Outsourcing/Off-shoring IT Security: Is It worth the Risk?

Wil Rodriguez

East Carolina University

Enterprise Information Security 4040 Section 601

Dr. Lunsford & Mrs. Boahn

April 13, 2015

Abstract

Information Technology (IT) companies are always trying to improve and streamline business processes to increase customer satisfaction, while decreasing operational and infrastructure costs. One of the growing trends for U.S. IT companies is to outsource certain job functions or all IT related functions to another IT company within the U.S. The other trend is off-shoring jobs and or IT related functions to other countries such as India. However, some of the IT functions that are either outsource or off-shored pertains to IT Security, where it encompasses Intellectual Property (IP). Furthermore, IT Security services such as firewall and configuration management, monitoring, and IT security jobs are also outsourced or off-shored. For this research, the disadvantages and advantages to outsourcing or off-shoring IT Security will be discussed, along with the risks involved and choosing what aspects to IT security should be considered for outsourcing and off-shoring.

Keywords: outsourcing, off-shoring, IT, security

The terms outsourcing and off-shoring are sometimes used simultaneously, however, each term is different when it comes to location and worker selection in any industry, specifically in IT Security (Schmidt and Jones, 2015). When a company outsources business functions or jobs, it typically involves third-party workers to provide or perform business tasks that were once done by internal employees. On the other hand, off-shoring occurs when a company decides to shift some or all of their services to another county (Schmidt and Jones, 2015). Regardless of which method companies decide to pursue whether to outsource or off-shore tasks or jobs, one of the commonalities is to save short-term and long-term costs. Outsourcing is a common practice most often found in shipping and medical. For instance, most companies rely on shipping services such as United Parcel Service (UPS) and FedEx to transport their products either locally or internationally. In other words, instead of using internal employees to ship the products, companies depend on UPS and FedEx because it may be more cost effective, secure, and reliable. The same applies to medical services. Companies may not have the means to provide in-house medical services, however, they provide health insurance so their employees can be treated by a doctor of their choice. Outsourcing and off-shoring also applies to IT Security, where companies hire other IT companies to manage and or operate their security infrastructure.

According to Schneider (2002), "Outsourcing security has a lot in common with another vital service—medical care—that we regularly outsource and literally trust with our lives" (p. 20). Schneider's comparison with security and medical care highlights the importance of both services where outside resources are trusted for support and guidance, after all, every company needs security just like everyone needs medical care. Each company may have specific reasons as to why they would outsource or off-shore their IT Security, but financial is usually the main reason. Per Schneider (2002), "The primary argument for outsourcing is financial: a company

can get the security expertise it needs much more cheaply by hiring someone else to provide it" (p. 21). When a company needs IT Security, they would need to post open positions, interview candidates, select a candidate, and possibly perform background and credit checks before making the hiring official. One can assume this may involve a long and costly process for each company to endure for each IT Security position. Furthermore, depending on the requirements, companies may have to hire more than one IT Security position to monitor and secure the security around the clock. Consulting companies like VeriSign can offer the expertise and manpower to provide the IT Security a company would require, therefore, eliminating the need for the company to hire and train IT Security personnel (Schneider, 2002. P. 21). For example, a consulting company can have a fully staffed operation center where they can monitor a company's security infrastructure and take remedial actions if needed. Outsourcing IT Security not only applies to businesses, but it may also apply to home security networks. According to Feamster (2010), most home users do not know how to properly secure their home networks. Offering a service to manage home networks will remove the burden from home users of having to secure their networks. In most homes, there is not likely an IT Security person who may know how to manage, operate, and secure a network. Feamster mentions network switches in households that can allow remote management in order to manage home networks (2010). The same concept applies to businesses but at a larger scale in which devices will be placed on premises that would allow outsourcing security companies to monitor and manage their client's network. With the increase of personal devices, smart TV's, and smart appliances, there is also an increase of security vulnerabilities and poor network management, which may lead to undesirable results due to poor manageability.

Although outsourcing IT Security may have its advantages, there are some disadvantages, which leads to risks for organizations that may choose to outsource. In a research conducted by Oladapo, Zavarsky, Ruhl, Lindskog, & Igonor (2009), outsourcing IT Security has the potential to introduce the following risks: compliance with legislation, impact of sensitive breaches, compromise to confidentiality, integrity and availability of information and information systems, reverse incentive, and organization level of IT security maturity (p. 457). When companies decide to outsource their IT Security, they may not have complete control of the desired outcome even though there are expected service level agreements. For example, the integrity and availability of information and information systems are at the hands of the outsourcing organization. In addition, companies have to totally trust that the data confidentiality is maintained at all times, if not, there could be legal implications, which will fall out of compliance with legislation. There are government agencies in North Carolina such as Department of Public Safety, where by FBI-CJIS (Criminal Justice Information Services) prohibits information systems to be outsourced due to the nature of the data and the compliance of federal government. Therefore, it is crucial for organizations to decide what exactly can be outsourced when it comes to their IT Security. In addition to risks involved with outsourcing, there are also risks when off-shoring IT Security to another country outside of the U.S. One of the risks is the intellectual property. In fact, "A survey by IDC of U.S. executives concerning offshore business models revealed "unknown legal rights" to be among their top concerns" (Frank, 2005. P. 60). Each country may have different laws and regulations when it comes to handling intellectual property. In an example provided in the article, there was a case in which one of the software developers in India for a U.S. based company was discovered to have sent files and source code to a personal Yahoo e-mail account (Frank, 2005. P. 60). Furthermore,

when the U.S. company proceeded with legal actions in India, the local police did not investigate.

Organizations face difficult business decisions every day, however, deciding what exactly to outsource when it comes to IT Security can be difficult and unclear due to many changing laws, regulations, and internal company policies. There is one aspect of IT Security that is favorable for outsourcing and that is security monitoring with the use of anonymized logs. According to Zhang, Borisov, & Yurcik (2006), as security monitoring gets more complicated and more sophisticated, the demand for outsourcing security monitoring to Managed Security Service Providers (MSSPs) has increased. Zhang, Borisov, & Yurcik (2006), further explain how MSSPs have the necessary skilled security professionals and security infrastructure that is shared across multiple organizations that allow them to correlate attacks and provide more effective responses. However, not all companies decide to use MSSPs due to the sensitivity nature of their intellectual property. MSSPs infrastructures are shared among other organizations, which poses a risk since sensitive data can be leaked to competitors. Therefore, companies take the risk of consuming the cost of hiring their own IT Security staff (Zhang, Borisov, & Yurcik, 2006). In order to comply and maintain the confidentially, and protection of intellectual property, a solution proposed by Zhang, Borisov, & Yurcik (2006), anonymizes the data from the security logs before the data arrives at the MSSPs. In other words, any sensitive data pertaining to the company is removed from the security logs. The figure (figure 1) below is the proposed architecture by Zhang, Borisov, & Yurcik (2006). In figure 1, all the security logs are sent to a local server where all sensitive information is removed before the data is sent to the MSSPs. Once the security logs reach the MSSPs, the MSSPs responds with a security status based on the information they received. The practice of removing sensitive information is

common among systems administrators. For example, when opening a support request with a vendor, it is a common practice for the customer (client) to remove any server/system name and IP address to hide the identity of the system just in case information sent to the vendor were to leak.

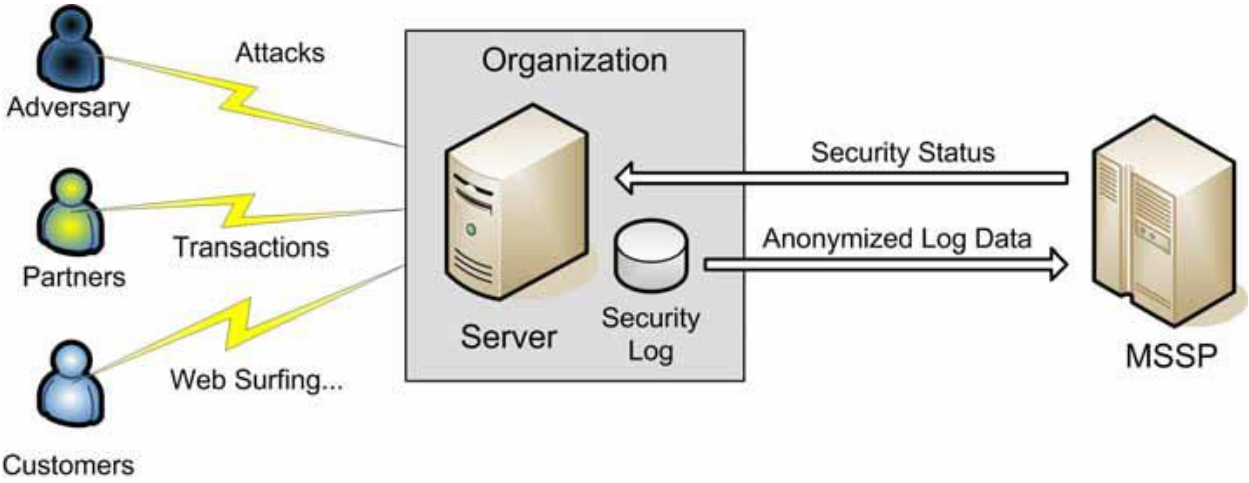

Figure 1

Whether outsourcing or off-shoring IT Security is risky or not, it really all depends on the organization. What may be deemed as a risk for one organization, the same risk may not apply for another organization. Not all organizations have the means or budget to hire a IT Security staff to monitor and operate their security infrastructure, therefore, are left to outsource or off-shore their security requirement elsewhere to alleviate the costs, all while increasing their security need. On the other hand, the risks of outsourcing or off-shoring are far greater than the risk of cost when it comes to their intellectual property. Intellectual property may be too valuable and highly sensitive, therefore, the risks are too great. Organizations may want complete control of their security infrastructure and would rather hire their own IT Security staff regardless of the costs involved to protect and secure their information and information systems. Either way, whether organizations decide to outsource or off-shore, or take a hybrid approach where only their security log management is outsourced/off-shored, not all IT Security is the

same. Furthermore, not all MSSPs or consulting companies are created equal. The decision and risks involved to outsource or off-shore IT Security is in the organizations control.

References

Feamster, N. (2010). Outsourcing home network security. In *Proceedings of the 2010 ACM SIGCOMM workshop on Home networks* (HomeNets '10). ACM, New York, NY, USA, 37-42. doi:10.1145/1851307.1851317 *

Frank, S. J. (2005). Source out, risk in [offshore software development]. *Spectrum, IEEE, 42*(4), 60-62. doi:10.1109/MSPEC.2005.1413734 *

Jianqing Zhang, Borisov, N., & Yurcik, W. (2006). Outsourcing security analysis with anonymized logs. Paper presented at the *Securecomm and Workshops, 2006,* 1-9. doi:10.1109/SECCOMW.2006.359577 *

Oladapo, S., Zavarsky, P., Ruhl, R., Lindskog, D., & Igonor, A. (2009). Managing risk of IT security outsourcing in the decision-making stage. Paper presented at the *Computational Science and Engineering, 2009. CSE '09. International Conference on, , 3* 456-461. doi:10.1109/CSE.2009.95 *

Schmidt, S., & Jones, A. (2015). What Is the Difference between Outsourcing and Offshoring? Retrieved March 14, 2015, from http://www.wisegeek.com/what-is-the-difference-between-outsourcing-and-offshoring.htm#didyouknowout

Schneier, B. (2002). The case for outsourcing security. *Computer, 35*(4), 20-26. doi:10.1109/MC.2002.1012426