WHITE PAPER

symantec.

Managing Enterprise Security

Considerations for in-house security management versus outsourced managed security services

INSIDE

INSIDE

- Measuring the cost of managing security
- Considering security management options
- Benefits of managed security services
- Selecting a managed security services provider

Contents

Executive summary 3

Challenges in the business environment 4

Measuring the cost of managing security 5

- Equipment 5
- Personnel 6
- Facilities 7

Considering security management options 8

- Comparing in-house versus outsourced security management 8
- Example: in-house versus outsourced managed security costs 8

Benefits of managed security services 10

Selecting a managed security services provider 11

- Vendor analysis – staying power 11
- Breadth of services offerings 11
- Organizational support 12
- Recommended MSSP profile 12

Conclusion 13

References 13

Executive Summary

Security is an integral and necessary component of business today, increasingly so due to the expanse of the Internet and the big "E's": e-business, e-commerce, and e-retailing. Security has never been so critical to an enterprise's survival, competitive advantage, and ability to maintain stakeholder value. An effective security program, therefore, is not only about security devices and technology, it must also incorporate people and processes.

At the same time, enterprises face a number of barriers to achieving and maintaining effective security programs. These barriers include:

- Shortage of qualified, skilled security professionals
- Lack of resources and infrastructure to support a 24X7 security program
- Rising complexity of security technology
- Lack of formal training
- Lack of time to focus on persistent security management and operational tasks

As a result, many organizations that manage security in-house are looking for alternatives to overcome these barriers. They require a way to maintain a strong security posture while focusing on core, revenue-generating e-business functions.

Outsourcing security tasks, similar to outsourcing physical security and information technology, is becoming an increasingly attractive option. According to Gartner Dataquest, managed security services, defined as outsourced management and monitoring of security systems, is the fastest growing segment of the information security services market. "Managed Security Services Providers (MSSPs) use high-availability security operation centers (either from their own facilities or from data center providers) to support 24X7 services designed to reduce the number of operational security personnel an enterprise must hire, train, and retain to maintain an acceptable security posture."[1]

So, for many organizations, two alternatives have emerged: in-house security management or outsourcing security management, either completely or in part.

The question most organizations have when facing an outsourcing decision is: *Can we effectively outsource or co-source security management functions while still realizing a cost benefit?*

Properly identifying and evaluating the risks and benefits of outsourcing security is a daunting task. Considerable study and extreme care must be given to weighing factors of managed security services providers, such as:

- Staying power of the company
- Expertise of the security professionals
- Range and flexibility of the services
- Cost benefits
- Security philosophy, culture and people
- Commitment to service-level agreements
- Supported technology
- Existence of secure operations facilities

Of these factors, evaluating the cost of outsourcing can be the most challenging because most organizations cannot fully estimate the financial impact of such a decision. In fact, a recent InfoWorld outsourcing study of 100 technology professionals said that 61 percent of organizations did not know how much money their company would save in the next 12 months by outsourcing IT functions.[ii] This is true for most organizations considering outsourcing security services.

This white paper helps organizations calculate the cost for managing security and provides real-life scenarios of cost comparisons to help organizations build a foundation for a financial analysis when considering a managed security services provider. It also discusses benefits of outsourcing security functions and provides guidance companies can use to evaluate potential managed security services providers.

Challenges in the business environment

E-commerce and e-business initiatives inspire companies to move toward an open, distributed network-computing environment. These environments are designed to bring together employees, customers, partners, suppliers, and distributors to exchange and access information critical to conducting business today. Unfortunately, these same networked environments create vulnerabilities that allow disgruntled workers, hackers, and other types of attackers—both internal and external—to wreak havoc on corporate systems through malicious acts of fraud and vandalism. The resulting damage can negatively impact a company's bottom line, tarnish its corporate image, and adversely affect customer trust.

BUSINESSES TODAY FACE THE FOLLOWING CHALLENGES:

There has been a discernable rise in deliberate criminal behavior directed at corporations.

With customers and business partners dependent on accessing critical product and service data via open networks such as the Internet, companies must ensure the integrity of this information or risk jeopardizing their reputation and brand equity. The need to protect the bottom line, as well as the corporate image, drives the demand to effectively manage information security.

An increasingly mobile workforce, telecommuting, and remote computing create special security problems for companies.

Companies are driven not only by the desire to protect their information and physical assets, but also by the need to ensure worker productivity. There is an increasing acceptance of worker mobility and remote computing, but traditional corporate LANs and WANs are insufficient to support this growing off-site work force. As remote access to corporate networks increases, so does the need to protect transmission of information to these remote points.

Security may not be a company's core competence, but it is a core requirement.

Companies focusing on e-commerce and e-business must ensure their information assets are properly protected. Managing information security requires constant vigilance and a strict accounting of every change in the state of the network. It is an enormous undertaking and rarely falls within the core competency of a rapidly growing business's technical staff.

Limited corporate IT resources are needed to support the organization's primary business requirements.

CIOs and corporate technology managers seek support to free operational resources for higher, value-added activities involving core competencies and business strategies. In-house information security specialists have an intimate knowledge of the mission-critical business applications running on the network and the impact these have on both bandwidth and corporate operations. In an ideal world, these talented in-house resources would be most effectively used to plan future network redesigns and migrations to support strategic business initiatives or to implement new applications that focus on areas of greater return-on-investment (ROI) potential.

In-house IT staff lack the resources and expertise to protect valuable information assets.

In-house IT staff may lack the resources to maintain the level of expertise that enables them to differentiate between real and unintentional attacks and consequently may inadvertently expose systems to these vulnerabilities. The result is escalating in-house costs required to ensure workers are trained and stay up to date on the most current technologies and security threats.

Experienced information security professionals are hard to find, expensive to hire, and difficult to retain.

Companies are finding it expensive to recruit and extremely difficult to retain skilled information security talent because of the extremely strong market demand for these professionals. In addition, the high attrition rate among security workers reduces a company's ability to effectively safeguard its valuable information assets.

Measuring the cost of managing security

The total cost of ownership for a security management program includes manpower and supporting hardware, as well as software and equipment to build, upgrade, maintain, operate, and control the systems.

When a company considers outsourcing managed security services, it must estimate several variables over the duration of the managed security services contract:

- All relevant capital and operating costs
- Costs of supervising the managed security services provider
- Likely increases in costs for salaries, benefits, and service contracts
- The "cost of money" and interest costs
- Residual value of equipment and facilities
- Cost of transition, including personnel
- Cost of changes in direction and level of resources
- Cost of contract modifications

To effectively compute the total cost of ownership of in-house security management, a wide range of costs must be considered over a number of years. A company must identify and evaluate both overt and hidden costs. The following sections list many of the costs of a security management program.

EQUIPMENT

Hardware and software costs

For in-house security management, companies must determine the cost of all hardware and software necessary for security management and operations. This includes servers, PCs, and peripheral equipment, as well as all associated operating systems, database, application, and security software. Additional hardware and software required to support the security operations include system and network management tools, help desk systems, integrated management consoles, and knowledge-based management systems and software.

For outsourcing, depending on the MSSP's approach and technology support, the list of supported security technology may be restricted. Some MSSPs will only manage certain security technologies. In some cases, MSSP's require a specific brand of security technology to be purchased or swapped-out for an organization's existing technology. Other MSSPs require additional purchases of specialized or proprietary technology for log file and event stream collection, analysis, and filtering.

License costs

The cost of all software licenses, including patches, incremental updates, and new versions of the software should be calculated over the expected software lifecycle.

Maintenance

Maintenance fees for software and equipment must be factored into the total cost for ownership. Software maintenance is typically 15 to 25 percent of the cost of the software annually. An organization with $1 million in software licenses will pay $150,000 in maintenance costs (on the low end). Companies should be aware of the level of support they receive for that cost. Some managed security services contracts provide 8 or 10 hours of coverage and support, while others deliver 24X7 support.

PERSONNEL

Staffing for information security professionals is perhaps the most crucial, most difficult, and most costly component of an effective security management program. The top market challenge is hiring and retaining a skilled base of security professionals. The cost of staffing includes not just the cost of salaries, but also additional compensation (bonuses, stock incentives, etc.), space and equipment costs, and the cost of ongoing education and training. The salaries of security administrators—and security officers—vary depending on geography and level of skill and expertise. According to a recent survey by InformationWeekresearch.com, average compensation for staff level (not management) information security professionals in the Dallas, Texas area is:

High	Average	Low
$88,375	$71,750	$64,000

If a company has a typical 8 am to 5 pm operations day, but plans to expand to 24X7 security operations, then it must consider staffing multiple shifts of workers to provide coverage 365 days per year:

- Shift 1 for the morning
- Shift 2 for afternoon/evening
- Shift 3 evening/early morning hours
- Shift 4 weekend work and time-off coverage for shifts 1, 2, and 3

Thus, it would take a minimum of four resources to cover one seat in a 24X7 security operation. And these additional resources would need a range of expertise or specialization in different types of security issues.

Recruiting

Due to the high turnover rate in the IT field, organizations may also need to consider the cost of recruiting. Whether internal HR staff or external recruiters are used, the cost of recruiting may average 20 to 30 percent of total annual compensation costs for the position being recruited.

Training and education

Ongoing training and education of security professionals is essential to honing skills and, more importantly, keeping staff current in an ever-changing, fast-paced technology environment. Ongoing education must encompass the latest security tools and technologies, threat techniques, and 75 protection strategies. Costs in this area may include:

- Product or technology training
- Training in general security awareness
- Certification preparation classes
- Certification costs
- Attendance at major security conferences or shows
- Books, magazine subscriptions, journals, or e-learning courses to keep security professionals abreast of the latest technologies, tips, techniques, threats, and safeguards in the industry

It is typical for organizations to provide guidelines on the amount of training an employee receives each year. A minimum of two weeks is frequently provided, but more is often necessary. Most security courses are one week in duration; therefore, each employee would be eligible to attend two security courses per year. Since the cost of courses may range from $1,500 to $3,000, a typical cost per headcount for training would be $5,000 a year.

FACILITIES

Security Operations Center

The cost of building and staffing for 24X7 security operations can be extremely high. It is cost-prohibitive for most organizations to build or lease a security operations center (SOC), as building or leasing space in a network/security operations center can exceed $100 million in capital expenditure.[iii] If existing space is already established or available for security management and monitoring, the build-out cost for a reasonably sized security operations center, perhaps 30 seats, will be upwards of $1 million. When added to required equipment, redundancy, power, HVAC, and fire suppression systems for high-availability, redundant operations, the cost can be prohibitive for many organizations.

Considering security management options

COMPARING IN-HOUSE VERSUS OUTSOURCED SECURITY MANAGEMENT

Given the challenges of the business environment and the market, it is no surprise that organizations are looking for alternatives. Beyond pure cost, there are a number of advantages a company receives by the very nature of a professionally managed service contract with a team of dedicated, experienced security professionals. Partnering with an experienced, well-established, professionally managed security services provider decreases the risk of cyber threats. Greater levels of protection, 24X7 diligence, and a strengthened security posture may benefit an organization the most. Some advantages are highlighted in the table below.

	Traditional Software License	Managed Security Services Provider
Entry cost	High	Low
Installation and implementation	Requires in-house resources	MSSP handles implementation
Time to value	Long	Short
Skilled resources	Company must hire, train, and retain talent	MSS provides skilled resources
Security risk	Company must assume all risks	MSS partner shares operations risks
Efficiency and effectiveness	Limited scalability prohibits efficiency and effectiveness	Greater efficiencies via scalability (1:many) is inherent in SOC operations
Security posture	Dependent on skill, processes, and expertise of internal staff	Improved by diligence, guaranteed response times, security vulnerability research, and cumulative expertise of MSS team
Response	Dependent on skill, processes, and expertise of internal staff	24x7 protection, critical alert notification and levels of response per severity

EXAMPLE: IN-HOUSE VERSUS OUTSOURCED MANAGED SECURITY COSTS

When considering the expenses and cost associated with in-house versus outsourced security management over a two-year program for a mid-sized company,[iv] the benefits and cost savings of a multi-year managed service contract should be considered in totality. In some cases, the first year's savings may be considerably higher when compared to subsequent years, as security requirements evolve and change.

COMPANY PROFILE Sand Pharmaceuticals is a pioneer and world leader in discovering new treatments for debilitating diseases and medical conditions. The company employs 3,000 personnel and has an IT staff of 40, with five dedicated to managing information security. Sand Pharmaceuticals has implemented firewalls and is now deploying intrusion detection system (IDS) technology. For maximum protection of the company, its security staff has deployed three firewalls and also needs network-based IDS for six network segments, and host-based IDS 24X7 on 10 critical servers in the enterprise.

The following table illustrates a company's costs for two in-house scenarios (one daytime and one 24X7 security operations) versus one outsourced scenario.

Year 1	In-house 8:00–5:00 (5 staff)	In-house 24X7 operations (15 staff)	Outsourced MSS Solution
Resources			
Salaries[1]	$501,000	$1,503,000	N/A
Training[2]	$25,000	$75,000	N/A
Recruiting[3]	$37,575	$288,075	N/A
Equipment			
Software[4]	$81,875	$81,875	$81,875
Maintenance[5]	$12,281	$12,281	$12,281
Implementation and Setup[6]	Cost varies	Cost varies	$23,960
Management	N/A	N/A	$348,000
Total	$657,731 + set-up	$1,960,231 + set-up	$466,116

Assuming the company keeps its 5 daytime IT staff for mission-essential in-house security support, first-year savings for outsourcing 24X7 security operations is approximately $836,384.

Year 2	In-house 8:00–5:00 (5 staff)	In-house 24X7 operations (15 staff)	Outsourced MSS Solution Resources
Resources			
Salaries[7]	$546,090	$1,638,270	N/A
Training	$25,000	$75,000	N/A
Recruiting[8]	$40,957	$112,870	N/A
Equipment			
Maintenance	$12,281	$12,281	$12,281
Management	N/A	N/A	$348,000
Total	$624,328	$1,838,421	$360,281

Again assuming the company keeps its 5 daytime IT staff for mission-essential in-house security support, second-year savings for outsourcing 24X7 security operations is about $853,812.

[1] Based on InformationWeek Salary Advisor. Mean high total compensation (including salary, stock options, and bonuses) of typical security professional in Houston, TX. Salaries of typical security professionals in Houston, TX. Salaries include four staff ($88,375) and one manager ($147,500).
[2] Training cost estimated at $5,000 per employee based on two classes per year at industry standard prices for security training courses.
[3] This scenario assumes the company already has the five daytime positions on staff. It also assumes a conservative 30 percent annual turnover rate for security personnel. To plus up for 24x7 in-house operations, first-year recruiting costs are high because, in addition to the 30 percent turnover of the original five positions, 10 new positions are necessary. Recruiting cost is based on 25 percent cost of total annual compensation for in-house security professionals.
[4] Software cost based on three unlimited user licenses for Symantec Enterprise Firewall/VPN, Symantec NetProwler IDS licenses for six network segments, and Symantec Intruder Alert host IDS licenses for 10 servers.
[5] Maintenance cost based on 15 percent of software license cost.
[6] Setup cost includes implementation and setup services for remote management and ongoing maintenance for software. Without MSSP, implementation services are costlier and company must provide ongoing software maintenance (upgrades, patches, etc.) with internal resources.
[7] Salary increases based on average high 9 percent increase over previous year.
[8] This scenario assumes a conservative 30 percent annual turnover rate for all security personnel. Recruiting cost is based on 25 percent cost of total annual compensation for in-house security professionals.

Benefits of Managed Security Services

Companies are increasingly dependent on information and information sharing to support continued operations. With the proliferation of scripts and intrusion technique descriptions, many companies are facing serious risks that did not exist five years ago. Since many businesses do not have the resources or desire to employ a full-time security team required to address these needs, they are looking for alternative approaches.

A good managed security services provider (MSSP) can offer an organization several advantages:

Improved information protection.

Security for today's networks and information systems is more complex and more critical than a few years ago. The methods and technologies used by hackers grows more sophisticated each month. If security is not the core focus of an organization, it is at a major disadvantage in having to provide a complete, rock-solid security management program.

The training, expertise, time, and diligence required to stay abreast of the latest protection strategies is time-consuming for in-house staff and takes them away from other mission-critical activities.

Leverage cumulative knowledge and experience of security experts.

The expertise of the MSSP's security analysts and engineers who manage and monitor security devices on a full-time basis is a valuable resource. These analysts see and respond to security incidents and attacks every day. This means they are considerably more aware of potential threats and more knowledgeable about how to thwart attacks than a company's in-house staff.

Stay abreast of the most recent security research and techniques.

An enterprise's MSSP should have a research organization dedicated to staying abreast of the latest cyber threats, vulnerabilities, hacker techniques, and security developments. Constant monitoring of security alerts and advisories is essential to providing maximum protection against security threats.

Share responsibility with a trusted security partner.

MSSPs offer service-level agreements that provide the contractual obligation to deliver services in a particular manner within a certain response time. The managed security services also include other features that mitigate potential security breaches, reduce liability, and provide peace of mind. In addition, MSSPs provide security expertise with considerable experience with intrusion detection and incident response practices. An MSSP acts as the company's security partner and shares the burden and the responsibility of security management and incident response.

Get reliable 24x7 security management.

A managed security services provider should provide around-the-clock coverage for the enterprise's most critical systems. This protects information assets and is especially important in an "always-on," always-connected, business environment. MSSPs watch their clients' networks and infrastructures to ensure protection during the very hours most hackers will attack. This also means corporate staff can free up valuable technical resources to work on mission-critical projects that provide higher return on investment.

Get the most from the security products already on hand.

Many companies purchase security products that, for a variety of reasons, are never fully implemented. A good managed security services provider ensures that purchased solutions are installed, implemented, and integrated to provide the on-going value a company needs and expects.

Take a cost-effective approach to security management.

By using an MSSP to provide protection for critical information assets, a company can avoid extensive personnel costs associated with hiring, training, and retaining security professionals. Managed security services reduce total cost of ownership by allowing transfer of personnel costs to a variable expense. Because managed services are billed on a monthly basis, it also allows a company to better predict and manage its security-related budget.

Selecting a Managed Security Services Provider

While determining the cost may be complicated, it also can be a relatively small part of the overall evaluation of a managed security services provider. Other key factors organizations should consider when evaluating a MSS provider include:

VENDOR ANALYSIS—STAYING POWER

According to Gartner, more than $1 billion in venture capital has been pumped into start-up managed security services providers.[v] Many of these organizations will fail, and numerous mergers and acquisitions will take place before the market settles. For this reason, it is imperative that organizations take necessary precautions to thoroughly analyze potential MSS vendors. A company should inquire about vendors' strengths and request documentation and other information to substantiate their strengths, experience, and success in the following areas:

- Financial stability
- Years in business
- MSS experience
- Customers
- Reputation

BREADTH OF SERVICES OFFERINGS

Companies evaluating MSSPs should investigate:

- How new managed security services are implemented
- Technologies, strengths, and weaknesses in the security services arena
- Expertise of the MSSP staff

In addition, organizations should determine whether the MSSP's offerings are flexible and broad enough to meet the company's current and future needs. Companies can evaluate the MSSP's management, monitoring, and response techniques by asking:

- What products and technology does the MSSP support
- How will the MSS staff operate in an emergency
- Is the MSSP able to hire and retain staff with sufficient skills to support the enterprise
- Does the MSSP have contingencies for adding specialized consultants should the additional expertise become necessary
- Are the service-level agreements stringent and flexible

ORGANIZATIONAL SUPPORT

When determining the level of organizational support, companies should ask MSSPs:

- Do they have access to or own any SOC facilities
- What are their staffing practices
- How is their staff retained and compensated
- How do they ensure client confidentiality

Companies should also ask about MSSPs' research and development departments, and funding for these areas:

- How is the MSSP staff kept abreast of the latest industry trends
- What specialized knowledge and security expertise does the MSSP staff have

RECOMMENDED MSSP PROFILE

Recommended MSSP Profile	Symantec MSS
Security is core business	✔
Demonstrated long-term financial stability	✔
Comprehensive suite of MSS offerings	✔
Uses proven MSS policies, standards, and procedures	✔
Recruited and trained professional security staff	✔
Defined staff development and career path	✔
Background checks to verify staff trustworthiness	✔
24X7 manned global operations	✔
Multiple, redundant SOCs with global coverage	✔
In-depth technical and security support skills	✔
Dedicated threat and vulnerability research support	✔
Dedicated team per client	✔
Services support multiple vendors' products	✔
Can implement security products	✔
Security and financial risks accepted under contract	✔
Tailored service level agreement	✔
Incident handling and response capability	✔

Conclusion

A comprehensive scheme of software, hardware, staff and expertise is required for complete security management. Whether it comes from inside or outside of the enterprise is a decision that must be made within the corporation using only its best data. The decision that's right for one enterprise may vary for another company.

A thorough cost analysis is important but is only part of the total analysis when choosing an MSSP. Also important are levels of staffing, expertise of the vendor, specialized skills that may only exist within the enterprise, and systems—hardware, software, firewalls—already in place.

Making the decision on whether to staff in-house for security services or hire a managed security services provider is a decision best made with much research, hard work and budgetary scrutiny with scenarios ranging over a number of years, focusing on maintaining a strong security posture while enabling revenue-generating e-business functions.

References

[i] Gartner Dataquest. "The U.S. Security Services Market Forecast, 2000–2005," June 1, 2001

[ii] Dinley, D. "Should outsourcing be part of your IT act?" InfoWorld Outsourcing Study, InfoWorld, February 12, 2001.

[iii] Carey, Allan, and Dean, Richard. "2001 Information Security Services: A Competitive Segmentation and Analysis," IDC, June 2001

[iv] The company is a sample representation of a mid-sized company. The cost assumptions are approximate and subject to change without notice.

[v] GartnerGroup Research Note. "Surviving the Managed Service Shakeout," March 15, 2001

SYMANTEC, A WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOLUTIONS TO INDIVIDUALS AND ENTERPRISES. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, REMOTE MANAGEMENT TECHNOLOGIES, AND SECURITY SERVICES TO ENTERPRISES AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS LEADS THE MARKET IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 37 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1.408.253.9600
1.800.441.7234

www.symantec.com

For Product Information
In the U.S., call toll-free
800-745-6054.

Symantec has worldwide operations in 37 countries. For specific country offices and contact numbers please visit our Web site.