Global Information Assurance Certification Paper

Why Are Companies Outsourcing Security?
Deidre Perkins-Moore
November 29, 2001

How important is security to businesses? Most business executives say that security is high on their list. Unfortunately some companies are not spending the amount of money for security necessary to adequately protect them. Even though the Internet is full of potential threats, many businesses are opting to set aside security and focus on their core product. Haven't you heard the statement, "Let's just overlook this so that it will not stop production"? As a matter of fact, I just heard it today. Setting aside security is just fine, right? Out of sight out of mind, until the company gets hit with something major like the 'I Love You' virus. Then they try to scurry out and obtain protection and security expertise and possibly spend a great deal more money than if they had made the expenditure up front to have the appropriate security infrastructure. In the article "*How Secure Are you*?" Mark Lobel, senior manager of technology risk services for PricewaterhouseCoopers, which fielded the *InformationWeek* Global Information Security Research study, states "*A small security review up front might cost $100,000, while an emergency response to an incident after the fact would run $350,000 to $500,000.*" [Breidenbach]

E-businesses are ever increasing. Many of these companies have no established base of expertise.[Strugnell] An E-business, cannot afford to have any downtime on their web sites. If a site is not available, a competitor site is just a click away. To ensure that the sites are up at all times, a company would need to employ network people, security people, database administrators who are available on a 24x7 basis. However, finding and retaining security personnel has been difficult for many companies. According to an article published in *Information Week*, Allan Paller, research director for the Sans Institute, stated, *"The biggest problem in security is the lack of trained security people,"* Paller says. *"Some 2.3 million machines are being attached to the Internet each month, and each of them is full of holes that need to be fixed.*"[Breidenbach] If a company were successful at finding and hiring security expertise, it would become extremely expensive to retain them. What other options do companies have?

Establishing and maintaining a security infrastructure can be expensive. So how can these companies resolve the security holes? Do they seek out and employ security personnel? As the Internet population increases so do the security threats. However, the pool of security resources has not increased at the same speed as the threats. I did a search on Dice.com for security job openings in California and the search engine returned 4952 matches. Then I narrowed my search to just Sacramento, California, and received 58 matches. (Later I will show this bit of information to my boss).

Many companies are addressing the shortage of experienced security personnel by outsourcing their security needs. There are a wide range of affordable security services offered from a variety of vendors. MSPs (managed service providers) are offering services such as virus scanning, managed firewall and VPN services, vulnerability scanning, security policy development, and general security consulting. Depending upon an organization's security requirements, they may opt to outsource anywhere from anti-virus to network perimeter protection services. These MSPs are defined by their promise to deliver not only outsourced applications but also infrastructure management and other value-added processes. [Moore]

MSPs are becoming quite appealing to companies that want to focus their resources and efforts on their product, not security or technology. MSPs are also appealing to startup companies or companies with budget and staffing constraints. Computer security is a never-ending process of maintaining, training, and upgrading and diverts the energy of a company away from its core work. Therefore, more companies have started looking outside for help.[Salkever]

Some companies may struggle with giving outside entities access to their critical data and business information. How secure are these MSPs? Most MSPs go through great lengths to ensure

that they can offer a secure service by constantly reassessing and improving their services. It is the MSPs responsibility to secure their customers' data. If the provider's security is breached then the MSP would most likely be out of business.

Due to their focus on security, MSPs are generally able to operate in a "proactive" mode as oppose to a "reactive" mode that many internal IT shops do. Security personnel for MSPs are continually exposed to the latest hacks, challenges and other security issues. Internal IT staff are typically understaffed and do not have the luxury of operating in a proactive mode. Many times internal IT staff are implementing solutions to resolve a current security issue, as opposed to implementing solutions to ward off potential vulnerabilities. MSP security techs are able to concentrate their focus on security, which enables them to resolve security issues quicker. In the same *InformationWeek* article, Kurt Ziegler, chairman and CEO of eBSure Inc., a software developer that uses the provider RIPtech for its network perimeter protection, states, *"We benefit from what RIPtech learns about all the incidents across its broad customer base."*[Breidenbach] Instead of investing in hardware and software to support a secure infrastructure, many companies are turning to MSPs

More and more companies such and ISS, Network Associates (myCIO), and Genuity are joining the managed services business with companies such as RIPtech, Intira and DefendNet. The International Data Corporation estimates the managed security market will grow to $2.24 billion in 2003 from $512 million in 1998.[Andress] You might ask yourself which MSP is best for me or where do I start. Do I choose a company that offers Intrusion Detection services (IDS), or 24/7 firewall management and monitoring?

Table 1 Subset of vendors that offer varying managed security services.

Provider	**Security Services**
Genuity	Firewall, VPN
Intira	Entire security infrastructure 24/7 management
ISS	Firewall, IDS, VPN, viruses, Web and URL filtering Strong Authentication, router management, vulnerability scanning
MyCIO	Firewall installation monitoring and management, virus scanning and management
Sprint	Firewall, Internet utilization reports
DefendNet	Security Admin, monitoring and reporting, network management
Exodus	Vulnerability detection, host protection, incident response
Counterpane	IDS, firewall and IDS log monitoring
RIPTech	Entire security infrastructure 24/7 management, security policy development, assessment and auditing, penetration testing, incident forensics, and response

If your company is considering outsourcing their security management, develop a detailed description of your company's security requirements. **Table 1** displays a sampling of vendor and some of the security services that they provide. Would your company need network perimeter monitoring and management, on going anti-virus protection, vulnerability assessments, or general security consulting? And, how much control would your company want to maintain? Does your company already have a security policy in place? Your company's security policy could be used to assess the compatibility of the prospective vendor's security infrastructure.

Table 2 According to IDC, factors driving businesses to adopt the ASP model [Strugnell]

• Proven benefits of outsourcing, including the ability to reduce costs, focus on the business instead of technical issues, and break free from the ever-increasing pace of upgrades
• Limited access to IT expertise and other resources required for implementing large-scale applications
• Growth of e-commerce and other new technologies in which the company has no established base of expertise
• Advances in networking technology that make the networking component of using an ASP more reliable and more affordable
• Global market expansion, which puts a premium on the ability to respond quickly to change

Table 2 lists some factors driving businesses toward application outsourcing to an application service provider (ASP). The ASP model is similar to the MSP model in that the responsibility of the application or service is passed on to a provider. Why are companies outsourcing security? In just about any industry, outsourcing can be the quickest and least expensive, yet secure approach to marketing their product on the Internet.

References:

[Andress] Mandy Andress and Brian Fonseca, *Outsourced Security: Consider it Carefully*, Infoworld.com

[Boyd] Jade Boyd, *Cradle to Grave Site Management*, Internet Week

[Breidenbach] Susan Breidenbach, *How Secure Are You*, http://www.informationweek.com/800/security.htm

[Briere] Daniel Briere and Beth Gage, *Getting your Managed Security Wake-Up Call*, The Edge, 06/21/00

[Dice] http://www.dice.com

[Harrison] Ann Harrison, *Let Your ISP Scan for Viruses*, Computerworld, 09/21/99

[Intira] http://www.intira.com/home/news/press_analyst.html

[ISS] http://www.iss.net/securing_e-business/sec_management_sol/managed_sec_serv/index.php

[Kontzer] Tony Kontzer, *MetaSeS Unveils Security-Service Plan,* InformationWeek, 8/17/00

[Moore] Cathleen Moore and Jennifer Jones, *Corporations Lured by Managed Services*, InfoWorld.com 09/25/00 http://www.infoworld.com/articles/hn/xml/00/09/25/000925hnnplusi.xml

[Pappalardo] Denise Pappalardo, *Genuity Pushing Managed Security Bundles*, Network World, 07/03/00

[RIPTech] http://www.riptech.com/more/index.html

[Salkever] Alex Salkever, *Why Internet Security Systems' Stock Could Be a Safe Be*t, Business Week Online, 04/24/00

[Strugnell] Anne-Christine Strugnell, *Tracking the Trends: IDC on Outsourcing*, http://www.oracle.com/oramag/profit/00-Feb/p10idc.html

[Weil] Nancy Weil, *An ASP to Protect Your P*C, IDG News Service, 01/31/00

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event