Luke Glayat

Professor Smith

FINC 385

25 April 2015

A Half Remedy For Cybercrime

As increasing rates of cyber terrorism in the past decade scare corporations and individuals, many question the methods of risk management to prevent such a threat. In response to a recent influx of crime ware and other sorts of hacking technology, more and more insurance companies are offering cyber insurance, which is also known as cyber liability insurance. As of now, cyber insurance is generally accepted to be the most effective method of protection from any sort of cyber crime aside from proper risk management. Around 50 plus companies in the U.S. now offer cyber insurance and the first secretary of Homeland Security, Tom Ridge, has founded a cyber insurance product recently as well.

Although cyber terrorism has more recently become a larger issue, other forms of simplified cyber insurance existed for companies that needed a limited range of coverage. Around 20 years ago Errors & Omissions Insurance (E&O’s) was sold to technology companies for issues not very common today such as a simple virus. Since then it has evolved, along with our technology to meet our needs. Companies with a large amount of data from consumers also felt unprotected as their Internet security needs became realized. A cyber insurance article written by Lauri Floresca states “Cyber coverage can mean different things to different people. Most commonly, cyber coverage is some combination of four components: Errors and omissions, media liability, network security and privacy.” (Cyber Insurance 101)

These four elements cover the broad spectrum of what cyber insurance currently can provide a remedy for. Remedies can be for either first party costs or third party costs depending on the coverage. Errors and Omissions cover anything that occurs in within a business such as a typo on a printer. It is also named professional liability insurance. Media Liability is a special type of coverage “designed for publishers, broadcasters, and other media-related firms. The policies are typically written on a named perils basis and cover the following broad areas: defamation, invasion of privacy, infringement of copyright, and plagiarism.” (IRMI.com) This form of policy has changed as well over time and can cover offline content also.

The third area of coverage is known as network security coverage. It covers both first and third party costs, which is helpful to have for lawsuits. Any unauthorized access of data, harmful software, theft and destruction of data, and missed opportunity cost is covered. When most people think about cyber insurance, this is the coverage many associate it with. Finally, privacy covers both first and third party costs as well. Any damages from data revealed by someone within or outside of the company or any physical records or devices will be covered.

Now that the general types of coverage are laid out, it is evident that there are variations of cyber insurance for almost anyone or any type of corporation. Individuals want to have protection from Internet risks for obvious reasons. Tim Francis, the enterprise cyber leader at Travelers, claims “Cyber events can have a significant impact on the bottom line and a significant impact on the reputation… That’s as true of a small company as it is of a big company and everyone in between.” (Morgan, ”Cyber is a must”) For many businesses, the amount of data exposure that company has is a valuation of how crucial insuring their assets are.

Vast amounts of sources have been documenting many well-known corporations such as JP Morgan, Target and Chase Co. purchasing cyber insurance recently. An LA times article has indicated that spending on cyber attack insurance has doubled from 2013 to 2014 to around 2 billion. It also states “Insurance offices are struggling to keep pace. Nearly every insurance agent polled last fall by reinsurer PartnerRe Ltd. Reported growing demand for cyber attack liability insurance, with 45% reporting a significant uptick.” (Panzar, Paresh) According to the cyber attack insurance provider Beazley Group, the number of policies in its book has risen over 100% since 2012. With such a recent affluence of cyber insurance policies, there are proportionate amounts of actual cyber terrorism committed.

Every year Verizon compiles a yearly Data Breach Investigations Report, or DBIR for short, with an analysis of the previous year’s security issues with a concentration on data breaches. In the 2015 edition, the statistics are astonishing, quite frankly. With 70 countries contributing data, Verizon has found around 80,000 security incidents. “In 60% of those cases, the attackers were able to compromise an organization within minutes.”(7-9) To highlight the most significant breaches, a timeline in the appendix highlights “Jan: Snapchat 4.5 million compromised names and phone numbers, Feb: Kickstarter 5.6 million victims…Nov: Sony Pictures Entertainment: Highest profile hack of the year”. (62) With all of the data compiled in 2014, Verizon’s bottom line from its 70-page summary is that it is extremely difficult to be completely safe from the wide array of methods of cyber attacking.

In like manner, Go-Gulf.com has posted an informational blog about current and future predictions of cyber terrorism. The top three causes of direct financial costs of cyber attacks in the U.S. are fraud, theft/loss, and repairs. Also, the aforementioned four coverage areas in cyber insurance can remedy these threats depending on the coverage one purchases. Most importantly, the article states, “In 2017, the global Cyber Security market is expected to skyrocket to 120.1 billion from 63.7 billion in 2011.”(Go-Gulf.com) Currently there are 556 million victims per year, 1.5 million per day, and 18 per second. If one doesn’t think that their company needs insurance from ex-employees stealing company data then one should know that 59% of them have admitted to doing it. That privacy coverage might not sound too expensive now. When it comes to the industry, crimes have been committed largely in businesses (35.1%), the healthcare industry (38.9%) and the educational industry (10.7%). If cyber terrorism has not been considered a real threat for one a decade ago, the times have surely changed.

When it comes to determining the cost of ones premium for cyber insurance, it is most definitely not a one size fits all situation. Christine Marciano, the president of Cyber Data Risk Managers, claimed in an article “…as premiums are factored on a company’s industry, services, data risks and exposures, computer and network security, privacy policies and procedures and annual gross revenue.” (Marciano) She also provided samples of her client’s annual premiums ranging from an $859 dollar premium for a healthcare social worker to a $120,000 premium for a Data Storage Center. These of course are generally opposite ends of the spectrum showing the versatility of the Cyber Data Risk Managers who work for the insurance agency.

Although cyber insurance may cover cyber security in its policy, it still is not cyber security itself. Cyber insurance can remedy a various amount of damages with proper compensation, but it is not a substitute for managing the risk before the breach happens. Some damages cannot be remedied by cyber insurance such as defamation and loss of future income. Due to that fact, the only way in the future cyber insurance can proliferate constantly, is if the methods of risk management themselves become more efficient as well. Certain common mode failures can be eliminated with proper education about cyber security.

In 2015 Sony Pictures Entertainment was set to release the film *The Interview*, in which Seth Rogen and James Franco were supposed to assassinate the prime minister of North Korea, making it one of the most globally controversial movies of all time. Prior to its release, hackers from North Korea wiped Sony’s data and spread it across the web, in which Sony took as a legitimate threat so it cancelled the movies release. This resulted in around 100 million dollars worth of costs for Sony from lost revenues, lost data and so on. Sony has cyber insurance and the CEO claims that all of its costs are going to be covered by the policy. There are alternative speculations that the policy will not matter due to Sony cancelling the release themselves. In many views, planning to release such a controversial film is risky to start out with.

Given the notable amounts of cyber terrorism attacks and cyber insurance policies growing at the constant rate they have been, it appears a new key risk will continue to be more prevalent as we shift towards technology. As a result, cyber insurance must only be at its infancy and is more than likely to be around for a long time. Cyber insurance is the clear compliment to proper risk management and it is crucial that employees stay educated and the inherence of this risk is known.

Works Cited

Bhattarai, Abha. "Cyber-insurance Becomes Popular among Smaller, Mid-size Businesses." *The Washington Post* n.d.: n. pag. Web.

Bissell, Kelly. "Cyber Insurance: One Element of Risk Management - Deloitte CFO - WSJ." *Cyber Insurance: One Element of Risk Management - Deloitte CFO - WSJ*. The Wall Street Journal, n.d. Web. 27 Apr. 2015.

"Cyber Crime Statistics and Trends [Infographic]." *Web Design Dubai Dubai Web Design and Web Application Development Company Cyber Crime Statistics and Trends Infographic Comments*. Go Gulf Web Technologies, n.d. Web. 27 Apr. 2015.

Floresca, Lauri. "Cyber Insurance 101: The Basics of Cyber Coverage." *Cyber Insurance 101: The Basics of Cyber Coverage*. N.p., n.d. Web. 27 Apr. 2015.

Marciano, Christine. "How Much Does Cyber/Data Breach Insurance Cost?" *Data Breach Insurance*. N.p., n.d. Web. 27 Apr. 2015.

"Media Liability Coverage." *- Insurance Glossary*. N.p., n.d. Web. 27 Apr. 2015.

Panzar, Javier, and Paresh Dave. *Los Angeles Times*. Los Angeles Times, n.d. Web. 27 Apr. 2015.

Pharro, Richard. "Cyber Insurance Still No Substitute for Cyber Security | ITProPortal.com." *ITProPortal*. N.p., 24 Apr. 2015. Web. 27 Apr. 2015.

Smith, Morgan. "Cyber Is a Must for Small Businesses-Including Yours." *Cyber Is a Must for Small Businesses-Including Yours*. N.p., n.d. Web. 27 Apr. 2015.

Thompson, Mary. "Why Cyber-insurance Will Be the next Big Thing." *CNBC*. N.p., 01 July 2014. Web. 27 Apr. 2015.

*Verizon Data Breach Investigations Report*. Rep. Vol. 2015. N.p.: n.p., n.d. *Verizon Enterprise*. Web. 25 Apr. 2015.