ITSEC™

SECURITY DELIVERED

What Business Leaders Need To Know About Cyber Insurance

The Risks, Problems & Challenges

Essential Reading for CEO's, CISO's, COO's, CIO's and CFO's.

What Is Cyber Insurance?

The first cyber insurance policies were geared toward information technology companies responsible for managing networks and systems used by other businesses and consumers and protected a service provider from the risks involved in managing a third party's infrastructure. The cyber insurance space has evolved since the mid 90's when this kind of insurance was common. Current cyber insurance protection comes in three forms: third-party written coverage, first-party written coverage, and implicit silent cyber coverage (sometimes called non-affirmative cyber exposure), it's worth drilling down into each of these to take a look at them in closer detail.

3rd Party - Third-party liability cyber insurance reimburses the insured party for the costs incurred by their clients because of data breaches, malware infections, or other cyberattacks in which the insured party was at fault. Third-party liability coverage is the cyber equivalent of medical malpractice, where businesses are insured against the harm they inflict on their clients by their action (or, as is usually the case with cyber risk, inaction). Many early policies were of this form.

1st Party - In the mid-2000s, cyber insurers began offering first-party expense coverage, which expanded insurance offerings to any company that uses technology. First-party expense cyber insurance reimburses insured parties for the costs of a cyberattack that directly affects their business. First-party policies can be broad or very specific, depending on the needs of the company, and may cover post-cyberattack expenses such as credit-monitoring and other data breach expenses, hiring crisis management consultants to restore brand reputation or negotiators to handle ransom payments, and data recovery costs. It can also include assistance for their customers.

Silent - Silent cyber risk is a third type of cyber insurance coverage that is not a cyber insurance policy at all, but a term that refers to potential cyber-related losses stemming from traditional property and casualty (P&C) policies which were not specifically designed to cover cyber risks. Say for example a hotel's computer system is infected with malware, which sets the sprinkler system off, damaging the interior and causing a patron to slip and fall. If cyber perils are not explicitly excluded, the hotel's traditional property and casualty coverage would be expected to cover the damage to the hotel caused by the sprinklers and the medical bills of the injured patron.

What Should Cyber Insurance Cover?

Types of cyber coverage currently available include:

Data breach coverage - This pays out for expenses that result from a data breach. Covered expenses typically include notification of the victims, setting up a call center, credit monitoring and restoration services for victims, and crisis management services.

Regulatory civil action coverage - This pays out in cases where the insured is facing fines from GDPR, or from the federal government after a violation of the Health Insurance Portability and Accountability Act (HIPAA,) or similar regulations. Some policies only cover the cost of defending against the action, while others may pay the fine as well.

Cyber extortion coverage - For cases where a hacker steals data from the policyholder and then tries to sell it back, or someone plants a logic bomb in the policy holder's system and demands payment to disable it. Policies usually cover the cost of a negotiator, and the expense of offering a reward leading to the arrest of the perpetrator.

Virus liability - Pays in cases where the policyholder is sued by someone who claims to have gotten a virus from the policy holder's system.

Lost income coverage - Replaces revenue lost while the policy holder's computer system or website is down. Insurers often apply minimum downtimes of 12 or 24 hours, or require proof of actual losses.

Loss of data coverage - Pays for the cost of replacing the policy holder's data in case of loss. Backup policies are not always effective, and accidents and sabotage happen.

Errors and omissions coverage - Otherwise known as O&M policies, this type of coverage predates cyber insurance, but is increasingly added to cyber policies to cover alleged failures by the policy holder's software.

Insurance Coverage Packaged With Penetration Tests

In principle this is a good idea, it means that they understand the inherent risks in an organizations cybersecurity defenses before issuing the insurance. In the UK they substitute penetration tests with CyberEssentials certification which a business can obtain to certify that their cyber defenses meet a certain standard, resulting in lower insurance premiums. Insurers like the fact that a business has put into place cybersecurity controls, it lowers the risk to them having to pay out aby money. For larger businesses, the NIST cybersecurity framework or the SANS 20 controls are good alternatives that fulfill the same purpose. So it makes sense that an insurance company would want to provide insurance coverage only after a penetration test has been carried out, it means they are able to properly understand the risks and able to make specific recommendations to lower the risk even further, simply by having the customer implement the security recommendations which follow a penetration test.

Barriers To Cyber Insurance Adoption

One barrier to widespread adoption of worthwhile cyber insurance is having a sufficiently good cyber forensic capability in place to be able to back up any claim. In the event of an incident, the evidence is often not preserved because most of the time it is not obvious that a cyber event has occurred until later making it difficult to validate claims.

Another problem is that cyber insurance policy language is not standardized. The types of risks covered under cyber insurance vary significantly across policies and businesses, and insurers do not always agree on what loss events are covered under those policies. The features of cyber events, including a limited loss history, the unreliability of past data when predicting future events, and the possibility of a large-scale attack where losses are highly correlated across companies and/or industries, make it difficult to write comprehensive policies.

How Do You Quantify Cyber Risks?

Insurers have yet to develop an evidence-based method to assess a company's cyber risk profile. This can result in high premiums, low coverage, and broad exclusions. Cyber risks are difficult for insurance companies to quantify due to the lack of actuarial data. Insurers compensate for a lack of data by relying on qualitative assessments of applicants (a penetration test would qualify). These assessments include examining the business operation, the number of customers, its scope, network security policies, network security procedures, web presence, and the type of data collected and stored. Because of this, policies are often highly customized making them more costly and this customization results in a standardization problem that extends not only to differences between individual policies but a lack of coverage uniformity offered by major insurers.

The Problems Of Underwriting And Writing Cyber Insurance Policies

There are fundamental aspects of cyber insurance that make it difficult for insurers to write and price policies that cover a broad swath of risks.

1 - There is only a limited loss history for insurers to use when setting prices for cyber insurance premiums and coverage loss limits, and this introduces risk. When insurers set auto insurance premiums, for example, they can rely on a long history of accidents and damages to model the probability that a driver with a specific set of characteristics will get in an accident and then set premiums to cover this expected loss. Cyber insurers, working in a fast-developing market, instead rely on a number of indirect factors to try to price policies appropriately, including market estimates of the cost of cyberattacks, questionnaires to determine the riskiness and pricing by other insurance companies.

2 - Cyber attacks are constantly evolving as both private and state-sponsored hackers develop new methods to infiltrate networks. The rapid evolution of hacking capabilities and strategies makes it difficult for insurers, which rely on clients having relatively consistent risk profiles, to assess the true risk of a potential client being hacked. The frequency and costs of cyberattacks have risen in recent years. In the U.S. the reported cost of the average cyberattack rose 29% from $21.2 million in 2017 to $27.4 million in 2018. Despite this, the cyber-insurance market remained profitable for underwriters.

3 - Cyberattacks are highly scalable as they can potentially hit thousands of companies simultaneously, causing large interrelated losses for insurers. One type of problem would

occur if an important service, such as a large cloud computing platform used by many policyholders, went down. The insurer may then have to pay claims on all of its policyholders at once. A similar dynamic can be seen in natural disasters, where private insurers are often reluctant to offer flood insurance (and usually explicitly exclude it from policies), because if a single house in a neighborhood was hit by a flood, it is likely that many houses around it were also hit at the same time.

4 - Another problem cyber insurance faces is the possibility of cascading failures caused by a cyberattack. One common example of a cascading failure is an attack on a power grid, where the destruction of a piece of critical infrastructure leads to failures across the rest of the grid. Cyberattacks using self-reproducing malware can also spread across a network of computers. Such an attack occurred in 2017, when a piece of malicious Russian code dubbed NotPetya targeted Ukraine. By exploiting a vulnerability in Windows to gain control over unpatched computers, NotPetya then used this access to gain passwords of other machines on the network and jumped across the globe, causing over $10 billion in estimated damages. Such an attack could easily happen again.

5 - Breaches can go undetected for an extended period of time meaning that there can be an accumulation and compounding of losses. This delay is a challenge in the context of determining when the policy has been triggered. Individuals do not know that their information has been breached until a company notifies them, meaning that only after an organization notifies its customers of a breach does it receive an actual complaint constituting a claim that triggers the policy. The costs incurred by the company to notify customers of the data breach may not be covered as the insurer may say those costs were incurred before coverage was triggered. These costs can be substantial and could lead to disputes between insurers and the insured.

How Do You Deal With This? - The difficulties in properly pricing cyber insurance products and the looming possibility of a large-scale cyberattack encourage insurers to write policies that limit the amount of coverage a business can get, as well as the risks that are insured. Capping payouts is another viable model of reducing exposure. Even as insurers acquire additional historical data on cyber loss events, the modeling of cyber risk will continue to present challenges. At the heart of the problem of modeling cyber insurance is that yesterday's attacks do not inform us about tomorrow's risks. In order to help insurers accurately price future cyber risks, predictive cyber-risk models will have to be developed.

The Legal Uncertainties Of Cyber Insurance

Adding to the uncertainties insurers face when attempting to structure cyber insurance policies is the lack of legal precedent on core issues pertaining to cyberattacks. When facing uncertainty regarding fundamental questions, insurers wait until such issues are resolved before offering policies or only write policies with restrictive coverage and capped claim payouts that are less useful to businesses.

For example, data breaches and data theft are a common source of damages from cyberattacks, yet important case law on this issue is still unresolved. Legal cases involving data breaches rest on the nature of the alleged harm: If personal data are exposed due to a cyberattack on a database, has the person whose data was exposed suffered sufficient concrete harm or does there merely need to be “substantial risk” that future harm will occur? Courts are split on this issue. Several courts have found that victims of data breaches do not have standing to sue when no actual identity theft or fraud occurs, while others have found that the risk of data misuse that results from a breach confers standing to sue.

Case Study - Lawsuits that are directly concerned with cyber insurance coverage have already begun to appear. One case that has particular significance for the development of the cyber insurance market, between Mondelēz and Zurich Insurance Group, began with a disagreement about a common “act of war” exclusion. In June 2017 a virus called NotPetya was released into Ukrainian information technology systems. The virus quickly spread to multinational companies, including Mondelēz who claimed $100 million in damages from the attack. At the time, Mondelēz had a contract with Zurich that covered “physical loss or damage to electronic data, programs or software” triggered by “the malicious introduction of a machine code or instruction.” The policy contained an exclusion for “hostile or warlike action in time of peace or war”.

In 2018, the White House called NotPetya a “reckless and indiscriminate cyberattack” on the part of the “Russian military” and “the Kremlin which resulted in Zurich denied Mondelēz’s claim on that basis that the White House’s declaration qualified NotPetya as an act of war. Mondelēz began to sue Zurich in January 2019 and If Zurich successfully argues that NotPetya qualifies as an act of war, it will establish a precedent that many of the cyberattacks that companies face are not covered by their insurance. It is too early to know what impact this case will have. Some observers have suggested that if Mondelez wins its court battle, private industry might finally see “a new market in cyberattack insurance overnight.”

Conclusion

The cyber insurance industry faces significant challenges, including a lack of historical data, a lack of ability to predict the future of cyber risk, the possibility of large cascading loss events, uncertainties among market participants about what is specifically covered under such policies, and legal battles over fundamental issues. The future growth of the market will depend upon how these issues are resolved. The dominant view remains that the cyber insurance market is immature compared to other insurance markets and the datasets used to understand and accurately price cyber risk are still underdeveloped.

Recommended Further Reading

HM.gov UK Cybersecurity: The Role Of Insurance In Managing And Mitigating The Risk