A Beginner's Guide to Cybersecurity Insurance

UpGuard

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.

81% of large organizations suffered a security breach, down from 86% a year ago. 60% of small businesses reported a breach, down from 64% in 2013.

Gov.uk Press Release

Today's Threat Landscape

According to the Identity Theft Resource Center (ITRC), 781 data breaches were tracked in the U.S. in 2015-- the second highest year on record since 2005. 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. Moreover, an increasingly complex ecosystem of partners and service providers often leave organizations exposed due to circumstances out of their control.

You would hardly be blamed for declaring 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. 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. The latter has proved challenging for many organizations, not for lack of cybersecurity insurance products on the market, but instead--lack of standards for pricing said products. 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. In the absence of accurate cybersecurity risk models, cybersecurity insurance is ill-fitted to 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.

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 Coverages

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

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

Items Not Covered by Cybersecurity Insurance Policies

Losses arising from a cyber breach that are not typically covered by cybersecurity 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)

Emerging Cybersecurity Insurance Standards

Various government and public efforts are coalescing to provide a more regulated and guided approach to the pricing, selling, and purchase of cybersecurity insurance. For example, the National Association of Insurance Commissioners (NAIC) and state insurance regulators are actively building a framework for use by the cybersecurity 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, cybersecurity insurance should never be a replacement for strong cybersecurity. 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 IT assets that matter the most coupled with an optimal cybersecurity 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.

Sources

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-Insuranc e-01-15-2015/

https://www.zenedge.com/blog/2016-cyberinsurance-primer-what-every-executive-and-board-member-should-know

http://www.foxbusiness.com/features/2011/06/17/heres-how-many-car-accidents-youll-have.html

https://www.allstate.com/tools-and-resources/car-insurance/who-invented-car-insurance.aspx

http://www.itbusinessedge.com/blogs/data-security/odds-grow-that-your-company-will-suffer-a-breach.html http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

http://insurancelawhelp.com/first-party-vs-third-party-insurance-coverage/

http://www.computerweekly.com/news/450281086/UK-cyber-crime-growing-exponentially

http://www.datacenterjournal.com/ten-things-need-know-cybersecurity-insurance/

http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf

https://www.gov.uk/government/news/cost-of-business-cyber-security-breaches-almost-double

UpGuard is the world's first cyber resilience platform, designed to proactively assess and manage the business risks posed by information technology.
By validating and automating IT processes, we help organizations build resilient digital businesses on-site and in the cloud.

909 San Rafael Ave.
Mountain View, CA 94043
+1 888 882 3223
www.UpGuard.com