SECURITY OUTSOURCING COMES OF AGE

KEY ISSUE:

Security outsourcing benefits grow and broaden, but also require diligent oversight

Today's security teams are increasingly challenged to mount a competent defense of the organization via prevention, detection, response and recovery activities. **Large enterprises with security operations centers (SOCs), as well as smaller organizations without deep expertise, look to strategic security sourcing as a way to enhance their capabilities, but need to weigh the benefits against potential risks.**

The increased maturity and complexity of threats, scarcity of security talent and budgetary pressures all converge to force security teams to take advantage of efficiencies of scale by paying for specialists to handle of variety of security tasks. [1][2][3][4]

The potential benefits to strategically sourcing some or all of the security functions are compelling:

- Access to specialized security technology and expertise.[5]
- Reduced costs (both CapEx and OpEx).
- Improved operational efficiency and service levels.[6]
- Capital preservation.

Yet organizations have long perceived the risks of outsourcing to be obstacles:

- Loss of control.
- SLA limitations.
- Concerns about confidentiality, integrity and availability, both on the part of the provider and any subcontractors.

CHALLENGES AND OPPORTUNITIES:

Trends toward increased strategic security sourcing provide context for risk/benefit analysis

Security is now seen as one of the areas with the greatest potential for improving service and reducing costs.[7] Almost 30 percent of companies choosing to strategically source security take a blended approach, outsourcing both operational and highly technical areas of security while retaining some key functions internally.[8] One development that allows for increased use of security outsourcing is an increase in service provider acountability. Many managed security service providers (MSSPs) have well-known reputations. These providers track SLAs and have confidentiality agreements backed by law and insurance. [9][10]

Prime strategic sourcing candidates used to include tasks such as security monitoring, patching and firewall management, as well as identity and access management, application security and vulnerability scanning.[11] **The trend today goes beyond this: companies are looking to strategic sourcing as a means of enhancing internal security capabilities.**

How many companies can afford to build an internal malware reverse-engineering function? The cost, lack of expertise and potential threat to the network make this a prime candidate for working through a strategic partner with existing expertise.[12] The same goes for advanced security functions like hunting for threats and forensic capabilities. These functions can be done more effectively by a provider that has broad vision across many different types of companies and environments.

- Businesses expand their outsourcing activities related to network traffic analysis, network forensics, payload analysis and endpoint forensics, according to Gartner.[13]

An enterprise cannot outsource accountability. Strategic sourcing is rarely advised for governance, risk and compliance functions that are designed to manage these processes, no matter if they are provided internally or by strategic partnerships. Enterprises must ensure the service provider complies with legal, regulatory and industry requirements. Setting strict goals and establishing performance metrics are a part of an enterprise's continued responsibility, regardless of the sourcing model utilized.[14] [15]

THE PATH FORWARD:

Discuss security goals and understand current threats

EVALUATE NEED

Outsourcing needs should be evaluated by asking the following questions:

- Can the security program scale to the level of the organization to keep from being a drag on productivity?
- Does the enterprise want to own the required technologies, or just rent those technologies since the "best solution" continually changes?
- Can the enterprise afford the type of operational expertise needed to face evolving threats?

For example, when considering strategically partnering for security operations, capabilities examined should primarily consist of security analysts organized to prevent, detect, respond and recover from cyber security incidents. Specific questions based on the above include: [16] [17]

- Are experienced security operations staff available internally?
- Are 24x7 security staff required? And if so, available internally?
- Is it possible to train and retain SOC personnel at the rate of growth needed to keep pace with broader business needs?
- Is it possible to balance size and visibility/agility internally, so the SOC can execute effectively?
- Is this a function that makes sense to own, or is it better to strategically source since leading practices and capacity needs seem to change quickly?
- Is it possible to match the results of sourcing providers who collate and correlate information from potentially thousands of diverse sources, and perform highly complex operations such as hunting for a competitive price?

If some level of strategic sourcing is called for, the next step is to refine what blend of services is required given an enterprise's goals and internal capabilities. For example, specific capabilities to request from service providers could include:[18]

- Improve security capabilities (forensic investigations, hunting activities, vulnerability management, security monitoring, identity and access management)
- Enhance service levels (firewall management, VPN, patching, anti-DDoS)
- Reduce costs (disaster recovery, log monitoring, anything that requires excess provisioning to handle peak loads)

MANAGE RISKS

Carefully consider the delivery model and service level agreements. Questions to ask the service provider could include:

- What are the operational hand-off points, and who is responsible for defining accountability for these specific critical functions?
- Will delivery be cloud-based, managed on-site equipment or a hybrid model?
- How will the quality and cost of service be measured?
- Is there a proven ability to meet compliance requirements?

Contract negotiations will require a very clear definition of your needs, goals and SLAs, as well as validation requirements. Remember that accountability can never be outsourced, and contract negotiations will be the start of enforcing governance over the sourced processes. The contract should include specifics on the boundaries between the responsibilities of your staff and that of the strategic sourcing provider. [19]

CALL TO ACTION

Clarity is required before engaging with a service provider about the desired end state of a strategic sourcing relationship. This clarity will drive the most valuable investment, and will allow an enterprise to develop oversight mechanisms that allow it to keep its finger on the pulse of delivery while receiving significant value from the relationship.

The security landscape is too complex to manage in isolation. It is too expensive for most enterprises to develop the breadth of expertise needed internally. Defending against ever-maturing security threats requires an economic model that can scale, and one where the suite of solutions are provided by an ecosystem of trusted service specialists. With a trusted partner and a credible oversight process, an enterprise can simultaneously expand capabilities and save money by tapping into this growing ecosystem.

1 Ashford, Warwick. "Best Practice in outsourcing security". ComputerWeekly. Feb 2012, Retrieved from http://www.computerweekly.com/feature/Best-practice-in-outsourcing-security
2 "Get Ahead of Cybercrime". Ernst and Young. October 2014. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf
3 Morgan, Steve. "Cybersecurity job market to suffer severe workforce shortage" CSO. July 2015. Retrieved from http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html
4 Chapple, Mike. "Outsourcing Security Services". Information Security Management, March 2013. Retrieved from http://searchsecurity.techtarget.com/ezine/Information-Security-magazine/Outsourcing-Security-Services
5 Chapple, op cit
6 "Disaster Recovery Tops List of Outsourcing Cost Savings" Computer Economics. August 2015. Retrieved from http://www.computereconomics.com/article.cfm?id=2117.
7 Masters, Greg. "Outsourcing IT security continues to grow, study finds" SC Magazine. August 2015. Retrieved from http://www.scmagazine.com/outsourcing-it-security-continues-to-grow-study-finds/article/433657/
8 Ashford, op cit.
9 Pros and cons of outsourcing security" Computers.In4mnation.com November 2014. Retrieved from http://computers.in4mnation.com/pros-cons-outsourcing-security/
10 Ashford, op cit.
11 Chapple, op cit.
12 Liska, Allan, Building an Intelligence-Led Security Program (Rockland, MA: Syngress, 2014) 154.
13 Kavanaugh, Kelly. "Technology Overview for MSSP Advanced Threat Defense" April 2015. Gartner. Retrieved from http://www.gartner.com/document/code/269742?ref=grbody&refval=3175118
14 Ashford, op cit.
15 Newing, Rod "Service Suppliers: Risk or Rigour" December 2011. Racontour. Retrieved from http://raconteur.net/technology/service-supplie-rs-a-security-risk-or-a-security-boost
16 "Ten Strategies of a World-Class Cybersecurity Operations Center" MITRE. 2014. Retrieved from https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf
17 Steinnon, Richard "When should you outsource security?" Forbes. Sept 2011. Retrieved from http://www.forbes.com/sites/richardstiennon/2011/09/21/when-should-you-outsource-security/
18 Computer Economics, op cit.
19 Chapple, op cit.

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

1.16 | F1