WHITE PAPER

Going the MSSP Route

Understanding Total Cost of Ownership Issues

When determining the most cost-effective way to secure your organization, be sure to fully evaluate the cost-benefit tradeoffs between managed security service providers (MSSPs) and in-house solutions.

Introduction

As information security becomes both more important and more complex for enterprises of every size, business model and industry, IT organizations are confronting strategic decisions on how best to secure their companies' most vital assets. Whether it's customer records, confidential employee information, intellectual property or ensuring the ability to pass the next compliance audit, IT decisionmakers are grappling with how best to resource this vital set of functions.

Although working with managed service providers and outsourcing firms has become a standard practice for IT organizations for many years, IT decision-makers only recently have started to more aggressively work with specialized service providers for information security. These days, it's common practice for companies to evaluate the benefits of hiring these firms as opposed to managing security tasks internally.

This white paper is designed to help IT professionals understand how best to analyze and evaluate the benefits of working with an MSSP organization in a critical context understood and appreciated by both IT and non-IT managers: Total Cost of Ownership (TCO).

It's not just a matter of saying, 'It costs us X to secure the enterprise,' but putting it in relevant business terms, such as the price per customer transaction or the cost per email filtered."

Who Should Read This White Paper

- » CISO/CSOs
- » CIOs
- » CFOs
- » Directors of Security
- » Security Architects

Make or Buy? Putting MSSP Evaluation into a TCO Context

Core versus context. For decades, companies have used this yardstick to help guide their decision-making process for addressing IT capabilities. Conventional wisdom holds that tasks that are part of a company's core capabilities and contribute to its competitive advantage should, for the most part, be handled internally, while those that provide operational support for those capabilities should be outsourced to an external expert.

At the heart of this build-versus-buy decision (in-source versus outsource) are economic considerations: Does it cost an enterprise more to manage certain IT functions internally than it does to entrust an experienced third party to do it? As IT security has become more complex and more expensive to manage — and as IT budgets have been squeezed — many companies have analyzed the best economic solution to the IT security beast. More and more often, a comprehensive total cost of ownership (TCO) analysis points to the benefits of using an experienced managed security service provider (MSSP).

While evaluating the possibility of going with a service provider on a core-versus-context basis is hardly a new approach, the basis for that evaluation has changed. "Twenty years ago, that decision was driven largely by the desire to shift the cost of IT staff and facilities off your books," pointed out Joe Panettieri, editorial director of MSPMentor.com, which tracks the MSP community. "Now, the focus is about how to deliver IT services such as security in a cost effective, yet expert manner."

This move toward outsourcing certain IT security functions is borne out in a recent survey conducted by Tech Target over more than 150 IT security professionals. Those survey respondents indicated a growing movement among their firms toward hiring MSSPs to carry out a variety of security-related tasks. Nearly 60 percent of both IT and non-IT respondents to the survey said they felt positive toward outsourcing as an IT security strategy, primarily due to such factors as cost savings, access to specialized security expertise, cost predictability and 24/7/365 security monitoring. More than 20 percent of the survey respondents said their organizations either will begin using MSSPs for the first time this year or will increase their usage of those partners' services, while an additional 21 percent said they will at least maintain their current usage levels of MSSP services.

When determining the economic benefit of using an MSSP for security functions, IT decision-makers need to understand both the direct and indirect costs associated with carrying out those security tasks. While quantifying indirect costs is subject to some debate, there's little doubt that they should be part of the evaluation process. Perhaps the most important reason is that in order to make an apples-to-apples comparison, IT managers must understand their full cost of IT security operations, and this is where many TCO analysis projects fail to yield actionable data.

"The only way to do a fair and accurate TCO analysis is for a company to ask itself, 'What do we actually pay for this service?'" advises Paul Pinto, managing partner of SylvanVI, an IT consulting firm. "Many companies often overlook stuff that a very sharp IT executive will intuitively understand, or be able to find out the answer to. It's not just a matter of saying, 'It costs us X to secure the enterprise,' but putting it in relevant business terms, such as the price per customer transaction or the cost per email filtered."

Experts agree that it all comes down to getting a good handle on all relevant costs that, as best as can be determined, can be isolated to security activities. It's a bit trickier to do that today than it was years ago, because security is often embedded into most IT operations. But a balanced analysis of security TCO on an internal or external basis should include the following cost considerations:

- **Internal security staff: Because security today is much more than anti-virus software or spam filtering, more experienced resources are necessary to ensure the security of a company's vital assets.**

  Forty-four percent of organizations say they are dissatisfied with investment in cybersecurity technology because they lack the in-house expertise to leverage it.[1] For a typical enterprise-class IT organization, security monitoring and management will probably require at least five full-time employees. Average U.S. base salary

[1] Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis*, May 2015.

for an IT security administrator is $80,000 according to salary.com, so you're talking about $400,000 in direct costs — to start. Of course, that's just a piece of the cost structure.

Most conservative financial estimates put incremental staff-related costs at a minimum of 50 percent of salary, to accommodate such costs as taxes, benefits, training and "overhead" such as office space, utilities, technology support, etc. That bumps up your annual direct staff costs to at least $600,000 for an average sized enterprise. And, reminds Pinto of SylvanVI, "Don't forget that a typical IT employee turns over in 18 months, so you have to account for costs to hire and train new employees to the point where they can be as productive as the person who just left." Additionally, you need to consider the costs associated with having a vacant position unfilled for some time considering the worldwide shortage for qualified IT security professionals. Will other staff members have to pick up the slack in the interim, perhaps incurring overtime costs? What projects will be delayed and deferred while they fill in the gap? For many companies, just being able to save on the internal staff costs is the biggest reason to justify moving key security functions to an MSSP—a finding that was prominent in the Tech Target research study.

- **Infrastructure costs: Although IT organizations will continue to need hardware such as servers, storage and security appliances, using an MSSP will mitigate the need for additional investments to acquire, deploy and manage equipment for security management and monitoring — now and in the future.**

  The same holds true for SIEM-related software; a key advantage to working with MSSPs is that they are already utilizing the most up-to-date security tools on the market, and have figured out how to make them work with other, often incompatible tools across a wide variety of hardware and software platforms. Additionally, MSSPs already have made sizeable investments in their own hardened environments, called Security Operations Centers (SOCs), alleviating the need for customers to make the same levels of investments in data centers and network monitoring facilities.

- **Compliance costs: Working with an MSSP allows your IT organization to reduce the time and effort needed to comply with audit requirements when the auditor sees the evidence of controls that the MSSP is supporting through its services.**

  For the first time, in October of 2014, the Federal Communications Commission fined two companies $10 million each for maintaining "unjust and unreasonable" data security practices in violation of the Communications Act of 1934. The message is clear that regulators will be more active when a major breach occurs. Additionally, at least 23 states introduced or considered security breach notification legislation in 2014[2]. Working in concert with in-house IT organizations, MSSPs are a responsive, cost-effective asset to deploy and improve certain controls required for compliance mandates. MSSPs are expected to stay current on both broadly applied mandates and more obscure, narrowly focused compliance statutes, often providing even more specialized knowledge of those statutes than the internal staff possesses.

- **Security event response costs: According to a recent study by the Ponemon Institute, the average total organizational cost of all types of data breaches in the United States has increased 21 percent over three years.[3]**

  Today's organizations accept that they will likely be compromised. A "win" in today's cyber threat environment is defined by how quickly and effectively an organization is able to respond to hackers and extricate them from their systems. To win, it requires a significant level of manpower and expertise on a daily basis. A properly organized and staffed security team requires people with a variety of skills and certifications to deploy new technologies, keep up with a changing threat landscape, determine hacker motives, fix vulnerabilities, and deflect attacks.

  What chance does an understaffed, overworked internal IT team have to spot a potentially devastating security event before huge damage is done? Because MSSPs work with a wide variety of customers, chances are good that they know the telltale signs of trouble and can remedy the situation as soon as a threat is identified.

[2] http://www.ncsl.org/research/telecommunications-and-information-technology/2014- security-breach-legislation.aspx
http://www.securityweek.com/boards-dissatisfied-cyber-it-risk-info-provided-management

[3] Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, May 2015.

According to the Identity Theft Resource Center, the number of data breaches tracked in the United States was 781 in 2015. This represents the second highest number on record. These numbers are by no means the whole story, as ITRC has tracked 5,810 reported breaches since 2005.[4]

All this sounds good in theory — and, it often looks good on paper when you line up fully loaded internal costs side by side with monthly fees charged by an MSSP for those same services. In fact, Forrester Consulting conducted an independent Total Economic Impact study for managed security services used by a large, U.S.-based media company. That study revealed that using managed security services from Atlanta-based SecureWorks saved the company more than $3 million over a three-year period.

But everyone agrees that the key to realizing value from an MSSP is its ability to deliver those high-quality services at prices that do represent actual hard-dollar savings versus internal staff. As more companies work with MSSPs, success stories point out how small and large companies alike have seen real-world benefits.

For instance, take Encysive Pharmaceuticals, a Houston-based healthcare and biopharmaceuticals company with about 150 employees. Encysive was looking to insulate itself against cyber threats, but didn't feel comfortable taking on the cost of additional staff to meet the challenge. After evaluating several MSSP options, it selected SecureWorks to provide the necessary skills and to achieve a lower TCO. "It's much better to partner with an expert to help manage and monitor your firewall on a 24/7 basis — for us, it works extremely well," said Carl Burquist, senior network administrator for Encysive.

At the other end of the spectrum, consider the case of 3,200-employee Concord Hospital, a New Hampshire-based healthcare facility. A small but capable internal team was increasingly being taxed by regulations such as HIPAA and Payment Card Industry (PCI) mandates, as well as the need to upgrade its firewall solutions to safeguard against new security threats. Although Concord's parent organization, Capital Region Health Care, had used an MSSP for 24/7 network monitoring, it was looking for a more cost-efficient solution that could also handle the event logging model necessary to ensure more effective threat identification and resolution. By working with SecureWorks, Concord not only saved money but improved overall security monitoring and event management.

These are just a few situations where the most fundamental security task of "keeping the bad guys out" makes all the sense in the world for an MSSP, according to John Pescatore, vice president at IT consulting and research firm Gartner Inc. "Things like intrusion protection, firewall, antivirus and other functions where the threats are changing often, these are cases where MSSPs are far more likely to be on top of the changes than an in-house staff," he said. And, if an organization needs 24/7 coverage — and these days, that applies to more and more companies — then it usually makes more economic sense to contract with an MSSP than to hire five or more full-time staff to provide the same level of monitoring and management.

Of course, saving money is important — vital, in fact. But it's not the only benefit organizations can attain by working with MSSPs. A major reason why working with an MSSP can reap tangible benefits is simply the MSSP's ability to keep the organization protected and operating with greater effectiveness than an internal staff. Working with an MSSP allows an organization to lever age the collective experience and expertise of an MSSP's staff, which typically holds numerous advanced certifications in security and devote a sizeable portion of their workweek to ongoing training and education to spot newly emerging threats before they strike.

"When it comes to keeping up with the latest risks, and having the training necessary to deliver best-of-breed security services, MSSPs are generally in a much better position than inhouse staff which often is manned by IT generalists rather than security experts," pointed out Jeff Kaplan, managing director of Think Strategies, an IT strategy consulting firm. He added that utilizing MSSPs for security tasks also creates an important benefit by allowing internal staff to concentrate on activities that address an organization's core competency, rather than sit in front of a monitor eight hours at a time.

[4] Identify Theft Resource Center, "Identity Theft Resource Center Breach Report Hits Record High in 2015" January 25, 2016; accessed 2/24/16; http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

Summary

As IT budgets continue to be under pressure and companies look to maximize the value of all investments, small and large organizations alike are moving toward a managed services model for fulfillment of a wide variety of security functions. While many companies claim to offer managed security services, very few of them actually prioritize it as a full-fledged practice . . . and even fewer of them have the resources and experience to bring to bear on behalf of large and small companies alike across different industries.

Careful financial analyses have demonstrated the TCO benefit in using an MSSP can be substantial, both in terms of actual dollars saved and by allowing internal staff to be redeployed on activities that are closer to a company's core competency. Since most MSSP costs are subscription-based, those don't impact a company's capital budget. IT managers usually find it easier to get approval for operating expenses than capital expenses. When the relationship with an MSSP is managed properly, IT organizations benefit from having best-of-breed capabilities available to them on a "rental" basis instead of having to beg their CFO or other senior executives for additional staff — only to risk having it downsized in difficult business cycles.

In both economic booms and recessions, that kind of financial flexibility is extremely attractive to organizations.

About SecureWorks

SecureWorks provides an early warning system for evolving cyber threats, enabling organizations to prevent, detect, rapidly respond to and predict cyber attacks. Combining unparalleled visibility into the global threat landscape and powered by the Counter Threat Platform — our advanced data analytics and insights engine — SecureWorks minimizes risk and delivers actionable, intelligence-driven security solutions for clients around the world.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com