Cyber Warfare: An Emerging Market

Michael Fielding

Florida State University

Cassandra R. Cole, PhD

Mach 1st, 2015

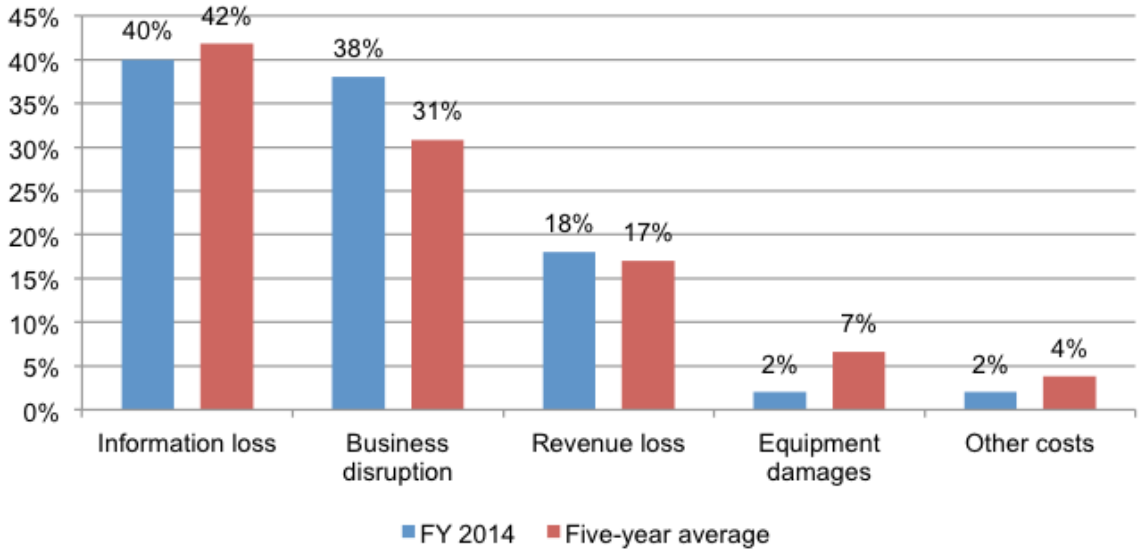
In recent years, the likelihood of a data breach or cyber attack has increased exponentially and the need for a data security and privacy insurance product is higher than ever; forcing risk specialists and companies to turn to non-admitted, excess and surplus lines carriers. According to FBI Director James Comey in an interview with *CBS's 60 Minutes*, "There are two kinds of big companies in the United States. There are those who've been hacked, and those who don't know they've been hacked." The risk of a cyber breach not only exists for large companies that handles sizeable amounts of data, but even retail businesses handling personal information such as customer's credit cards. The International Organization for Standardization (ISO) established policies that are made available to businesses by standard admitted carriers. These insurance carriers also provide cyber endorsements for existing Business Owners Policies (BOP). These forms of coverage may be sufficient for a small firm; however, mid to large size companies may need customized policies, giving specialty carriers an opportunity to promote products in a rapidly growing market. As such, there is still a need for standalone cyber risk policies, which provides specialty carriers with an opportunity to design new products in a rapidly growing market.

The frequency and severity of cyber attacks on U.S. firms has been rapidly increasing over the last few years, which is making it more difficult for firms to implement risk retention methods and ultimately resolve the repercussions. A survey conducted by the Ponemon Institute with Hewlett-Packard of 59 large-sized U.S. firms found the average annual cost of responding to cyber attacks was $12.7 million, up 96 percent over the previous five years (HP Study). The survey also suggests there is a positive correlation between the time it takes to resolve an attack and the amount of costs incurred. Specifically, the study finds:

> "The average time to resolve a cyber attack was 45 days, with an average cost to participating organizations of $1, 593, 627 during this 45-day period. This

> represents a 33 percent increase from last year's estimated average cost of $1, 035, 769, which was based upon a 32-day resolution period."

Not only can we see from these findings that the average incurred costs increased as the average time to resolve an attack increased, but also in general, average resolution times are increasing. For these reasons, it can be beneficial for mid- to large-size companies to turn to excess and surplus lines carriers because cyber risk endorsements on standard BOP policies available through admitted carriers may not provide sufficient claim limits nor some of the incurred costs such as business interruption during and after the attack. The survey also looked at the consequences of a cyber attack, focusing on four primary costs.



Information loss is still the most costly effect of a cyber attack, although down two percent compared to the five-year average. When a company's network becomes compromised and information is either lost or corrupted, the costs related to a company recovering the information can be abundant as a company's vital information is irreplaceable in many situations. This issue of information loss is related to business disruption because not only can operations be disrupted during the attack, but also a company has to spend resources that could be used elsewhere in order to recover. Another important cost associated with a network breach stems from an article

of legislation proposed by President Barack Obama requiring companies to inform customers within 30 days if their data has been compromised. Notifying a small amount of customers might not be too costly, but for companies with hundreds of thousands of customers or clients this new legislation could prove extremely costly. Besides legislative requirements, retailers may also face contractual requirements after a breach, which adds to the incurred costs. Many credit card merchants can hold retailers liable for any investigation costs, costs associated with issuing new credit cards, and also the fraud from the stolen credit card information. According to *CFC Underwriting*, these losses could run into the thousands of dollars for even small retailers (Insurance Journal). A standalone cyber security policy would assist businesses with all of these costs, including security breach remediation, data restoration expenses, business interruption, and additional expenses.

In addition to this issue in the United States, there is also an increasing global cyber risk exposure due to differences in privacy laws, motives, and other factors. One major difference between the United States' privacy laws and the rest of the worlds' is the United States and only several other countries require companies to notify customers in the event of a security breach (Zurich). With the absence of notification regulations, companies do not incur notification costs; however this affects the number of known breaches and also makes gathering loss data impossible. Not knowing the number of losses worldwide and costs incurred makes it more difficult for statisticians to forecast loss trends and other data, ultimately used by insurers to determine premiums and limits.

Although financial motives remain the top reason for a cyber attack, cyber espionage is becoming more apparent with competing firms in different countries attempting to steal intellectual property. A company's intellectual property includes their trade secrets, patents,

manufacturing methods, and even negotiation approaches. Insuring intellectual property is a challenging task for both admitted and non-admitted insurers because putting a value on intangible assets is difficult. However, cyber liability policies assist with the reparations associated with an intellectual property loss in order for the business to return to normal operations. Global instability and conflict contributes to another increasingly popular motive, political agendas. Also known as "hacktivists," individuals with a political vendetta towards a company may breach their systems in order to disrupt their operations and damage their reputation (Zurich). *Anonymous*, a political hacktivist group, is the most well known example of a party with a political agenda hacking companies in order to promote their ideals. *Anonymous* is credited with numerous cyber attacks over recent years, one of the most prominent being their 2010 attack of *Sony, Amazon, PayPal, MasterCard, and Visa*. Both *Visa* and *MasterCard*'s websites were brought down in result, leaving thousands of disgruntled and concerned customers. The overall intent was not to steal clients' financial information, but rather to delay the companies' operations and tarnish their reputation. Bryan Sartin, one of the co-authors of Verizon's Data Breach Investigations Report (DBRI) said, "in an activist attack, there are literally hundreds of ways you can hurt the victim, its about damaging a brand, retaliation, and the public perception that an entity has been hacked" (Verizon).

The costs attributed to poor public perception due to a cyber attack can be tremendous. In the largest data theft to date, retail store *Target* estimated that in the 2013 incident 40 million credit and debit card accounts were compromised, and identifying information for approximately 70 million customers was leaked. The *Target* security breach is still costing shareholders, forecasting incurred costs of $148 million dollars as well as plummeting stock prices (CIO). Although many cyber liability policies cannot provide sufficient coverage to

restore a business' negative public perception, such as *Target's* case, they can still cover the direct losses so that the company can plan to retain any possible reputational loss. In addition to covering those direct losses, under a cyber liability policy, a company's costs associated with hiring a public relations firm to either prevent or resolve negative perceptions is covered.

In regards to cyber risk and auto policies, the release of each year's newest model vehicle is accompanied with a variety of technological features leaving drivers more and more vulnerable to hackers. A study performed by the staff of United States Senator Ed Markey analyzed data collected from 16 major auto manufacturers showing that there are weaknesses in nearly 100 percent of cars, and also suggested that hackers can get into the controls of some popular vehicles taking control of acceleration and braking, turning, and dashboard readings (Advisen). This exposure could prove to be detrimental to any firms using a fleet of vehicles, especially since it is not covered under any standard Business Auto Policy. For example, if a hacker were to alter the dashboard readings of trucks in a shipping company, specifically the odometer and gas gauge, a driver might not record the correct mileage and gas usage of his trip, resulting in a loss of profit as well as major accounting problems. This could be a huge opportunity for specialty carriers to take advantage of in the near future because it is a relatively immature exposure.

Although many wholesale and E&S carriers already offer cyber liability policies for businesses and individuals, the sector is still very new and there is ample room for improvement. For instance, Tim Stapleton an assistant VP and professional liability product manager at Zurich North America stated, "insurance coverage is not yet available for many indirect losses because it is difficult to quantify the 'soft costs' of a data breach" (Strategicrisk). As seen by the Hewlett-Packard survey, cyber warfare is becoming a more common occurrence

and ‘soft cost’ data is becoming more readily available. Also many times following a breach a company may be subject to fines and penalties, occasionally requiring companies to upgrade and regularly maintain a sufficient security program. Many current cyber insurance policies may not cover the cost to upgrade security, which frequently requires companies to perform a full network overhaul, ultimately costing a large company millions of dollars.

Cyber risk is undoubtedly one of the quickest growing exposure areas for companies with the need of a cyber security and liability policy growing rapidly every year. The Vice President for cyber security and privacy brokerage at Lockton Cos, Ben Beeson said, “The amount of premiums spent on cyber coverage is estimated to total about $2 billion, almost double the level 18 months ago” (Treasury and Risk). Beeson suggests this is most likely attributed to the major breaches that occurred in late 2013, specifically the *Target* incident. Regardless of the cause, the increase in demand for a cyber liability product is positively correlated to the amount of policies made available by insurers. Due to the characteristics of this exposure, admitted insurers have a clear disadvantage. With countries proposing stricter regulations and technology constantly advancing, cyber risk is regularly evolving and a successful producer must be flexible to accommodate client’s needs. A surplus lines carrier has the ability to customize specific forms of coverage, as well as negotiate prices based on the individual exposures of the client. Because of this, carriers in the excess and surplus lines market are able to alter policies with the evolving conditions and situations of cyber risk, giving them the advantage when it comes to insuring cyber liability in the years to come.

Works Cited

AFP World News. "Advisen FPN." *Advisen FPN*. N.p., n.d. Web. 1 Mar. 2015.

Cook, James. "FBI Director: China Has Hacked Every Big US Company." *Business Insider*. N.p., n.d. Web. 1 Mar. 2015.

Insurance Journal. "CFC Underwriting Upgrades Cyber Policy." *Insurance Journal - Property Casualty Insurance News*. N.p., n.d. Web. 1 Mar. 2015.

Kelly, Susan. "Data Breaches Spur Demand for Cyber Liability Coverage." *Treasury & Risk | News, Analysis, and Solutions for Financial Professionals and Executives*. N.p., n.d. Web. 1 Mar. 2015.

LeClaire, Jennifer. "Cost of Target Data Breach: $148 Million Plus Loss of Trust - Computing on CIO Today." *CIO Today: Daily Briefing for Technology's Top Decision-Makers*. N.p., n.d. Web. 1 Mar. 2015.

Ponemon Institute. N.p., Web. 1 Mar. 2015.

Strategic Risk. "What Risk Managers Need to Do in the Fight Against Cyber Crime – in Five Steps | Online Only | Strategic Risk." *Strategic RISK - Risk Management and Corporate Governance Solutions*. N.p., n.d. Web. 1 Mar. 2015.

Travelers Insurance. N.p., Web. 1 Mar. 2015.

Verizon. "U.S. Treasury Secretary Lew and Verizon Discuss Cybersecurity for Financial Institutions | Verizon Enterprise Solutions." *News Center - Verizon Enterprise Solutions*. N.p., n.d. Web. 1 Mar. 2015.

Zurich. *Liability, Property and Casualty Commercial Insurance - Zurich NA*. N.p., n.d. Web. 1 Mar. 2015.