Global Information Assurance Certification Paper

SANS Institute – GIAC Security Essentials Certification (GSEC)

Practical Assignment Version 1.4c, Option 1

Submitted by Aaran Tooley

Outsourcing Security: "The way of the future?"

2/15/2005

Table of Contents

Abstract 3

The Growth of Outsourcing Security 3

Reasons to Move to Security Outsourcing 4

Choosing a MSSP 6

- Criteria for the MSSP 6
- Decision Making Guidelines 7

Negative implications to outsourcing security 8

The Scary Truth 10

Conclusion 11

References 13

Abstract

In today's fast paced world, technology is growing at an ever increasing rate. Recent vulnerabilities have shifted focus to security issues; however with the amount of vulnerabilities being uncovered today, security is growing at such a pace many companies are finding it hard to keep up. The need to secure data and resources is ever increasing and in many instances legislatively enforced. Many companies are looking to outsource their security tasks to third party vendors as they are finding they have neither the resources nor expertise. The sudden emergence of outsourcing security work has caused a spark within the IT world. This has lead to many evaluations and surveys on whether companies are putting their confidentiality and integrity at risk when they chose to go through outside means for protection of their assets. Recent surveys have noted that outsourcing of security will reach 90 percent by 2010 (Schwartz). This has alarmed many experts as they are now beginning to discuss the possible implications on our corporate IT world. Studies are currently underway to discover if and how outsourcing security is beneficial to a company. On the opposite end of the spectrum, studies have been conducted to determine the negative impacts of outsourcing a company's security work. This paper will focus on explaining the effects of security outsourcing from both points of view as the decision of outsourcing security is ultimately the company's decision.

The intent of this paper is to present factual information regarding security outsourcing. In turn a reader should feel capable of making informed decisions regarding outsourcing their company's security. It will also provide helpful statistical information that could be used when proposing views on outsourcing security jobs.

The Growth of Outsourcing Security

Outsourcing of information technology jobs has always been around. Many people are aware a large amount of software and application development is outsourced to companies in India and China; however a new wave of outsourcing has appeared on the radar. Outsourcing IT security has recently appeared and, over the last couple of years, this industry trend has exploded. Projections indicate this growth at an even faster pace in the next year.

Security Outsourcing can be handled in many different ways. IT doesn't have a consistent means to it. A company could potentially outsource any number of security tasks or all of them to a managed security service provider (MSSP). A good example is a company could outsource their Intrusion Detection System (IDS) only. A company may want to do this if they are a smaller company that would not be able to adequately provide 24/7 intrusion detection support. Outsourcing this aspect of their security would allow the MSSP to constantly monitor the network and then follow up on any unusual detection in a timely

manner. This could potentially save the integrity of the company by catching anything from a virus to a hacker accessing the network.

Studies conducted in the past year have returned alarming figures in regards to how security outsourcing will grow within the next three to five years. "In 2003, the market for MSSP was about $150 million, and is expected to hit $570 million by 2008" (Schwartz). The growth of security outsourcing is corresponding with outsourcing's cost savings for companies along with the added workloads involved from following new regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley, which are putting more of an emphasis on securing the private information of employees and customers.

Security jobs are in an increasingly higher demand and therefore it is more expensive to pay security IT professionals. This rise in salaries for security IT professionals has forced companies to look out for means of protecting their assets. The state of our economy has played a focus in the rise of outsourcing. Many companies are cutting back in as many ways as possible to survive. Smaller companies are affected more by the costliness to protect their data and coincidently are the area that turns to outsourcing security in most cases. Companies are doing what they must to just stay afloat. MSSP's are able to market themselves to match the company's needs. The marketability of MSSP's is a main reason for their fast paced growth. With MSSP's beginning to show up in the enterprise world, the market for MSSP's could grow by leaps and bounds. "With enterprise needs being addressed, the MSSP market will grow from $2.3 billion in annual revenues this year to $3.7 billion by 2010." (Schwartz)

With all of the growth of security outsourcing, many IT professionals are wondering where all the security IT professional jobs will go. Diane Morello, Vice President in research at Gartner, Inc., says that not all the jobs being outsourced overseas will mean workers are laid off. She says some of the jobs will be created by U.S. Companies opening IT operations in those countries, which will avoid layoffs here by starting new IT programs there. (Gaudin) This will of course involve moving IT workers to where the jobs are located which could result in a shifting of security IT professionals outside of the U.S.

Reasons to Move to Security Outsourcing

As stated in the introduction, the Yankee group is stating that 90 percent of all security will be outsourced by 2010. This is due to companies being unable to keep up with security holes, hacker attacks, and government regulations. Security has become a priority role due to laws like Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act and Sarbanes-Oxley Act. Companies are now accepting the added costs needed to secure their enterprise's assets by turning to outside help.

For many companies, outsourcing their security is a blessing in disguise. Many

small companies rely on these MSSP's for protection from attacks without burdening them with the cost of hiring their own security staff. Security is growing too rapidly for many enterprises IT shops to keep up. There have become too many patches to download, firewalls to watch, and reports to read and analyze. All of these added tasks have many administrators looking for more help. The cost of hiring the technical people for security jobs is now a larger burden on the wallets of companies due to the sluggish economy so these administrators are looking outside to find the assistance they need.

As more companies look outward for their security needs, others are sparked to put their security in the hands of a security provider also. Chris Warner, founder and CEP of E2Citizenship.com said, "We know what we're good at and we know what we're not good at" (Gaudin). Companies are now facing the realization that not properly protecting their assets could lead to destruction of the company as a whole. CEO's and executives have become aware that they need to rely on MSSP's if they want their company to continue to strive and survive in today's world. Chris Warner continues by saying, "We outsourced our security to Symantec because they are good at what they do and they are able to look for problems before they happen. We couldn't have done that" (Gaudin). People are aware that with the new high-tech networks of today, security must be monitored very well. The network needs to stay within tight restrictions. Any sort of variance from the baseline of the systems could mean disaster.

The Yankee Group identified that the increase in outsourcing is due to the fact that many companies are not able to provide the in house quality of security needed was leading to the increase in outsourcing. Outsourcing has become a more accepted idea due to the maturity of our firewalls and scanning services. The clear policies that are now in existence for these tools have made it easier for companies to hand their work over to someone else. Ken Hilving, a consultant with Schooley Mitchell Telecom Consultants, says "One of the statistics often stated is that 80 percent of the security breaches are internal rather than external." (Weinschenk) By moving your security to another company, the risks of the secure data being compromised due to social engineering is reduced. This would reduce the overall threat of compromise to your security systems.

Large companies have also begun to turn to security outsourcing but have made adjustments to the term "outsourcing" which allows them to keep their comfort levels. Grant Geyer, vice president of global management security services for Symantec, said, "A lot of times, especially with large enterprises, you need the expertise of security people who do this 24 hours a day." (Gaudin) Larger companies turn to MSSP's to do the majority of the hands-on work. These companies still keep control of their policies and strategies as well as ensuring they are effectively implemented. These partnerships between large companies and security outsource providers are referred to as "co-sourcing". It is called co-

sourcing because the company still maintains control of the direction of their security strategy but allows another provider to control the day to day tasks. Monitoring the potential millions of daily alerts that come out of a single firewall or intrusion detection system is very people intensive and expensive, which make outsourcing appealing to so many companies.

With more companies deciding to outsource their security services, many organizations have taken a closer look at the outsourcing process and developed and tailored a process to make any CEO comfortable with trusting the security of their network to an outside source. The Banking Industry Technology Secretariat (BITS) have released security guidelines located within a matrix specialized in outsourcing security. This 33-page spreadsheet provides a common set of expectations for companies to rely on when deciding on an outsourcing company. The guidelines were developed by BITS members, vendors, government agencies, and IT auditors. The creation of these guidelines allows for more companies to feel comfortable with turning to outsourcing as an option. The process involved with the completion of the matrix involves asking potential vendors questions during each stage. Risk management, planning, and testing are among the questions asked before deciding to turn towards security outsourcing for your company. An area that has recently been added into the guidelines developed by BITS is business continuity. BITS also encourages companies that are looking at outsourcing their security to take time to understand the procedures of the service providers and if needed write into the contracts provisions that would allow for audits and on-site reviews.

Choosing a MSSP

When the decision has been made to go with a MSSP for your company's security policies it is critical that you choose your provider with caution. There are two main areas that any company will contend with when picking a MSSP. The company must look at the technical capabilities of the MSSP, or the criteria for the MSSP. You must make sure the MSSP can do what you need them to do and that your security will be monitored to the extent you want it. Another area is the business aspect of the MSSP. You will want to follow guidelines when beginning contract negotiations with a MSSP. You want to know exactly who this company is and what they are all about before you hand over your sensitive information to them.

Criteria for the MSSP

The MSSP that your company chooses to go with should maintain adequate operation centers. An MSSP should have multiple locations where they house their operations. Ideally the locations would be dispersed appropriately to handle disasters. The MSSP should be able to keep the 24/7 intrusion detection monitoring functional if one of their locations were to go down. Finding an

MSSP that has locations complimenting yours would be ideal and if you do business internationally, the MSSP must meet all international standards for security practices.

The analysis and response time for the MSSP is crucial to your decision. They must be able to monitor and interpret the network data in real time. The MSSP needs to have the capability to monitor all your data. If a provider does sampling of the data then you will need to continue looking. A MSSP that does not monitor all data is leaving holes in the security of your network. A MSSP needs to be able to analyze company data and respond to breaches in an adequate amount of time.

The knowledge of the MSSP staff is an important aspect for your company to consider. The employees that will be securing your company's network need to meet your standards. Be sure to check into the certifications their security experts have. Look into the number of vendors and technologies they are certified in. It will also be important to guarantee all their top notch workers are not focused on a single shift. If a MSSP is offering 24/7 intrusion detection support then the expertise needs to be at a consistent level throughout all the shifts. This will guarantee that if a problem were to be encountered someone would have the knowledge to correct it during any shift.

Look at the amount of services the MSSP offers. It is vital to the company's security that they will be able to provide all the services needed to stay up with evolving technologies. The top MSSP's today offer complete packages of services. The services offered range from real-time monitoring, firewall management, intrusion detection systems, virtual private networks, and antivirus products.

Decision Making Guidelines

Since security is a mission critical part of any organization's network, outsourcing to another firm could spell trouble if not decided upon well. There are many important things to consider before deciding to trust your company's sensitive data in someone else's hands.

First do some checking; Kelly Kavanagh, a senior analyst from Gartner suggests that the company go and check out the potential MSSP on site and make sure they are a viable organization. She also states that you should get references from the potential MSSP to do some background work (Weinschenk). Some additional ways to research the company is by checking financial statements and the ways the MSSP does business. A good way to find the standing of your potential MSSP against the others in the industry is by reading publications specializing in outsourcing or IT security.

Next you will want to secure a strong service level agreement (SLA) in order to

ensure you are obtaining the service that you desire. The SLA is mission critical to obtaining the level of service your company needs. The company requesting the contract with the MSSP should be sure to keep some aspects of the work in their control. You would, for example, still want the ability to view trouble tickets or event logs in the case that a breach of your system does occur. This way you can observe what is going on in your network in case further investigation would need to occur. The organization also needs to develop regulations of what should be kept in-house and determine they are satisfied outsourcing the rest.

Finally the enterprise would want a final run through to verify that all systems are up and running. This could be done by staging a security breach or outage of the systems. You would then be able to see how the MSSP would react to the problem and what ways they had to resolve it. This final point is a good practice to keep up periodically during your agreement. A way to verify you are getting what you are paying for is to occasionally unplug the system and observe how long it takes for them to react.

Negative implications to outsourcing security

With the recent boom in outsourcing security, many enterprises have taken a step back and asked if this is really something they want to do. Placing the security of your company's data and assets into the hands of another is a huge risk; a risk that some companies are not willing to make. Companies are realizing that the financial savings associated with outsourcing their security is not as much as first thought. Security review and assurance policies are still needed by the company outsourcing their work in order to verify that the contractual work is being completed.

Before outsourcing your security services, administrators need to validate the integrity of the MSSP. Many outsourcing providers are now offshoring the work that they accept. This means that a company could be under the assumption that their security work is being done within the realms of the United States when it is being offshored to India or other countries. Many outsourcing providers for software or application development will offshore their work to India but the same idea is not as widely accepted when it comes to offshoring security work. This is due to privacy standards not being as strict as they are in the United States. For example, in India it is not considered to be an intrusion of someone's privacy if their email is read by another without their knowledge. A story that ran in the San Francisco Chronicle in late 2004 discussed the October 2003 incident that occurred in Pakistan. A Pakistani transcriptionist threatened to release recordings and transcriptions of patients' records onto the Internet if she was not paid for her contract work. (Rash) This story and many others like them show the scary truth of outsourcing security in today's world.

Another topic that companies will want to consider when looking at sending security to a MSSP is the amount of control the company wants to keep within

their realm. Many MSSP's will request to retain full control over the security systems they have been given to keep secure. This is because many MSSP's will have their own tools that they use to manage the security in the network. Their administrative processes could differ from the way the in-house administrators would evaluate the same systems. MSSP's find it easier to reduce the finger pointing if a catastrophe was to occur when they retain full control of the security systems.

One downfall of outsourcing your security to another business is the MSSP does not understand the inner workings of your company. The MSSP does not have the knowledge of your corporate culture and business security policies. It will take extra time to verify the MSSP has the knowledge of your policies in order for it to monitor the security settings properly. There is always the option of allowing the MSSP to provide the professional services to you as well, but like many things, it will come at an extra cost to the company requesting the service.

A huge surprise many companies come to find out when looking into outsourcing to a MSSP is the size of the administrative team. Whereas within the company you may have a small team of three or four employees with full administrative rights to the system, the MSSP usually gives the same administrative accesses to a team of around thirty or more analysts. This means on average ten times more people will have access to your company's systems and will therefore increase the risk of your systems being exposed.

Usually a positive aspect of outsourcing security is the response time of the MSSP in the event of a catastrophe. However, the time that a service provider could take to do a policy change may range anywhere from six to twenty-four business hours. This would require a company to plan ahead for instances where a change would need to be made by the MSSP. In many cases a company will not be aware of a change to policy until it is needed and therefore this timeline could cause an issue. It is important to make sure a SLA is in place that will make policy changes easier for your company when they are needed.

A downfall that many companies don't think about before they decide to outsource to a MSSP is that this is the business for the MSSP. They are in the business in order to get the biggest profit, just like all companies. However when deciding to outsource your security to them, it is something that you may want to think twice about. The preference of MSSP's is to perform as many tasks as possible on a large scale. Customization is more expensive and therefore not preferred to do within the MSSP. If a company had specific requirements that would require customization by the MSSP, it will be either difficult or expensive to do. Since any special requests would break their model and therefore make them less efficient. The amount of work the MSSP can take in and do successfully and efficiently is what makes them their amount of profit. Anything that may deter them from their amount of profit will be highly

discouraged within the MSSP's organization.

The Scary Truth

When thinking about outsourcing security to a MSSP, it is important that a company realize just what risks are associated. The following section is based on the story from Scott Berinato, Security Outsourcing Exposed! On April 25, 2001, Pilot Network Services went out of business and abandoned their 200 customers that relied on Pilot to complete their security. Pilot was not a new company just getting on their feet, they were a well established security provider that had been around for eight years and had nearly 400 employees along with customers that represented many large banks and health care institutes.

When Pilot recognized their demise was coming, they felt lost. Their services were wide open to hackers; the same services that were protecting their customers' networks. In some instances complete web services and office to office traffic through virtual private networks (VPNs) were wide open. The end was so bad that one of their customers sent several of their own employees to Pilot's operation center. This caused fear among many of the other customers because now one of their possible competitors was viewing their sensitive customer data. This is a worst case scenario but is not uncommon. Many MSSP's could experience their downfall as well, especially with the weak economy of the past few years.

The bankruptcy of Pilot affected not only the employees that lost their jobs but also affected the customers of Pilot on a much larger scale. One of Pilot's customers, VisionTek, had been a customer of Pilot's for four years. Just two weeks before their collapse, VisionTek had renewed their contract for a full year. Just after the renewal of VisionTek's contract with Pilot, VisionTek was made aware of Pilot's doom. This meant that VisionTek was not only wide open to hackers and suffering from network inefficiencies, but now they were out a year of paid security coverage from Pilot.

The ripple effect from the collapse of a security provider comes down hard on the CIO, or deciding party from the customer. In the case of VisionTek, the CIO had to explain to the business what happened. She was being held accountable as it was her job to manage the security vendor. If Pilot failed then in essence she failed as well. In this case, contingency was needed and luckily VisionTek had a successful contingency plan in place.

While VisionTek decided to stay with outsourcing and chose another vendor after Pilot's collapse, another ex-customer of Pilot chose to move their security in-house. Peoplesoft decided that security had become too crucial to continue to outsource. Neil Hennessy, VP of IT engineering for Peoplesoft, said, "It's [security] definitely far more expensive doing it in-house, on the other hand, there's far less risk. I'm paying to sleep well." (Berinato)

No matter what the outcome of your company's decision when a disaster strikes your MSSP there are some guiding steps to take to ensure your company handles the disaster well. The first step is to remember to brief the executives once a day. Keeping the leaders of the company informed will guarantee that your organization understands the potential outcomes. The next thing to do is to assign an IT staff member to monitor the MSSP situation. Assigning one of your own employees will ensure that you are receiving the correct information and it is not being sugar coated to make you rest easier. Documenting everything is a way to prepare for any possible legal action. Making sure that all conversations and actions are documented will make sure that your company is ready in case legal steps need to occur. Next would be to prepare a static webpage for you to place sudden outages on. Having a dedicated location for outages will allow check ups to be done in order to monitor the status of the disaster. Finally, negotiations will need to begin with alternative providers. If your company is still looking to outsource, you will need to begin the process of looking for another MSSP. However the option is available for you to move your security in-house instead.

Conclusion

With attacks on networks occurring more frequently now, companies are opening their eyes to the need for tighter security. Executives are opening their wallets to ensure that the integrity of their data is kept. Companies still have an option. They have a decision to make between outsourcing their security and keeping it in-house.

The decision of whether to outsource security or keep it in-house is a critical decision. Outsourcing has proven to work well for many companies, both large and small, however the risk of a security breach is still there. The risk of the security provider having a disaster can occur, whether it is a network or financial disaster. What the company has to ask itself is if they are willing to accept the risk.

Many companies still decide to keep their security in-house. Knowing that staffing a security group is expensive, they feel that the risk is less and therefore worth the added expense to keep the security controls of their data within their walls. These companies prefer to have full control over their security policies. They want to know exactly what is going on with their network and who may be trying to break in. They want to have the knowledge of what kinds of attacks are occurring and therefore have a better understanding of ways to prevent them.

Some key questions to ask yourself that could lead to your decision are: What is the risk tolerance of the organization? What are your budget limits? What are the current capabilities of your security? What are the operational capabilities that you want to achieve? (Weinschenk)

For some companies the decision is clear. Some companies have no choice due to their budget and size. Neither option is the clear cut winner; it is all a matter of choice. The decision is not up to the IT staff though, in these cases the decisions are made by executives. It is important that the executives understand the pros and cons of their decision. Their decision will have a ripple effect throughout the company. The deciding parties need to feel that their decision is supported throughout the company. This choice, when it is made, needs to be one that will let everyone sleep easier at night knowing that the security of their company is safe and guarded.

References

Berinato, Scott. Security Outsourcing Exposed! (Online) Available <http://www.cio.com/archive/080101/exposed.html> 1 August 2001.

Brenner, Bill. Firms to Seek More Security Help from Outsiders (Online) Available <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1002085,00.html> 24 August 2004.

Campbell, Bill. Security Outsourcing Taking Hold in Power Industry. (Online) Available <http://enterprisesecurity.symantec.com/industry/power/article.cfm?articleid=3236&EID=0> 15 January 2004.

Danahy, Jack. "Does secure outsourcing exist." SC Magazine June 2004: 70.

Gaudin, Sharon. Gartner: 1/4 of U.S. IT Jobs Offshored by 2010 (Online) Available <http://www.internetnews.com/dev-news/print.php/10792_3331751_2 > 26 March 2004.

Gaudin, Sharon. IT Burden Forces Security Outsourcing (Online) Available <http://www.cioupdate.com/trends/article.php/11047_3348561_2 >3 May 2004.

Hulme, George V. Outsourcing: Not When It Comes To Security, Most Say (Online) Available <http://www.informationweek.com/shared/printableArticleSrc.jhtml?articleID=22103494> 5 July 2004.

Mearian, Lucas. Bank group offers guidelines on outsourcing security risks (Online) Available <http://www.computerworld.com/printthis/2004/0,4814,89381,00.html> 26 January 2004.

Rash, Wayne. Outsourcing can bring on security migraines (Online) Available <http://www.infoworld.com/article/04/04/02/14secadvise_1.html> 2 April 2004.

Schwartz, Mathew. Yankee Group Says Security Outsourcing Set to Explode (Online) Available <http://www.esj.com/news/print.aspx?editorialsID=1112> 8 September 2004.

Weinschenk, Carl. Weigh the risks before outsourcing security (Online) Available <http://techrepublic.com.com/5102-6298-5029745.html> 31 March 2003.

Zhen, Jian. MSSPs Part 2: Reasons to be wary - Seven shortfalls of outsourcing security (Online) Available <http://www.computerworld.com/printthis/2004/0,4814,98114,00.html> 9 December 2004.

Zieger, Anne. Outsourcing Goes Mainstream - The Risk May Be Worth it (Online) Available <http://www.nwc.securitypipeline.com/howto/showArticle.jhtml?articleID=21600064> 10 June 2004.