Thoughts on Managed Security Services Provider Engagement

By Daniel Schatz – ISSA member, UK Chapter

This author reviews some of the resources that can help information security professionals to identify the right managed security services provider for their organization and highlights several key criteria to consider.

Abstract

Managing information security risks has become one of the top agenda points of almost every organization. Part of this is to understand the options available to handle the task and make an educated decision on the best option for the environment in question. Often the choice is to outsource this function to a company that specializes in managed security services so that the organization can focus on its core business. Finding the right vendor is not an easy task; getting the best value out of the contract demands work on side of the organization in order to truly understand its requirements and expectations. This article reviews some of the resources that can help information security professionals to identify the right provider for their organization and highlights several key criteria to consider.

Understanding the requirements and options

Information security risk is a hot topic drawing the attention of media, regulators, and consequently executives and board members. Business leaders become increasingly aware of these risks as shown, for example, by the World Economic Forum "Global Risks 2012"[1] and later editions. The report states that "Cyber security emerged as the key risk, and it encompasses a wide range of complex issues, ranging from behavioral to geopolitical in nature."

This is not a sudden development by any means but evolved rather steadily over the last few years and has led to increasing budgets supporting security risk management functions in organizations. Although IS departments are in a considerably better position now in terms of budget than they had been in the late 20th century, many are still struggling to put that money to good use as the talent pool for IS professionals remains shallow.

With this in mind it is no surprise that organizations investigate whether a Managed Security Services Provider (MSSP) engagement is the right solution for them. Some of the typical challenges organizations look to overcome by engaging with an MSSP are:

- Lack of skilled analysts to classify and interpret events in a meaningful way
- Lack of suitable security event correlation solutions
- No desire to invest in an effective in-house function due to significant cost for manpower and technology

There are other options available too. Xia, Ling, and Whinston[2] describe alternative risk management approaches that might be preferable in certain circumstances. They investigate risk pooling arrangements (RPA), a mutual form of insurance organization in which the policyholders are also the owners, and third-party cyber insurance as potential alternative risk transfer vehicles for organizations. While RPAs are more widely used in other areas of business such as the insurance industry or education,[3] cyber insurance is indeed an interesting risk transfer alternative with increasing uptake. The extent of what insurance can typically achieve is limited to reducing the size of the loss when it occurs and, very importantly, if it is indeed identified as such. Taking intangible values like reputation into consideration or increas-

1 Global Risks 2012 - Seventh Edition. Geneva: World Economic Forum – http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf.

2 Xia, Zhao, Xue Ling, and A. B. Whinston. 2013. "Managing Interdependent Information Security Risks: Cyber insurance, Managed Security Services, and Risk Pooling Arrangements," *Journal of Management Information Systems* 30 (1):123-152. doi: 10.2753/mis0742-1222300104 – http://www.uncg.edu/bae/people/zhao/papers/Zhao_Xue_Whinston_ManagingInterdependentInformationSecurityRisk.pdf.

3 Wondon, Lee, and James A. Ligon. 2001. "Moral Hazard in Risk Pooling Arrangements." *The Journal of Risk and Insurance* 68 (1):175-190. doi: 10.2307/2678136 – http://www.jstor.org/discover/10.2307/2678136?uid=3739960&uid=2129&uid=2&uid=70&uid=4&uid=3739256&sid=21104421482391.

ingly stricter regulatory requirements, it is in the interest of an organization to reduce the probability of a breach, not only the size of the resulting loss. Kesan, Majuca, and Yurcik[4] state "…the price of cyber insurance can be tied to the level of self-protection by the insured," which means that the underwriter can impose at least basic security protection requirements in their policies. This in turn requires at least some investment in security infrastructure, making cyber insurance only a complementary method. This is in line with findings by Xia et al. that to make a firm indifferent between using an MSSP and managing security in-house, the service fee of MSSP should be equal to the sum of in-house security investment and cyber insurance premium. Taking this into consideration an organization may decide that an MSSP engagement is the most viable decision.

Identifying suitable candidates

Allocating time and resources to search for suitable MSSP candidates is a cost factor to the organization and forms part of the overall transaction cost of the process; this stage is typically referred to as "searching cost."[5] Leveraging market research groups like Forrester, 451 Group, or Gartner can help to get a quick and cost-efficient overview of the current managed security services market landscape.

Forrester supplies a useful list of criteria to consider for a preselection when looking for a MSSP:[6]

- A complete suite of managed security services
- Sizeable MSS revenues
- Sizeable investment in their MSS offerings
- Large client bases
- Numerous devices under management
- A high number of completed MSS engagements in the past five years
- Significant number of dedicated security operations center (SOC) analysts

The report advises, "As you evaluate the service providers, keep in mind that one size does not fit all for every managed security service. Each service provider offers a unique value proposition and has its own strengths and weaknesses." While this is a good start, additional criteria should be added, depending on the requirements of the organization (e.g., a clearly defined road map/strategy or pre-existing customer relationship with the vendor would be key criteria to consider). Particularly the latter criterion can provide benefits from previous work done with the vendor giving an indication how trustworthy, reliable, and flexible the service will be. It is also

4 Kesan, Jay P, Ruperto P Majuca, and William J Yurcik. 2005. "The Economic Case for Cyber insurance," Securing Privacy in the Internet Age, Stanford University Press (2005) – http://papers.ssrn.com/sol3/papers.cfm?abstract_id=577862.

5 Ding, W., W. Yurcik, and X. X. Yin. 2005. "Outsourcing Internet Security: Economic Analysis of Icentives for Managed Security Service Providers." In Internet and Network Economics, Proceedings, edited by X. Deng and Y. Ye, 947-958. Berlin: Springer-Verlag Berlin.

6 Kark, Khalid. 2010b. "Market Overview: Managed Security Services." Forrester Accessed 2012-03-04 – https://www.forrester.com/Market+Overview+Managed+Security+Services/fulltext/-/E-RES56068.

Donn's Corner

By Donn Parker
ISSA Distinguished Fellow
Silicon Valley, USA Chapter

Limitations of the Need-to-Know

NEED-TO-KNOW IS AN IMPORTANT criterion for allowing access to sensitive information. This means entrusting a collection of information to trusted people that may include giving, reading, printing, copying, modifying, appending, taking, destroying, or controlling rights to specified information within the collection. Historically the need-to-know rule comes from military requirements of giving trusted people only the information necessary to perform their tasks. This is unacceptably restrictive in many business organizations where innovation and broad sharing of business information predominate, making need-to-withhold the better rule. This better rule means giving everybody in the enterprise access to all information except the smaller amount that is sensitive and must be made accessible only to the necessary few.

The restrictive need-to-know rule is used in governmental requirements by classifying information according to increasing sensitivity levels of confidential, secret, and top secret and all other information remaining unclassified or public. Specified people are then given access to each level of information sensitivity by "clearing" (authorizing) them to confidential, secret, and top secret status. Of course, even public information in government and business is sensitive and must be protected from plagiarizing and deceptive modification. I have found that multilevel need-to-know classification does not work well in non-governmental enterprises because of the overhead cost and large investment in security staff to operate the function that is otherwise compensated in government contracts.

Need-to-withhold is a more attractive rule for non-governmental enterprises, allowing access to all information except for sensitive information that is made accessible to only a necessary few. For example, a person at the *high* sensitivity level has access to all information. A person at the *low* level has access to all information except for specified items such as personnel files. And another person has access to all information except for personnel files and certain trade secrets.

In summary, need-to-know means entrusting only information needed to perform a job. Need-to-withhold (the inverse of need-to-know) means entrusting all information except specified, unneeded sensitive items required to be withheld. Need-to-withhold has the advantage of tending to give trusted people the most liberal access beyond just the information to do their tasks. Need-to-know tends to be more restrictive by giving trusted people access to only the information necessary to perform their explicit tasks. Use need-to-know in government and need-to-withhold in non-government enterprise.

All of this is summarized in three maxims:

58. The need-to-know rule: Entrust only needed information.
59. The need-to-withhold rule: Withhold only specified information.
60. If more information is sharable than not, then need-to-withhold may be the better rule.

Donn Parker, CISSP, Retired, Distinguished Fellow, and information security pioneer, donnlorna@aol.com.

expected that cost and time for contract negotiations will be reduced for existing vendor relationships. This can keep the contracting cost, as part of the overall transaction cost, low. For providers that are found to be suitable candidates, a more in-depth evaluation will need to be conducted, based on a wider range of criteria. I will take a look at some selected sources available that can help to plan out a structured review of MSSP candidates, but first I will mention some things to watch out for that I personally found to be important while going through such an exercise.

Vendor personnel

Technical skill set of the individual analysts

Managed security service providers are quick to confirm that their staff consists of highly qualified people, certified according to industry standards. They may present long lists of well-known certifications (e.g., CISSP, GCIA, etc.) that their staff holds, but this has little relevance unless the vendor confirms that this is indeed the staff working on the organization's contract.

What is the turnover rate of SOC staff?

Highly qualified security experts are sought after by many companies, which can lead to high turnover of staff if the MSSP is not actively working on retaining talent. For the customer this has the consequence that there is a constant *new-starter* or *training-on-the-job* process going on that has the potential to cause friction and service degradation.

What are the staff training plans and budgets?

MSSPs, just like any other organization, have to deal with economic challenges and might be tempted to cut budgets for head count and training. This inevitably leads to stress and frustration among employees, causing skill depletion thorough lack of training or staff resignations.

What is the customer-per-analyst ratio?

In line with the previous criteria this is an important metric to understand the level of service that can be expected from the prospective MSSP. If the vendor is stretching its analyst resources too thinly across its contracted customers, the service is likely to suffer due to time and stress issues.

Is security operations center (SOC) staff multilingual?

While focusing on the obviously important technical skills, it is easy to forget that clear and effortless communication between staff on both sides is an important part of the service. Any globally operating organization will find this to be a crucial requirement to avoid misunderstandings between the MSSP SOC and the organization's staff.

Technological capabilities

Is the vendor able to support the organization's technological road map?

Just as much as discussing the vendor's road map, it is important to discuss the organization's technological road map. Main focus tends to be given to the current technolo-

gies in use and the breadth of coverage by the MSSP for those technologies. However, MSSP lead times can be unexpectedly long before they are able to fully support new technologies that an organization may want to adopt. This can have an adverse effect on the organization's security strategy. It is advised to clarify this point early on.

Service Deployment

What overhead is required to deliver the service?

The way in which an MSSP provides its services can vary in terms of infrastructure requirements. Some might require very little modification to the organization's existing infrastructure, while others can only deliver service with considerable effort on part of the organization in terms of additional hardware, software, or communication channels. As pointed out by Ding et al., this can incur sunk cost in infrastructure investments when the organization considers switching its MSSP; it becomes "locked in" from an economic perspective and has to accept the loss or include it as buy out charge in a new MSSP's contract. This obviously not only adds to the setup cost but also has the mentioned knock-on effect for switching cost later in the life cycle.

MSSP selection criteria guidance

There is limited industry or academic guidance to identify relevant and useful criteria for MSSP selection. While there is no shortage of largely commercially focused articles and vendor whitepapers about managed security services, the amount of impartial literature providing actual value to the selection process is found to be rather low.

Professional market research resources

From an economic and market-analysis point of view the approach followed by Forrester[7] is quite useful. It describes 78 individually weighted criteria broken down into 14 sections across three topical areas that aim to assist in selection and comparison of potential MSSP candidates (see figure 1).

The idea to assign a weighted percentage to each topical area, section, and criterion is useful and better suited than assigning simple relevance ratings (High, Medium, Low). Designing an evaluation form using percentage-weighted criteria allows for a more complete list as it can be tailored by assigning low or zero weighting to certain sections or criteria instead of removing them completely. It also allows for swift adjustments during group discussions when various opinions and viewpoints on critical areas of an MSSP engagement need to be considered.

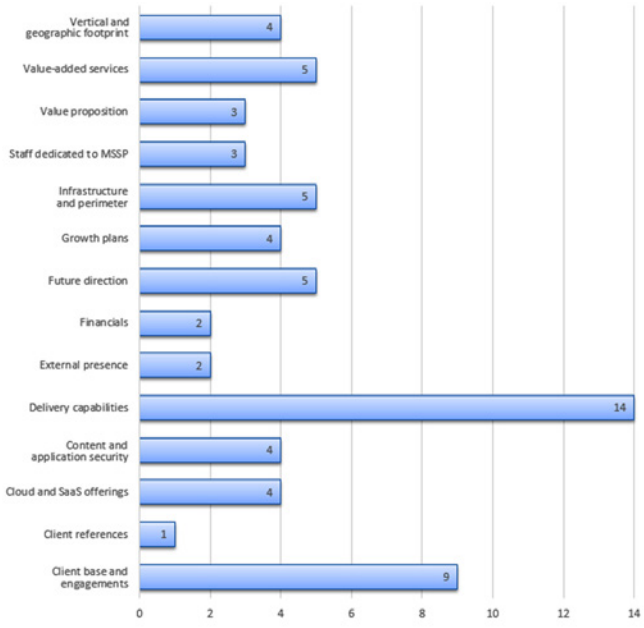


Figure 1 – Selection criteria overview, Forrester/Kark

Independent information security association resources

Guidance by the Information Security Forum[8] is largely focused on details of the actual service delivery. Covering 76 criteria in six key sections (Management, Contractual, Functional, Integration, Security and Resilience, and Additional), the material provides assistance on practical aspects of the evaluated service with a clear emphasis on intrusion detection services. I found particularly the *Functional* and *Management* areas to be a rich source of valuable evaluation criteria.

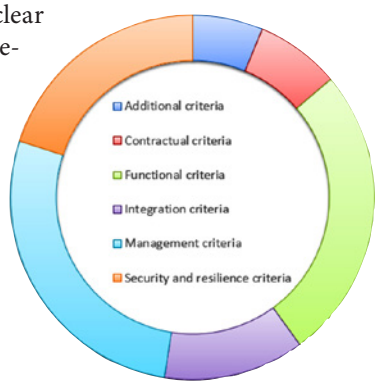


Figure 2 – Selection criteria overview, Information Security Forum

A good example is criterion B3, listed under *Contractual*; it describes the need to understand all parties involved to deliver the service on the side of the MSSP. The risk originating from a vendor's supply chain is often overlooked despite its impact on service quality and risk posture of the customer.

Unfortunately neither of the materials mentioned so far is freely available to the public; distribution is limited to members/subscribers of the Information Security Forum or For-

7 Kark, Khalid. 2010a. "The Forrester Wave™: Managed Security Services, Q3 2010." Forrester, Last Modified 2010-08-05 Accessed 2012-03-04 – https://www.forrester.com/The+Forrester+Wave+Managed+Security+Services+Q3+2010/fulltext/-/E-RES56674.

8 Information Security Forum. 2005. Tool to assess managed security services for intrusion detection. Accessed 2012-03-10.

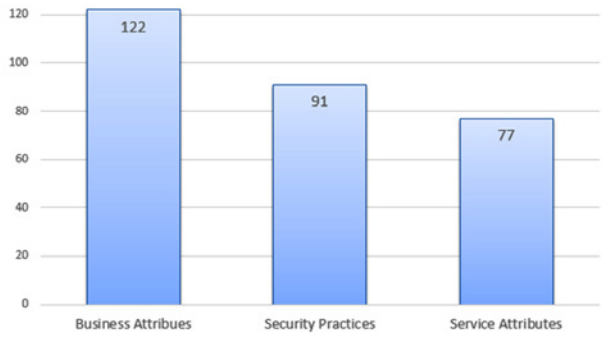


Figure 3 – CMU/SEI selection criteria overview

rester. This is one of the reasons, besides the fact that it is highly valuable guidance, why the remainder of the article will be focusing on the material provided by the Carnegie Mellon University.

Academic community resources

Guidance provided in the document "Outsourcing Managed Security Services"[9] by the Carnegie Mellon University Software Engineering Institute is categorized in four main areas (Engagement, Management, Termination, and Service-specific) with "recommended practices" aligned to each area. These practices are broken down further into attributes and categories providing a rich set of criteria to consider in each phase of the MSSP engagement. The three practices aligned with the Engagement phase carry advice on business attributes, service attributes, case studies, checklists, and security practices that are most relevant in terms of this article and are leveraging the same set of core attributes – Business, Service, and Security.

Categorizing the criteria is not as easy as it was for the previously mentioned sources. This is due to the different scope and nature of the paper; an attempt to harmonize the criteria in top-level categories can be done of course, but it flattens nuances of the SEI research rather crudely. Nevertheless the chart below provides a suitable overview on how detailed the guidance is with its 290 criteria of which several carry multiple sub options (see figure 3).

The business attributes deal with details of how an MSSP implements its business processes and customer engagement, controls itself, and measures business success. The service attributes are going into detail on the service delivery capabilities of the MSSP, providing guidance on important points like availability, scalability, architecture, and scope. The security section aims to ensure that the provider is capable and suited to provide a managed security service to its customers. When engaging with an MSSP, it is easy to assume that vendors adhere to the highest security standards in their own environment and skip over these important checks just because they sell security services. The last thing an organization wants is to outsource its security services management to a vendor that cannot get the basics right for its own environment. Following the "trust but verify" adage, this trap can be avoided.

A brief analysis of key criteria

Due to the richness of the guidance provided, the SEI recommends that "Readers should view all practice guidelines as a baseline checklist from which to choose and create their own set, based on their organization's business objectives and desired security services."

This section will focus on some of the criteria found to be particularly relevant in previous engagements.

Business attributes

Supply chain risk is a prominent topic for most information security teams, even more so if it affects the delivery of security services. The need to fully understand the use of tiered providers (i.e., channel partners, resellers, vendors, subcontractors, and other providers) is emphasized in *Relationships with Other Parties (RO) [P1.1.3]*. For example, criterion RO2 asks, "Where do you plan to use tiered providers to satisfy client requirements?" which is of importance not only for service delivery but also for contractual and possibly regulatory reasons.

Guidance listed under *Independent Evaluations (IE) [P1.1.4]* should be considered as a whole but in particular criterion IE5: "Indicate your agreement to participate in and deliver results from a periodic full security evaluation performed by a mutually agreeable independent organization" stands out. Following a "trust but verify" approach, this is an important part of the vendor relationship. Due to the critical role MSSPs have in the security posture of an organization, a simple certification or audit report (e.g., ISO/IEC 27001), while certainly required and being the absolute minimum, is not sufficient. Regular security evaluations (e.g., penetration tests), where results are shared with the organization, should be made a discussion point in your Request for Proposal (RFP) processes.

To further increase the understanding of the MSSP's security maturity insight into their own internal risk assessment processes, risk review practices and security policies should be requested (cf. IE1 and *Security Policies, Procedures, and Regulations (PP) [P1.3.1]*). An additional point that is not mentioned in the SEI guidance is to request the content of the vendor's risk register, pertaining to the customer, to be made an agenda item for regular service review meetings. This is particularly relevant for information security officers taking over an existing MSSP engagement or in large organizations where multiple stakeholders are involved in MSSP operations.

Key points listed under *Asset Ownership (AO) [P1.1.6]*, like the criterion AO2: "Is all intellectual property created by the provider on behalf of the client and in the course of the relationship owned by the client?" should be clarified to avoid issues later on. This is not always considered but in anticipation of involvement of the MSSP in value added activities (e.g., enhanced security metrics reports, tailored signatures for

9 Software Engineering Institute. 2003. Outsourcing Managed Security Services. Pittsburgh, PA: Carnegie Mellon University – http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6319.

network intrusion sensors or processes for intelligence data correlation in security information and event management (SIEM) solutions), the ownership needs to be clearly defined up front to avoid issues on termination of the contractual relationship. Related to this, SEI provides further guidance on *Exit Strategy (ES) P3.2.9*, highlighting the need to clarify the "destruction and/or return of client proprietary and other sensitive information" (ES2.d). This is again mentioned under *Data Handling (DH2) [P3.4.4],* requesting that "The provider affirms that all client data will be removed from all computers and media that is upgraded, deployed, and retired." While many contracts cover this nowadays, it is worth verifying and including it accordingly.

Service attributes

As mentioned previously, an MSSP's ability to timely support the technological road map of the organization is important. This point is captured in criterion *Service Scope (SP) [P3.3.8],* asking to "Describe 'emerging technology considerations and provisions for replacing, reducing, or adding services based upon technology changes.'" An MSSP that is not staying on top of security technology developments and, in worst case, preventing its customers from using these technologies in their own environment must be avoided. In the *Service Architecture (ST)* section the criteria listed in P1.2.3 and P2.2.3 are of particular value due to their impact on an organization's existing infrastructure. Particularly the criteria P1.2.3 (ST7b): "Are your management tools hardened and secured?" and P2.2.3 (ST2): "The provider adequately demonstrates that clients do not compromise each other's processing environment or data" highlight potential areas of concern about the security of the service architecture. Due to the nature of the concerns these are best aligned with the criteria discussed in the following paragraph.

Security practice

Continuing with the security architecture concerns, there are several criteria listed under the security practice umbrella that compliment this topic. *Secure Asset Configuration (SC) [P1.3.8]* goes into details on how the MSSP should provide proof that asset configuration is mature in terms of security requirement. This includes basic, but important, criteria like SC2: "The provider applies patches to correct security and functionality problems" as well as SC3: "The provider establishes a standard, minimum essential configuration for each type of computer and each type of service, storing this as a trusted base configuration." If you are wondering why you should worry about this, just ask yourself how timely, if at all, your MSSP addressed recent vulnerabilities like "Heartbleed" (CVE-2014-0160) or "Shellshock" (CVE-2014-6271) in its customer supporting environment. Each of these is important, but I feel that they should be seen in conjunction with and formulated as such in an RFP. *Software Integrity (SI) [P1.3.7]* describes requirements on antivirus and file integrity (SI1).

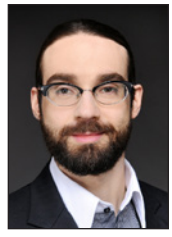
These criteria are further complemented by *Monitoring and Auditing (MA) [P1.3.10],* MA1: "The provider uses appropriate monitoring, auditing, and inspection facilities and assigns responsibility for reporting, evaluating, and responding to system and network events and conditions," ensuring a continual assurance about the state of the vendor's internal security controls.

Lastly, although business continuity (BC) and disaster recovery (DR) are well covered areas in most contractual relationships, one of the criteria mentioned in *Contingency Planning; Operational and Disaster Recovery (DR) [P2.3.2]* is especially relevant in this context. SEI recommends to "Evaluate if the provider has established 'preferred priority restoration' with other clients of their services.'" This is common practice when contracting third-party DR facilities but does not seem to be regularly considered in MSSP agreements. Adversaries are aware that organizations are particularly vulnerable in crisis situations as staff is exposed to heightened levels of stress and focusing on other priorities. This is a welcome opportunity to malicious actors and will be exploited wherever possible. It needs to be clarified and understood what the organization's expectations should be in case of a DR situation as, depending on the restoration priorities of the MSSP, it might have no visibility in terms of security events for a prolonged period of time.

The more you sweat in peace the less you bleed in war

This quote by US General George Patton seems to be a good fit when identifying the best-suited candidate for an organization's outsourced managed security services provider. Finding the balance between a simplified but resource-conserving and extensive but resource-intensive selection process is not easy. Experience shows time and time again that the effort invested during the preparation phase pays high dividends later on when the actual service is delivered without negative surprises. As mentioned earlier there is not a lot of impartial, yet useful, guidance available to support information security professionals in their search for the right MSSP. The few sources I highlighted in this article are all valuable in their own right and, if possible, should be taken into consideration. However, in my view the CMU/SEI guidance is the most exhaustive and useful material available to anyone venturing in this area. I strongly recommend you review the complete report as this article only highlighted a small selection of criterion that I found to be helpful.

About the Author



Daniel Schatz is the Director of Threat and Vulnerability Management for Thomson Reuters, working in London, UK. He holds several qualifications including CISSP, CISM, CEH, ISO27001 LA/LI, and MSc Information Security. He has been one of the organisers of the popular BSidesLondon security conference before stepping down in 2013 to focus on his professional doctorate studies. He may be reached at daniel.schatz@thomsonreuters.com.