Whitepaper

HackNotice

Recent Trends in Cyber Insurance:

Belt-Tightening, Adoption Issues, and Legal Complexities

General Interest

Cyber insurance: An evolving field

It's common knowledge that cyberattacks, breaches, and leaks can have devastating financial consequences on victims. Breached companies not only suffer direct financial damage from ransom payments, having accounts accessed, and business downtime, but also suffer the loss of reputation that can follow in the wake of a big cyberattack (especially if it's highly publicized in the media). All of these effects can result in millions upon millions of dollars of lost income. Often, smaller entities with less liquidity or resources simply can't weather the storm of a major cyberattack, and have to close shop.

Almost all companies invest (often quite heavily) in IT and security departments that focus on keeping the organization safe from hackers. That's a proven solution, but, obviously, companies continue to fall foul of cyberattacks. It just takes one breach, even if thousands have been successfully defended against, to wreak havoc. To effect a full stop-gap with regard to cyberattack losses, cyber insurance is an increasingly attractive option.

But it's a complicated insurance product. Litigation abounds, but there's still not a strong legal consensus about certain aspects of policies. The methods insurers use to assess risk is constantly changing. And it seems like every day new insurance methods, practices, and policies are being developed.

Cyber insurance policy language can be intricate, and there are a number of areas that aren't covered. Compliance fines issued by the government are rarely covered. And if any incidents, upon investigation, are found to be a result of negligently weak in-house cybersecurity measures, they won't be covered. (Cyber insurance underwriters are very diligent about uncovering non-insurable weaknesses in companies' security infrastructure.) Plus, there are often clauses for events such as "acts of war".
In this whitepaper, we'll explore the current pitfalls and positives in the cyber insurance landscape.

Transparency Issues: How Do Insurance Companies Calculate Risk and Premiums?

A major issue facing organizations shopping for cyber insurance is the lack of reliable data about just how these policies are developed, quantified, and priced.

While insurance companies are often seen as the sole organizations with specialized ability to quantify and price risks, there is almost no public information about how carriers actually assess cyber risk across firms and industries, and particularly, how they compute prices for cyber insurance premiums. Indeed, experts have stated that rate calculation equations are likely to be rudimentary, and based on very subjective inputs.

This lack of transparency in policies and practices is cited as one of the leading obstacles hindering adoption of cyber insurance, and presents significant challenges for senior executives seeking to manage risks across their organizations, because they are unable to effectively understand and compare coverages across insurance carriers.

The lack of transparency prevents these decision makers from using this information to shift security infrastructure and postures in ways that can lower insurance premiums and help their organization.

The industry in which an organization operates, the type of data they manage, their current security posture, and other factors such as the security status of their third-party vendors all play a role in price calculation. But, as stated, there are very few actual numbers available to the public.

What we do know: Currently, average premiums are priced between $10 000 and $25 000, with some carriers writing limits between $10 million and $25 million, and as high as $50 million. But these can vary greatly, depending on the type of company being insured and, obviously, the way that the insurance company (non-transparently!) calculates risk.

We'll look a bit later at reluctance to adopt cyber insurance policies. Certainly, a dearth of knowledge about what insurance companies are considering when determining rates is a contributor.

Legal Gray Areas

There exists a relative lack of legal precedent on cyber insurance and what it covers after cyberattacks. When facing uncertainty regarding these questions, insurers tend to wait until such issues are resolved before offering policies, or only write policies with restrictive coverage that are less useful to businesses. As well, insurance companies may increase rates simply out of anticipation of expensive litigation issues arising before solid precedents are set.

For example, data breaches and data theft are a common source of damages from cyberattacks, yet important case law on the issue is still unresolved. Legal cases involving data breaches currently focus on the nature of the alleged damage.

Here's the big question: 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? (Having data exposed is one thing, but having it used maliciously, or suffering reputational damage from the exposure, or needing to pay a ransom could be considered the actual harm.)

[5]

¡The Supreme Court has yet to directly address the issue of a right to sue in data breach litigation. In March 2019, the Supreme Court refused to hear an appeal from Zappos.com of a Ninth Circuit Court ruling that Zappos.com, who had only alleged that financial losses were imminent, also had sufficient grounds to sue.

The "act of war doctrine" and act of war exclusionary policy language is another issue faced by insurers and the insured. The "act of war" is a legal concept that has deep roots in insurance law. The concept is that insurance policies generally exclude coverage for losses that arise from war-related activities. Typically, the doctrine has been used to refuse claims when industry in combat zones is bombed or suffers from other "physical" attacks on infrastructure.

In the context of cyber insurance, the act of war doctrine has been invoked by insurers to argue that losses arising from cyberattacks perpetrated by state actors are not covered under the policy. Insurers argue that such attacks are akin to acts of war and, as such, fall outside the scope of the policy's coverage. But, as we'll see, that can be a tough claim to make. After all, a wide range of hackers are indeed sponsored by nation-states, and their actions, while indeed perhaps politically motivated on a tertiary level, are not necessarily acts of war.

Most popular cyber insurance policies in the market contain an exclusion pertaining to losses or damages resulting from an act of war, declared or undeclared.

For example, in a policy taken out by Merck, the insurer's exclusion states:

"This policy does not insure" against:
Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack:
By any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval, or air forces;
Or by military, naval, or air forces;
Or by an agent of such government, power, authority, or forces.

Here's how that exclusion language played out legally:

Merck: A Case Where An Insurer Attempted to Exclude Coverage Due to Acts of War

In a lawsuit brought by Merck against its cyber insurer, the insurers attempted to rely on the "hostile" or "warlike" exception to coverage, arguing that the attack was launched by the Russian government, and was likely done as an act of war.

Nevertheless, a lower court found that the broad exclusionary language did not apply to this cyberattack, noting:

The evidence suggests that the language used in these policies has been virtually the same for many years. It is also self-evident, of course, that both parties to this contract are aware that cyberattacks of various forms, sometimes from private sources and sometimes from nation-states, have become more common. Despite this, Insurers did nothing to change the language of the exemption to reasonably put the insured on notice that it intended to exclude cyberattacks. Certainly, they had the ability to do so. Having failed to change the policy language, Merck had every right to anticipate that the exclusion applied only to traditional forms of warfare.

But the insurers pointed out that the language of the exclusion clearly excluded attacks which were either warlike or hostile. The attack, by a foreign sovereign, was clearly "hostile." But the court noted that the exclusion is not for government actions but for actions of hostile "military" entities, noting:

"The exclusion of damages caused by hostile or warlike action by a government or sovereign power in times of war or peace requires the involvement of military action."

Indeed, the group most likely responsible for the NonPetya attack was APT29 or Cozy Bear, which is a department of Russia's Foreign Intelligence Service, not its ministry of defense.

Thus, even though the hack was essentially perpetrated by a nation-state, and was in large part motivated by animosity toward western entities, a specific "military action" did not occur. It's a fine line to draw, and that's part of why the current cybersecurity landscape is fraught with nuance and pitfalls. Such issues are likely to increase due to the conflict in Ukraine.

Current volatility and challenges

During the COVID-19 pandemic, ransomware attacks increased and, thus, cyber insurance premiums went up. The trend continued as US cyber insurance premiums surged 50% in 2022, with further increases in ransomware attacks (and the ever-skyrocketing presence of online commerce) driving demand for coverage.

But cyber insurance rates dropped around 10% in June 2023 compared with a year earlier, reversing those sharp rate rises, with claims proving smaller than expected by analysts. Throughout mid to late 2022 and into early 2023, the number of global ransomware attacks fell by 20%, following the start of the conflict between Russia and Ukraine, as hackers in those countries focused on military-centered cyberwarfare.

Still, in the long term, ransomware attacks are predicted to continue to increase, and analysts have forecast that the cyber insurance market will grow from $12 billion (in 2022) to $50 billion (2030).

And, despite the current recent fall in insurance rates, major players are tightening their regulations and requirements – and reducing their coverage limits. Lloyd's of London, which controls around a fifth of the global cyber insurance market, has discouraged its firm divisions from taking on cyber insurance business next year, industry sources told Reuters. Additionally, U.S. insurer AIG said in August it was cutting cyber insurance limits in 2023. American International Group, Inc. has also reportedly been tightening the terms of its cyber insurance policies, as well.

What happens next remains to be seen. Was the drop in insurance rates in early 2023 an anomaly? Risk appetite" is changing, with carriers trying to get ahead of spiraling loss costs. The impacts s have been serious: supply is at a premium and rate rises are high. Insurers are also demanding more from businesses' cyber resilience, and are only insuring f they are satisfied by the strength of companies' security.

dollar analysis of the 787's security systems by Boeing. Boeing concluded that there were no vulnerabilities that could be exploited.

Still, these postulations are food for thought. And, indeed, a source of worry for many regulators and industry players.

Essentially, insurance companies want to see exactly how much risk they are taking on, including the cybersecurity history of the company, the current state of its security posture, the unique risks inherent to the company's business model and industry, and the potential damages (and types of damages) expected in the event of a major breach. Or to put it differently, insurers are essentially cherry picking accounts based on companies' level of cyber security hygiene.

Reluctance to adopt?

Despite the strong motivation that organizations have to employ insurance as a cybersecurity strategy for specific threats, at the same time they seem reluctant to do so. Currently, only around one-third of US companies have purchased some sort of cyber insurance.

There is significant variation in cyber insurance across US industry sectors. For example, barely 5% of manufacturing firms have cyber insurance coverage, whereas the healthcare, technology, and retail sectors have reached an adoption of close to 50%.
Overall, in a 2022 survey, only 19% of organizations reported having cyber insurance coverage that extended beyond $600,000.

Reasons for a reluctance to adopt insurance include, as mentioned before, a lack of regulatory clarity about what cyber insurance has to cover, a lack of understanding about the importance of cyber insurance (and how much damage a cyberattack can cause), lack of knowledge about how rates are calculated, and, of course, being put off by high prices.

The territories that are experiencing the highest growth rates in cyber insurance include Australia, Germany, the Nordic countries, Israel, Italy, Spain, the United Kingdom and the United States. Despite being one of the most targeted regions globally, uptake in Asia remains low, as well as in Latin America.

Some countries are already far ahead in the cyber insurance-adoption game. For example, 87% of large companies and 8% of mid-sized companies have taken out cyber insurance in France.

The Growth of Personal Cyber Insurance

Personal cyber insurance, also called "cyberattack insurance," is often sold as an add-on to homeowners insurance and can cover a range of cyber crimes:
Cyber attack coverage pays for the removal of a virus from or reprogramming of personal devices, Wi-Fi routers and other internet access points, such as smart home devices and security systems.

Cyberbullying coverage helps people deal with online harassment that results in issues like wrongful termination, school expulsion, the need for therapy, or legal expenses.
Cyber extortion coverage pays for users to recover from ransomware attacks that block them from accessing personal data, plus the ransom fee. This coverage might include assistance from experts who can help regain files, and/or reimbursement for any ransom paid.
Online fraud coverage pays for direct financial losses due to problems like identity theft, unauthorized banking or credit card transfers, phishing schemes and other types of fraud.

Personal cyber insurance is much less expensive than organizational cyber insurance, because damages are likely to be lower. Additionally, there have not been a large number of claims submitted in recent years. So insurance companies consider personal cyber insurance a relatively lower-risk product.

The Role of Reliable, Real-Time Cybersecurity Metrics in Obtaining Cyber Insurance

When dealing with cyber insurance companies, one of the best ways to present the case that your company is insurable (and at a reasonable rate) is to bring reliable metrics to the table regarding your company's security posture. For example, when insurance companies can examine an organization's cyberattack history, breach and leak records, security culture status, and other information, they can feel much more confident making informed decisions about a company's insurability. And that confidence only increases if your organization is able to provide a potential insurer with information about your third parties' security state.

A full-spectrum threat intelligence platform such as HackNotice can go a long way toward building these sorts of vital statistics. With third-party monitoring, domain monitoring, end-user credential monitoring, a powerful dark web research service, and a user-centered threat awareness functionality, HackNotice gives you the raw data you need to see exactly where your company stands cybersecurity-wise. HackNotice monitors the dark web in real-time, so that you're instantly alerted to any breaches or leaks. Real-time, data-driven threat intelligence not only keeps you safer, but lets cyber insurance providers know they can trust you.

References

1. Cisco. “What Is Cyber Insurance?,” n.d. https://www.cisco.com/c/en/us/products/security/what-is-cyber-insurance.html.

2. @malwarebytes. “What Is Cyber Liability Insurance?” Malwarebytes, n.d. https://www.malwarebytes.com/cybersecurity/business/what-is-cyber-liability-insurance.

3. Munoz, Maria. “Cyber Insurance Premiums Surge by 50% as Ransomware Attacks Increase.” 14 June 2023. ""https://www.bloomberg.com/news/articles/2023-06-14/cyber-insurance-premiums-surge-by-50-amid-ransomware-attacks

4. Cohn, Carolyn. “Focus: Insurers Run from Ransomware Cover as Losses Mount,” Reuters, November 19, 2021. https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/.

5. Reuters. “AIG Is Reducing Cyber Insurance Limits as Cost of Coverage Soars,” August 6, 2021. https://www.reuters.com/business/aig-is-reducing-cyber-insurance-limits-cost-coverage-soars-2021-08-06/.

6. Reuters. “Cyber Insurance Rates Drop 10% in June, Report Says,” July 5, 2023. https://www.reuters.com/technology/cyber-insurance-rates-drop-10-june-report-2023-07-04/.

7. Howden Group. “Cyber Insurance: A Hard Reset.” Howden. 2023. Cyberhttps://www.howdengroup.com/sites/g/files/mwfley566/files/inline-files/Howden%20Cyber%20Insurance%20-%20A%20Hard%20Reset%20report_1.pdf

8. Tsohou, Aggeliki, Vasiliki Diamantopoulou, Stefanos Gritzalis, and Costas Lambrinoudakis. “Cyber Insurance: State of the Art, Trends and Future Directions - International Journal of Information Security.” SpringerLink, January 16, 2023. https://doi.org/10.1007/s10207-023-00660-

9. Romanosky, Sasha, Lillian Ablon, Andreas Kuehn, and Therese Jones. “Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?” OUP Academic, January 1, 2019. https://doi.org/10.1093/cybsec/tyz002.

10. Metz, Jason. “Do You Need Personal Cyber Insurance?” Forbes Advisor, November 11, 2021. https://www.forbes.com/advisor/homeowners-insurance/personal-cyber-insurance/.

The Role of Reliable, Real-Time Cybersecurity Metrics in Obtaining Cyber Insurance

Strengthen Your Defenses with HackNotice

HackNotice

Download on the App Store

GET IT ON Google Play

Available in the Chrome Web Store

Contact Us:

www.hacknotice.com

(833)HACK-900

contact@hacknotice.com

3616 Far West Blvd #117 - 583 Austin, TX 78731