CYBERCECURITY
DEFENDING YOUR ASSETS

A Beginner’s Guide to Cyber Risk Insurance

Introduction

Instruments for financial risk mitigation have always been staples of human enterprise, from clauses protecting Medieval seafaring merchants against unrecoverable losses to Ben Franklin's 1751 forming of the Philadelphia Contributionship—the first company in the U.S. to offer fire insurance. The types of emerging insurance serve as a barometer of the times: Franklin's firm was created in response to the prevalence of fire-prone wooden structures in Colonial-era New England. Similarly, automobiles have dominated much of the 20th century; as a result, the auto insurance industry continues to flourish. For average vehicle-owning consumers, liability coverage is critical for offsetting personal risk, so much so that it's required by law. If you received a driver's license at age 16, chances are you'll experience an automobile accident by your mid-30s. This comes out to 3 to 4 accidents over a life of driving for the average person.

The outlook is equally if not more disheartening for businesses when it comes to data breaches. A survey by the Ponemon Institute revealed that 47 percent of organizations were breached in the past two years, with numbers even higher depending on industry type and size. It's therefore no surprise that cybersecurity or cyber risk insurance has emerged as a byproduct of the status quo. Like drivers and the inevitable car accident, all businesses will likely suffer a data breach at some point.

> ***"I am convinced that there are only two types of companies: Those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."***
>
> *Robert S. Mueller III, Former Director, Federal Bureau of Investigation*
> *RSA Cyber Security Conference, San Francisco, CA, March 1, 2014*

Given that, it is not surprising that cyber risk insurance in the 21st century's version of Ben Franklin's fire insurance.

According to Allied Market Research, the cyber risk insurance market is growing at a compounded annual growth rate of 28% between 2016 and 2022 and will generate $14 billion in annual premiums by 2022[1] .

It is hard to look at any news source and not see constant news of the cyber breach of the hour. Whether it is Target or Home Depot on the retail front, Anthem and the other Blue Cross

[1] http://www.prnewswire.com/news-releases/cyber-insurance-market-to-reach-14-billion-globally-by-2022-allied-market-research-604767916.html

affiliates on the healthcare side or Yahoo in the online services business – even the government isn't immune. Wikileaks published a treasure trove of sensitive CIA documents in March 2017.

Target has spent over $250 million recovering from their breach. Let's say that your company is breached and it only costs $1 million to deal with it. There are investigations to conduct, people to notify, communications to manage and many other tasks to complete – not to mention lost business and potential lawsuits. Is that a cost that you can internally fund? For most companies, the answer is no and therefore many are turning to cyber risk insurance to help them deal with the cost.

Today's Threat Landscape

According to the Identity Theft Resource Center (ITRC), 781 data breaches were tracked in the U.S. in 2015 and 1,093 in 2016 – a new record. Of course, these figures don't include unreported/unannounced or undetected data breaches; notwithstanding, cybersecurity is no longer relegated to IT or the security team. For the C-suite, Board, and other executive stakeholders, managing cyber risk is essential to keeping the firm afloat. This starts with understanding what tools and instruments are available to mitigate the inherent dangers of digitization.

Today's cyber threat landscape is fraught with peril at every turn. Bad actors ranging from criminal organizations, competitors, geopolitical entities, and even disgruntled employees have a broad and bountiful field of opportunity in their midst. Computing and digitized assets serve as foundational pillars for today's businesses and most organizations have transitioned at least some of their critical business processes to the cloud. As such, organizations find themselves neck-deep in increasingly treacherous waters: security compromises, data breaches, and service disruptions have never been more damaging to the business. Adding to the risk is the sharing of data with third parties – sub-contractors, service providers, regulatory agencies and others.

You could declare IT security is a lost cause. Security firms around the world are constantly developing cutting edge technologies for detecting and countering novel and sophisticated attacks, to no avail: cyber criminals remain one step ahead of the game. Even if you declare it a lost cost, that won't stop hackers from trying to breach you and, if successful, customers will sue you and the media will beat you up. But while attackers may gain the upper ground in the cybersecurity battle, the business wins if it survives any assaults to its livelihood, digital or otherwise. Forward-thinking firms therefore anticipate impending data breaches, minimizing their losses by treating security as a function of business risk management. This includes layering security mechanisms to protect the IT assets that matter the most and acquiring proper cybersecurity insurance to cover any damages resulting from security incidents. Acquiring cyber risk insurance is a challenge for businesses because unlike, say, fire insurance, policies differ between insurers and policies between insurers are hard to

compare. Of course, commercial insurance policies for protecting businesses from injury and damage are nothing new. But the nascent cybersecurity insurance industry has only begun to formalize standards and actuarial models for assessing/quantifying cyber risk and pricing cybersecurity insurance policies.

Assessing and Quantifying Cyber Risk

Traditional insurance underwriters have the luxury of tapping into vast oceans of historical data for pricing health, real estate, business, and automotive insurance products. When it comes to cyber risk, however, a lack of actuarial data renders policies qualitative and relative at best. After all, it is likely that the vast majority of breaches, typically small ones, are not reported at all. In many cases, the business does not even know it was breached. Unlike a fire, there are no tell-tale charred remains to identify an event has occurred. True, there typically is forensic evidence to examine, but even when experts, costing hundreds of dollars an hour look at the remains, often it takes them months to figure out what happened. In the absence of accurate cybersecurity risk models, cyber risk insurance is hard to fit into an organization's security/risk posture and coverage requirements. Fortunately, an exponential growth in cybercrime across the globe and a subsequent rise in demand for more accurately priced products has prompted insurers to adopt less arbitrary measures for quantifying and measuring cyber risk. This includes the measurement of external risks as well as internal assessments of a firm's infrastructure security.

For example, Upguard's CSTAR--or Cyber Security Threat Assessment Report--is a rising standard for cybersecurity risk assessment. CSTAR enables insurance firms to create policies based on a composite score representing the collective vulnerability of every server, network device, and cloud service to the risk of breaches. By accurately quantifying the insurability of a company's IT assets with hard data regarding its infrastructure's actual configuration state and testing habits, insurance companies can more readily customize policies to an organization's actual cyber risk profile. There are several other respected scoring tools available for businesses and insurers to use such as Bitsight Technologies. All of these products score risk in their own way, providing a score similar to a credit bureau score – a higher number means less risk,

> ***"The mantra of any good security engineer is: Security is not a product, but a process. 'It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together."***
>
> *-Bruce Schneier*

Types of Cyber Risk Policies

Current cyber insurance policies usually cover direct and immediate losses due to data breaches and security compromises. Coverage for first and third party losses are discussed below, followed by items typically not covered per the usual cybersecurity insurance policies.

First-party Coverage

This type of coverage includes compensation for losses or damages suffered by the organization purchasing the insurance policy.

- **Forensic Investigation** - the cost of identifying a cyberattack or data breach occurrence, determining its cause, and remediation/recovery efforts.
- **Data Loss and Recovery** - the cost of physical damage and data loss from a cyberattack
- **Network Business Interruption** - lost revenue due to business discontinuity caused by a network security breach or failure
- **Cyber Extortion** - damages arising from a company's network or IT assets being held hostage by cyber attackers
- **Theft and Fraud** - damages arising from the theft and/or fraudulent use of a company's data or computing resources
- **Business Continuity** – costs to continue operating the business after a cyber event
- **Crisis Communications** – Costs of public relations activities after a breach

Third-party Coverage

This type of coverage protects the insured from being liable to third parties for losses or damages suffered due to a data breach or cyber-attack.

- **Notification Cost** - organizations that store private data are increasingly required by law to notify customers in a timely manner when data breaches occur

- **Credit Monitoring Service Cost** - credit monitoring services provided to third-parties (e.g., customers) impacted by the data breach
- **Cost of Litigation** - costs related to legal defense vis-a-vis lawsuits and any resulting judgements
- **Regulatory Proceeding Defense Cost** - costs to related to defending against regulatory proceedings, to include (in some cases) assessed fines and penalties
- **Crisis Management Cost** - covers crisis management and PR expenditures for handling data breaches and security compromises
- **Online Defamation and Copyright/Trademark Infringement Costs** - covers costs related to defamation, copyright, and trademark infringement claims
- **Credit card Industry charge**-backs and fines. For even a small breach, that could be over a million dollars.

Items Not Covered by Cyber Breach Insurance Policies

Losses arising from a cyber breach that are not typically covered by cyber breach insurance include the following:

- Loss of intellectual property (e.g., source code, product designs)
- Damages resulting from reputational harm (e.g., lower sales, loss of contracts)

These two costs can often dwarf the other costs. Target spent tens of millions of dollars to recover its brand reputation after its breach. When hacking tools used by the CIA and The Hacking Team were publicly released, the millions of dollars of intellectual property investment these organizations made in developing them was flushed down the sewer overnight. Often times the loss of intellectual property is not publicly disclosed in order not to further damage brand reputation, but that doesn't reduce the value of the loss.

Emerging Cyber Risk Insurance Standards

Various government and public efforts are coalescing to provide a more regulated and guided approach to the pricing, selling, and purchase of cyber risk insurance. For example, the National Association of Insurance Commissioners (NAIC) and state insurance regulators are actively building a framework for use by the cyber risk insurance industry. In 2015, the NAIC's Cybersecurity (EX) Task Force released the **Principles for Effective Cybersecurity Insurance Regulatory Guidance**, outlining 12 principles that direct insurers, producers, and others to combine efforts in identifying risks and solutions.

For example, principle #12 states the following:

"Cybersecurity regulatory guidance for insurers and insurance producers must be flexible, scalable, practical and consistent with nationally recognized efforts such as

those embodied in the National Institute of Standards and Technology (NIST) framework."

Government regulations dictating how insurance companies price and sell cybersecurity policies must therefore be in line with industry-accepted standards like NIST's cybersecurity framework.

Other developments in this arena include NAIC's new reporting requirements for insurers, enabling interested parties to track cyber insurance policies issued in the marketplace. Additionally, various consumer protection/education initiatives and a cybersecurity consumer bill of rights-- the **NAIC Roadmap for Cybersecurity Consumer Protections**-- outline valid post-breach expectations insured parties should have of their insurance providers and agents.

Conclusion

At the end of the day, cyber risk insurance should never be a replacement for strong cyber risk mitigation practices. Often times the cost of a breach exceeds the insurance coverage as Target and others are aware. In addition to the costs, the business disruption alone is a sufficient reason to mitigate, to the best of your ability, cyber risk. And despite being inevitable, data breaches and security compromises should be handled like any business threat and countered with a proper risk management strategy. This includes continuous security for protecting the information and system assets that matter the most coupled with an optimal cyber risk insurance policy for protecting the business when technical defenses fail. Only then can firms fully capitalize on the benefits of digitization without incurring the risk of security issues capsizing the business.

One question that is often asked is how much insurance to purchase. That is a business risk decision that the company's Board and risk management team need to decide together, but some insurance is almost always better than no insurance.

Resources

http://www.naic.org/cipr_topics/topic_cyber_risk.htm
http://www.riskandinsurance.com/analyzing-cyber-risk-coverage/
https://www.hklaw.com/PrivacyBlog/Protecting-Against-Cyber-Risk-A-Primer-on-Cyber-Insurance-01-15-2015/
https://www.allstate.com/tools-and-resources/car-insurance/who-invented-car-insurance.aspx
https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=10688
https://www.nyse.com/publicdocs/Veracode_Survey_Report_Cybersecurity_Corporate_Liability.pdf
http://www.jdsupra.com/legalnews/cyber-risks-2015-a-board-primer-13169/
https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf