly, many organizations have responded "no" and are turning to security service providers that offer the security management expertise and sophisticated protection needed for today’s enterprise environments. The main benefits associated with outsourcing security management to a security service provider are as follows:

- **Manage security complexity.** Enterprises and end users worldwide are continuously deploying new technologies, utilizing Web applications, and transforming their IT infrastructure to improve business operations, reduce costs, and increase revenue. While virtualized environments, Web applications, mobility, VoIP, and green IT initiatives have demonstrated significant cost savings and increased efficiency, they have also called for an integrated and proactive approach to security management. This IT transformation has brought significant benefits to the enterprise, but it has also increased the opportunities for information security vulnerabilities and threats, identity and access management loopholes, and compliance violations. To proactively handle the complexities associated with the management of IT
security, organizations can better focus on their core business by strategically outsourcing key security management functions to a trusted security service provider. This approach will enable organizations to primarily focus their internal resources on more strategic projects while leveraging a service provider whose core competency is security.

- **Manage cost.** For many companies, managing cost, especially during an economic downturn such as the one we are facing today, has become a critical priority. With an increase in technology complexity and significant proliferation of security threats and vulnerabilities, organizations are faced with mounting costs to protect their IT infrastructure investments. To do so, they are required to deploy and manage a robust security infrastructure, hire and train security experts, and meet compliance regulations. As a response to this situation, many service providers have developed cost-effective security solutions to enable customers to reduce cost and focus resources on core business while gaining access to security skills and expertise that the organization may lack. The use of third-party services can also enable organizations to improve their internal processes and procedures to meet compliance regulations and manage risk proactively. By strategically outsourcing key security management functions to a service provider, customers will be able to leverage industry best practices, security expertise, and a variety of security technology solutions at a fraction of the cost compared with performing these tasks in-house.

- **Manage compliance requirements.** Government and industry regulation initiatives to protect consumers and enterprises have become more stringent. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA); the Sarbanes-Oxley Act (SOX); the Gramm-Leach-Bliley Act (GLBA); ISO 17799 (now ISO 27002); ITIL; PCI; SB 1386; PIPEDA; the EU Data Protection Directive; and the USA PATRIOT Act, Title III require companies to have in place robust corporate risk management programs to prevent instances of data loss that could expose them to serious legal and financial repercussions. While security service providers cannot guarantee compliance with government regulations, they can assist enterprises in handling policy creation and management, compliance measurements and audits, and reporting in a cost-effective and timely manner.

**Managed security services: An extension of your staff**

Managed security services such as firewall, intrusion detection, and intrusion prevention services provide 24 x 7 monitoring and management solutions. This means that the service provider becomes the customer’s trusted advisor and acts as an extension to the staff to enable the customer to focus on its primary business. Managed security services can also serve as a detection mechanism for
any potential hole within the IT infrastructure. Outsourcing security management functions to a service provider is not just a tactical business decision to managing cost but also a strategic approach to developing the foundation blocks for proactively managing risk and vulnerabilities.

Challenges and Considerations

At a time when organizations are looking to reduce spending and optimize current investments, employing security solutions from a third party to manage both cost and security could have a tremendous impact on the actual business. Organizations that are evaluating third party-type managed security services should consider evaluating which services would be best addressed by a third party. Furthermore, organizations should perform due diligence on a service provider's security operation centers, solutions, and tools, as well as the security products it supports. Lastly, organizations should evaluate a service provider's partner arrangements and SLAs to determine the appropriate service levels. A prime candidate for meeting today's security and business needs is a service provider that provides flexible managed security service solutions and meets agreed-upon SLAs.

Conclusion

Managed security services can help organizations alleviate the cost and complexity of proactively securing the IT infrastructure. As discussed earlier in this paper, the IT infrastructure is constantly being challenged with new and increasingly complex threats and vulnerabilities with severe business impacts. As a consequence, organizations are continually in the process of finding ways to protect their businesses with innovative security products and services that help them not only improve overall security and reduce security overhead but also accomplish these objectives within limited and constrained budgets. Finding an optimum balance between these frequently conflicting goals will enable organizations to run a secure and efficient IT infrastructure while staying focused on their primary business objectives.

Copyright Notice

The analyst opinion, analysis, and research results presented in this IDC Executive Brief are drawn directly from the more detailed studies published in IDC Continuous Intelligence Services. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. Contact IDC Go-to-Market Services at gms@idc.com or the GMS information line at 508-988-7610 to request permission to quote or source IDC or for more
information on IDC Executive Briefs. Visit www.idc.com to learn more about IDC subscription and consulting services or www.idc.com/gms to learn more about IDC Go-to-Market Services.

Copyright 2009 IDC. Reproduction is forbidden unless authorized