Industry Profile #1:

Acquisition and Procurement Risk in the Cybersecurity Industry

DeBora King

CSIA 350 7980

Cybersecurity in Business and Industry (2172)

February 19, 2017

University of Maryland University College – Spring Semester, 2017

Introduction

The skyrocketing cybersecurity industry continues to soar. Founder of security advisory firm SSP Blue, Hemanshu "Hemu" Nigam, reports that the global cybersecurity market is expected to be worth $170 billion by 2020 (Morgan, 2015). Increased product demand for security analytics, like SIEM tools, threat intelligence and mobile and cloud security is on the rise. Cybercrime is becoming more sophisticated and is a big component of expenses surrounding the Internet of Things (IoT). The industry of finance has become more dependent on cybersecurity to deliver automated services to stay competitive. Consumer and commercial vehicles require a higher demand of security because as they are more equipped with technology, they are more vulnerable to hacking. The insurance industry is exploding in the cybersecurity sector. Security awareness is needed across the board, so the need for training is increasing. The cybersecurity industry benefits society because nearly every consumer has access to a digital device or tool that connects them to information and resources. But with this convenience comes vulnerabilities, and this is where cybersecurity is essential to consumers. Consumers purchase hardware, software, mobile devices, automobiles, and appliances (among other things) with the assumption that the product is functional (as advertised), reliable and safe. They buy software or services, including cloud services with these same assumptions. Businesses, government entities, and other organizations need to obtain cybersecurity related products and services for one or more of these objectives: to increase capital, to stay competitive, and/or to maintain their credibility.

Analysis

Operational Risks

How operational risk affect the security posture (integrity) of products and services. An operational risks overview section in which you provide an overview of sources of operational risks which could affect suppliers of cybersecurity related products and services and, potentially, compromise the security of those products or services. Discuss the potential impact of such compromises upon buyers and the security of their organizations (risk transfer).

Manufacturing

Rick Schreiber is a partner and National leader of the Manufacturing & Distribution practice and National Association of Manufacturers (NAM) board member. Schreiber states that manufacturers are trying to get caught up to making sure their data, consumers, products and factory floors are secured (Hunter, 2016).

Hardware

When a Japanese division of McDonalds decided to do a promotion with MP3 players in 2006, something went very wrong. The restaurant chain had selected 10,000 winners to receive 10 loaded songs on devices that they picked out from a catalog. Unfortunately, these devices were loaded with QQPass malware that logged keystrokes, passwords and personal data when users connected them to their computers (Singer, 2015). Apparently, a factory worker from the production line injected the Trojan horse into the devices. This is an alarming incident that is becoming more sophisticated. What's more alarming is microchips. They reside in countless devices, such as cell phones, many household items, airplanes, and even military equipment (i.e. missiles). The following vulnerabilities can be undetected when it comes to malicious penetration inside hardware products (such as chips and devices) upon being built: the device

could be set up to trigger as follows: on a particular calendar day; within certain data set up by the attacker; when the device reaches a certain destination (given a GPS indicator by the attacker); a specific time to stop services (overt attack); or a backdoor attack to access the system at a point in time. The problem with these attacks is that users may know that there's an issue but may never be able to identify the cause. On a minor scale, some users may chalk it up to the fact that it is merely an inconvenience. On a large scale, microchip and device hardware attacks can be a global catastrophic nightmare, as it is impossible to alter chip hardware once it departs from the factory.

Software

Although malware can be built into microchips and hardware devices at the manufacturing stage, software can also be maliciously altered in the developmental stage. Each year Open Web Application Security Project (OWASP) lists its top 10 application security risks. Many of these risks can endure tampering through the developmental stage. OWASP's security risks associated with software applications are as follows: 1) third party entities can inject code in small quantity to deceive an application; 2) a genuine user ID can be set up to be accessed through broken authentication and session management; 3) a malicious site can be set up using cross-site scripting (XSS); 4) when the system neglects to protect one user's information from another with insecure direct object references; 5) misconfiguration which could happen at any stage of the software development process; 6) improper display of sensitive data that should not be exposed 7) when users are allowed access outside the realm of their level (referred to as missing function level access control); 8) setting up a malicious sender request disguised for legitimate, trusted credentials; 9) improper or lack of control of open source software; and 10) redirects and forwards that are not validated (Blier, 2016).

Data Center

InfoSecurity identifies five threats that make data centers vulnerable as follows:1) DDoS attacks; 2) Web application attacks; 3) DNS infrastructure exploits; 4) SSL-induced security blind spots; and 5) Brute Force Attacks – weak authentication (Cross, 2014).

Telecommunication Systems

Many vulnerability issues surrounding telecommunication systems have to do with regulation not being in line with the evolution of communication security threats. Protocols is another factor and as new generations surface, the importance of security will be much more prevalent (Mitnick, n.d.).

Product Liability

With cybersecurity issues being so new, product liability in the green industry requires more research and information sharing. Dan Geer, a researcher, was the keynote speaker at Black Hat/Def Con in Las Vegas, and he discussed having the government obtain detailed documentation of companies experiencing computer breaches and he also feels that vendors involved in product liability suits should be exposed if they do not reveal the source codes to consumers who have experienced bugs resulting in their losses (Menn, 2014). When users are privy to how they are protected (or not), they can make informed decisions about how to protect themselves upon making a decision to purchase a product or service. A product liability section in which you provide a summary of the current legal environment as it pertains to product liability in the cybersecurity industry. Discuss the potential impact upon buyers who suffer harm or loss as a result of purchasing, installing, and/or using cybersecurity products or services.

Risk Transference

The key to transference of risk in the cybersecurity industry is transparency. An article from the State of Security recommends best practices for risk transference as follows: 1) each party having a clearly defined responsibility; 2) having auditing provisions while meeting regulatory compliance; 3) assessing compliance that follow laws, regulations and policies; and 5) having actions planned and prepared for disaster recovery (The State of Security, 2016).

Governance Frameworks

Just as years ago, financial institutions were deemed too big to fail, this is the case for digital vulnerabilities across the globe. We have probably all yet to see the fallout of our biggest threat to consumers, businesses, and government – not just locally, or nationally, but on a much bigger global scale. For this reason, governance is of the utmost importance. One such organization of guidance and a good start to organizations refining their infrastructure is the National Institute of Standards and Technology (NIST). There must be a chain of management, a clearly defined work culture, training and awareness of vulnerabilities, and risk mitigation plans with a continuous ability to keep in line with advanced technology (Binwal, 2015).

Risk Mitigation Strategies

Building a risk management program insuring that executive management is on board, involved and informed is a good start to a risk mitigation strategy. Roles and responsibilities clearly defining who is responsible for what is also important. Assets should be defined and vulunerabilities should be assessed and documented. Security controls should be put in place along with policies and implementation plans. As stated above, security awareness is imperative. In addition, “lease privileges” access must be put into action. For operational risks, monitoring, controls, and logs, must be continually assessessed and maintained. Contingency plans must be

in place. For insecurie SDLC risks, risk analysis, defining key guidelines, building a threat model, and documenting misuse cases is important. Secure code reviews, security testing and penetration testing will also adie in mitigating risks in this area. Deterrance, detection and investigation of physical assets is another risk mitigation. A key component that may often be forgotten is vetting third party vendors, business partners and organizations where operations and processes are outsourced. Insuring that the business policies of third party vendors are in line with your organization can be a saving grace.

Summary and Conclusions

Risk Profile

The cybersecurity industry is not only here to stay, but the explosion of consumer demands coupled with technology advancement, not only in business and industry but cyber criminal behavior just makes it more prevailant. Therefore, consumers, businesses, and government entities are continually trying to keep up with the evolution of supply and demand. Corporations are charged with producing new products and trying to stay competitive. The must also maintain the level of integrity that comes with continued growth in the industry. Consumers require that a product is of good use as advertised and in order for companies to deliver, they must follow certain protocol to insure that product delivers as promised. In the cybersecurity industry, however, products may be compromised in the midst of end to end development. In that case, who is responsible? Suppliers must be held accountable for their responsibility to the consumers and therefore must assume risks involved with insuring a wholistic, trustworthy product. Transfer of risk is up and coming in the cybersecurity industry. As the cybersecurity industry grows, risk insurance will be able to measure data associated with vulnerabilities. Risk mitigation and governance frameworks can be the backbone of delivering a reliable product.

References

Morgan, S. (2015, December 20). Cybersecurity market reaches $75 billion in 2015; expected to reach $170 billion by 2020. *Forbes*. Retrieved from http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#595d3c3e2191

Villasenor, J. (2011, May 4). Ensuring hardware cybersecurity. *Brookings*. Retrieved from https://www.brookings.edu/research/ensuring-hardware-cybersecurity/

Hunter, K. (2016, June 21). Cybersecurity jumps to the top of manufacturers' biggest risks. BOD. Retrieved from https://www.bdo.com/news/2016-june/cybersecurity-manufacturer-risk

Singer, P.W. (2015, February 17). Hacked hardware could cause the next big security breach. *Popular Science*. Retrieved from http://www.popsci.com/nowhere-to-hide

Blier, N. (2016, July 15). OWASP Top 10: application security risks. *BlackDuck.* Retrieved from http://blog.blackducksoftware.com/owasp-top-10-application-security/

Cross, K. (2014, November 18). The top f data center threats you need to know. *InfoSecurity*. Retrieved from https://www.infosecurity-magazine.com/opinions/the-top-5-data-center-threats/

Mitnick, K. (n.d.). Telecom Security System. *University of Cambridge*. Retrieved from https://www.cl.cam.ac.uk/~rja14/Papers/SE-17.pdf

Menn, J. (2014, August 11). Government action, insurance software product liability urged for cybersecurity. *Insurance Journal*. Retrieved from http://www.insurancejournal.com/news/national/2014/08/11/337207.htm

The State of Security. (2016, January 5). More executives turn to cyber risk transfer. *Tripwire*. Retrieved from https://www.tripwire.com/state-of-security/security-awareness/more-executives-turn-to-cyber-risk-transfer/

Binwal, P. (2015, June 29). Creating a cybersecurity governance framework: the necessity of time. *Security Intelligence*. Retrieved from https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time/

Cyber security risk mitigation checklist. (n.d.) *National Rural Electric Cooperative Association*. Retrieved from

https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Documents/CyberSecurityRiskMitigationChecklist.pdf