WHITE PAPER

WHY MOVE TO AN MSSP?

SECURING I.T. IN AN ERA OF THREAT SURPLUS AND TALENT SCARCITY

Trustwave®

Smart security on demand

WHY MOVE TO AN MSSP?

SECURING I.T. IN AN ERA OF THREAT SURPLUS AND TALENT SCARCITY

This paper identifies and analyzes the most common reasons provided by IT directors and chief information security officers for moving IT security functions to a hybrid or fully managed security services provider (MSSP) model. While rationales ranged from tactical to strategic, MSSPs offered unique methods of overcoming several common challenges. Depending on an organization's ability to hire, train and retain in-house security experts, and efficiently use their costly skill sets, the case for an MSSP goes from being a convenience to the only viable way to effectively expand the breadth and depth of an organization's security coverage to acceptable levels.

Broadly speaking, the three most significant reasons to move to an MSSP are to augment skills, stretch security budgets and improve security outcomes. The degree of each benefit depends on a number of variables, including organization size, industry, location, relative information security budget, brand profile, specific security gaps to cover and one's general IT philosophy. In this white paper, we will review each MSSP rationale in depth, offering insight into which factors make the case to move to the MSSP model more or less compelling.

AUGMENTING SKILLS

Finding, training and retaining qualified IT security employees remains a challenge across industries. There is broad consensus in the cybersecurity world that the number of attackers, threat techniques and vulnerable attack surfaces are increasing faster than IT security budgets, teams and countermeasures can keep up. Even though IT departments are recruiting heavily, experts estimate that the shortfall in IT security staff is more than one million jobs globally. Forrester Research's Ed Ferrara reported in the January 2015 report, *Understand Cybersecurity and Risk Budgets for 2015,* that IT security budgets across all industries increased almost 80 percent between 2012 and 2014. But, Gartner Analysts Jeremy D'Hoinne and Tom Scholtz confirm that the security budget increase will not be sufficient to close the skills gap (Gartner, *CISOs Should Review Their Enterprise's Security Skills Portfolio Now*, 19 February 2015). Network World reported that, "Cybersecurity job postings grew 74 percent from 2007 to 2013, which is more than twice the growth rate of all IT jobs." Some CISOs Trustwave has spoken to believe IT security actually has a negative unemployment rate. Yet even Fortune 500 companies with large budgets, recruiting clout and ample perks have trouble hiring enough qualified IT security professionals to cover all their bases. Finding capable security professionals is even more of a challenge for small- and medium-sized organizations with less budget. IT security talent is also more difficult to recruit for sites located outside of the largest dozen or so U.S. metropolitan areas, where the supply of IT security experts is proportionately less.

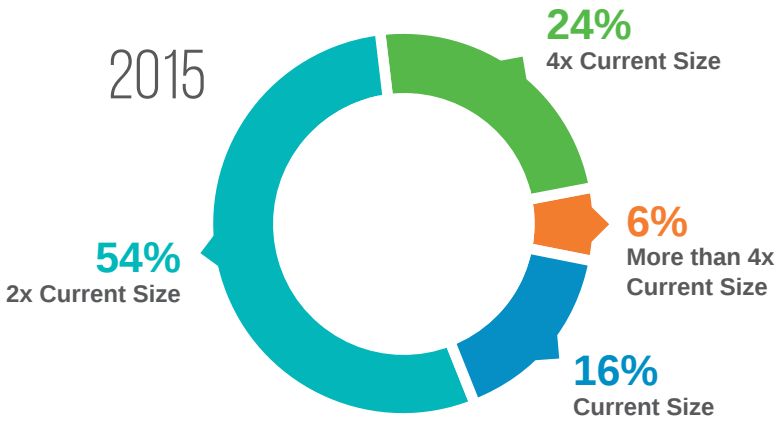
49% *of security positions were left unfilled in 2014*

…experts estimate that the shortfall in IT security staff is more than one million jobs globally.

Just how short staffed is the typical IT security group? According to the 2015 Security Pressures Report from Trustwave, based on a survey of more than 1,000 security professionals, 54 percent believe they need to double their IT security staffing, and 24 percent believe they need four times as many security staff. This chronic shortfall has many practical impacts. Basic security tasks are deferred. Event streams and alerts that should be monitored continuously are overlooked. According to published

reports, some of the largest retail chain payment card breaches of the last two years involved organizations that had breach detection systems in place that produced alerts, but there were not enough security analysts on staff to properly interpret and investigate these alarms. As IT environments increase in scope and complexity, this task gets even more challenging. Trustwave SpiderLabs research has shown that the typical breach is not detected for 188 days, and 81 percent of the time is first discovered by someone outside the organization, such as a customer, law enforcement or the media.

What is Your Ideal Security Staffing Size?"
(based on respondents to the 2015 Trustwave Security Pressures Report)



A lone in-house expert is potentially a single point of failure. For smaller organizations, even if they have a qualified information security professional in a critical role, that person likely is their only resource. An employee is not always available because of vacations, illness, personal matters or other job duties, or they have already worked 40 to 60 hours that week. Additionally, security professionals are in such high demand that they change employers frequently. They are often recruited away by other short-staffed organizations offering better compensation, status or workload. Ironically, the more indispensable an IT security employee is, the more likely they are feeling overburdened and seeking out a less stressful position. They have many choices. Employers do not. According to an ISACA and RSA Conference 2015 survey, more than 32 percent of open IT security positions take six months to fill or cannot be filled at all. Finding a replacement for a single in-house expert can take months and leave a serious void in one's security posture.

While the complete elimination of risk is impossible, IT departments generally work to manage risk down to acceptable levels for their particular industry, brand, business model and compliance mandates. Unfortunately, most organizations today are forced to accept excessive risk because they lack the skills or cycles to take reasonable preventative steps. Particularly telling is that 77 percent of organizations are pressured to unveil new IT projects before they are security ready. These businesses simply don't have the bodies and depth of skill to follow rapidly evolving security and compliance best practices. While IT budgets are growing on average, they do not appear to be keeping pace with the perceived increase in risk.

Risk reduction in an era of talent scarcity requires more resourcefulness from IT security teams. While added training for employees can bridge some shortages, it takes extra people to augment an IT group's time and efforts. MSSPs provide a team of security specialists to back an IT team up. They can help as broadly or narrowly as desired, from offering depth of expertise for small organizations to flexible augmentation for larger ones. MSSPs can help shield an organization from single points of failure. They provide redundant experts without the customer paying additional full-time equivalents (FTEs). MSSPs also are able to manage a wide range of security devices, customize and update policies, and consistently monitor and attend to systems to optimize protection.

MSSPs are particularly helpful for offloading tedious or bulk security tasks…such as 24x7 log monitoring.

If needs suddenly grow, the MSSP offers a means to handle workload spikes, as well as recruitment and training. An MSSP can also remove worries over an abrupt loss of in-house IT security personnel, giving IT security managers more control and peace of mind.

MSSPs are particularly helpful for offloading tedious or bulk security tasks. For example, these providers are able to do the heavy lifting of 24x7 log monitoring. Their experts are efficient and effective at threat correlation. This preserves in-house staff for handling escalations, strategy and tasks requiring more idiosyncratic knowledge of a particular organization. In essence, MSSPs allow organizations to focus on higher value-add functions that are strategic to the business.

STRETCHING SECURITY BUDGETS

Many IT teams have constrained systems and resources. Shortages may include:

- No security operations center (SOC), or a limited SOC
- Insufficient capital expense budgets
- Insufficient headcount for the growing threat range
- Lack of time, since non-specialist IT people are less efficient and slower at security
- Inadequate recruitment budget, since security staff are highly sought after, frequently change jobs and must be replaced often
- Not enough work to justify an FTE for some tasks

While some of these can be mitigated with enough budget – and security spending plans have been trending upward – the need is outpacing available funds. IT security groups are exploring various ways to do more with less. MSSPs offer a number of opportunities to stretch IT security budgets.

MSSPs provide a 24x7 SOC without an organization having to build and staff one themselves. This is crucial to rapid detection and response to security events and breaches. A round-the-clock SOC means there are experts available whenever a security event occurs. MSSP personnel can investigate automated alerts, escalate serious incidents, and quickly interdict and minimize threats. Smaller organizations often lack the budget or economies of scale necessary to erect a fully functioning, certified, enterprise-grade SOC that will operate around the clock.

IT departments gain several security operations benefits from using an MSSP. They obtain a world-class SOC that meets high-facility standards for a fraction of the cost of standing up their own center. They get seasoned experts to operate the SOC who have gained experience supporting similar organizations. They obtain mature best practice procedures, which improve responsiveness and efficiency enough to prevent or contain breaches sooner.

MSSPs can minimize or eliminate large upfront capital costs for best-of-breed and additional systems. MSSPs often provide equipment on a subscription. The MSSP model often includes options for managing one's existing systems – or adding new capabilities. MSSP offer subscriptions to Unified Threat Management (UTM), anti-malware and Secure Web Gateways (SWG), Secure Email Gateways (SEG), Web Application Firewalls (WAF), Network Access Controllers (NAC), Security Information Event Management (SIEM) appliances and more. If an organization is looking to add or upgrade such a system, a MSSP offers a way to shift the cost from capital expense to operating expense, and reduce the upfront cost and labor of deploying such a system. This speeds up the ability to acquire and implement security.

Working with an MSSP can be easier to justify than adding permanent staff. Some organizations scrutinize headcount requests more than outsourcing requests. Managed services offer more flexibility to add or subtract people without involving bureaucratic or political obstacles. Reallocating experts from lower-risk to higher-risk vectors is also usually easier, allowing faster response to emerging threats.

MSSP may stretch budget by being more efficient. MSSP specialists are further along the learning curve and able to resolve issues faster than an in-house IT generalist using the same tools. MSSP technicians have more experience installing, configuring, tuning and managing specialized security systems. They develop high-level acumen by being exposed to many other enterprises, and each individual MSSP client gains the benefit of the MSSP's streamlined skills. Also, they are more up to date on best practices. They work with many other technicians in the same area of security, jointly developing, iterating and sharing effective, efficient techniques. Typically this reduces non-productive cycles and increases the amount of useful security benefit for time spent.

Recruitment and training costs are eliminated or reduced when using an MSSP. The cost to search for, onboard, train, ramp up and, all-too-often, rush to replace in-house security talent can be considerable. Given the protracted searches and frequent backfilling required, most organizations are surprised and pleased how much an MSSP can reduce their heavy recruitment costs.

As for FTEs, some organizations have strained security budgets because they hired in-house experts they cannot fully use. The function is critical, but the need is sporadic. They pay to have an in-house expert on standby, but the actual workload does not constitute a full-time equivalent. There is an alternative to overpaying for an expensive and underused in-house expert. With an MSSP, organizations obtain access to multiple experts, but pay only for what they need.

IMPROVE SECURITY OUTCOMES

Surveys, news reports and analyst research agree that many IT security teams are not receiving best-in-class outcomes from their security investments. Depending on the layer or system, analysts reportedly find that fewer than 20 percent of IT organizations are able to achieve a proactive security posture. Perceived deficiencies, or at least easily recognized missed opportunities, include:

- Unable to cover all the desired threat vectors
- Not keeping systems patched and running latest versions
- Underused software, or software not used at all
  - Recent surveys show 28 percent of organizations own under-deployed security software
  - Lack of skills and time are often the biggest causes of unused security technology
- Unable to spot global security trends early enough to benefit
- Insufficient familiarity with security tools to get full benefit
- Slow to add capacity, people and systems
- Slow to develop skills capable of covering newer threats

Taken individually, the deficiencies listed above are serious. When combined, they can be catastrophic. However, using an MSSP to adequately fill critical roles and stretch budgets can have direct and indirect effects on improving security outcomes. To assess how, it is helpful to examine MSSP's effects on each of the above-listed common obstacles to effective security.

MSSPs help cover more threat vectors. A MSSP does this by augmenting one's team, bringing more expertise to bear, using their time and tools more efficiently, adjusting to new threats faster and freeing up internal resources to add higher-order value. MSSPs also have mature methodologies to mitigate the biggest risks sooner and the efficiency to mollify more total risks.

19% *of pros admitted IT **did not understand the software** well enough to implement it*

MSSPs keep systems more up to date. MSSPs that manage solutions they sell have more advanced notice on patches and more insight into the importance of these updates. They also have practical and financial reasons to keep systems up to date and optimally configured, reducing costs and improving reputation. In addition, up-to-date systems diminish risk windows when new attack methods or vulnerabilities are discovered.

MSSPs help reduce "shelfware." MSSPs don't get paid for unimplemented systems. By definition, they have the skills and time to deploy any system they manage. Shelfware is a big security problem. According to the Security on the Shelf Report from Osterman Research, while security software spending per employee is increasing, $33 out of every $115 spent is underused or wasted, and as much as 60 percent of security software goes completely unused. The report goes on to say that shelfware remains an issue largely because IT organizations often lack the time or expertise necessary to implement security software adequately. As a security expense, shelfware is 100 percent waste. MSSPs provide the time and resources needed to implement the security they manage.

MSSPs are likely to spot new and emerging threats first. With MSSPs, one benefits from having a large team of specialists working closely together, monitoring a large portion of the internet and keeping each other abreast of fast-moving developments at various enterprises. Statistically, MSSPs are in a much better position to learn of emerging threats – and mitigate such risks – than in-house experts.

MSSPs are driven to use up-to-date practices. MSSPs are, out of necessity, pioneers of (and leading-edge implementers) of new best practices. MSSPs have greater specialization and economies of scale from providing similar services to many organizations. They have the opportunity to refine technique iteratively for greater effectiveness. This enhances security outcomes. Additionally, MSSP professionals who manage technology that their company produces have even more insight into adopting and mastering proactive security practices for those solutions.

MSSPs are more familiar with their security tools. Using security tools across many different enterprises allows MSSP specialists to be more skilled with the tools than the typical IT department employee. MSSPs tend to know the features more thoroughly and recognize more quickly the necessary approach to most problems. This expertise is enhanced through a direct connection with the engineers who designed the security tools, allowing for further enhancements and optimization.

MSSPs are typically faster to add capacity, people and systems than in-house management. Extra experts are usually just a phone call away. Capacity (especially on cloud-based managed services) is often available at the flip of a switch. New sites can be brought online more quickly. New services, such as log monitoring or threat correlation, are more readily added. By avoiding unnecessary delays, vulnerability windows are shortened, and security outcomes tend to be improved.

MSSPs are usually faster to develop new skills to combat new threats. Some full-spectrum MSSPs offer complementary services, such as forensic incident response and penetration testing. Incident response investigators travel on site to learn how attackers are operating in real-life breach scenarios. Penetration testers frequent the criminal underground to understand where adversaries obtain their tools. As a result, they replicate hackers' techniques to more deeply understand the nature of the threat and how better to prevent it. Some pen testers also have laboratories and use honey pots to gain deeper insight into the leading edge of threats. This level of research and acquired skill in countermeasures is generally not available to IT department employees.

BALANCING THE FACTORS

While MSSPs are not the right answer for every problem, and not every MSSP is right for every organization, certain trends have emerged that shed light on when it makes the most sense to use an MSSP.

Organizations facing IT security hiring shortfalls or excessive turnover should consider MSSPs for staff augmentation. Organizations should first apply MSSPs to where they will obtain the largest increase in security posture or the greatest freeing-up of internal staff for more strategic tasks.

Typical areas to consider applying an MSSP to are network security, application security, web and email security, and SIEM. These are functions where superb results depend more on deep understanding of a powerful security solution than intimate knowledge of an enterprise's inner workings. Conversely, functions like data loss prevention are harder to undertake without substantial knowledge of what constitutes normal acceptable behavior by employees.

The degree of offloading to the MSSP is flexible thanks to dashboards and command consoles that enable flexible allocation of tasks to the experts. Tasks can be partly delegated to the MSSP, or more fully managed (such as bulk event monitoring or threat correlation) by the MSSP. This allows in-house staff to focus on escalated alerts that may benefit from being on premise to resolve.

MSSPs increase job security for in-house IT staff. The net gain in security coverage afforded by an MSSP reduces risk of the types of avoidable incidents that threaten IT security team members' jobs: breaches, compliance failures or simple lack of visibility. MSSPs help deliver broader security coverage, address compliance requirements and see more clearly how to allocate resources to ensure one has met their organization's security needs for now and the future.

Small- to medium-sized organizations have more to potentially gain from MSSPs in terms of a first-tier SOC, 24x7 coverage, and paying for only as much expert time as needed – and no more.

The greatest benefit of an MSSP varies depending on the particular organization. While most organizations initially assume the primary benefit of MSSP is improving security outcomes, the accelerated pace at which the MSSP allows security to be deployed and maintained can actually expedite IT projects that affect the top line of the business. Some applications, cloud services and website enhancements that would otherwise have been delayed for unresolved security concerns can "go live" sooner, aiding strategic business growth. There are also scenarios where an MSSP actually reduces overall costs, thereby benefitting the bottom line.

Overall, the increasing complexity of securing information technology requires greater expertise, specialization and numbers of tools to stop the diversified threats. MSSPs are a logical option for simultaneously meeting these demands.

HOW TRUSTWAVE FITS

- Trustwave's mission is to make effective IT security available to organizations of all sizes and skill levels. We offer a wide range of IT security technologies globally and around the clock to efficiently protect data, applications, networks and assets. Trustwave provides extensive managed security services to augment IT teams and enable them to maximize protection.
- Trustwave views providing security technology and managed security services as a natural synergy. Our experts are more proficient at using security tools because we create the tools ourselves. Trustwave engineers make the security tools better because our MSSP experts use the tools in many different environments and provide continuous feedback.
- Trustwave Managed Security Services are also stronger because of our SpiderLabs group. SpiderLabs is Trustwave's elite team of ethical hackers, forensic investigators and researchers helping organizations fight cybercrime, protect data and reduce risk. SpiderLabs conducts hundreds of incident response forensic investigations each year and thousands of penetration tests.
- Trustwave manages many leading third-party IT security solutions, our own patented security technologies and hybrid installations. This speeds deployment, enhances flexibility now and in the future, and offers opportunity for balancing security, cost and convenience to best meet business needs.

Trustwave's mission is to make effective IT security available to organizations of all sizes and skill levels

In sum, we have more event streams, field investigators and managed security solutions enriching our big-data global threats database than any other vendor. We take that rich data and use our industry-leading SpiderLabs experts to apply those findings. As a result, we believe Trustwave prevents more types of new attacks than any other vendor.

Whether MSSPs are sought to bridge staffing shortages, flexibly access expertise or stretch budgets, the incremental benefit they provide to security is considerable. Organizations that use Trustwave as an MSSP find they are able acquire a well-tuned balance of technology and skills to cover more attack surfaces against more types of attacks – and generally within existing budgets – hence optimizing their security outcomes.

To talk to a Trustwave expert about where managed security services might make the most sense for a particular organization, click here.

Trustwave®

Smart security on demand