Cyber insurance: Heads they win, tails they win, too?

Strategies for ensuring your cyber insurance pays when it should.

TANIUM

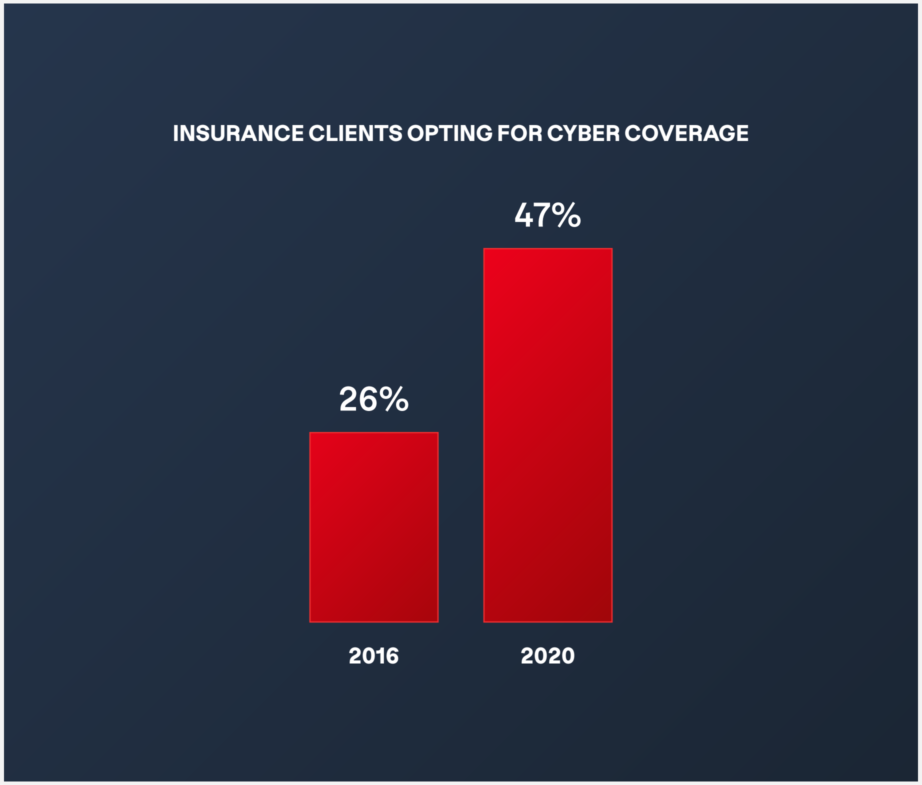
Cyber insurance: Heads they win and tails they win, too?

Strategies for ensuring your cyber insurance pays when it should.

Contents

Introduction

The rush to buy cyber insurance has grown in recent years, driven by the dramatic rise in cyber breaches and corporate concern about prevention. According to a recent analysis by the Government Accounting Office, insurance clients opting for cyber coverage rose from 26% in 2016 to 47% in 2020.[1]



Despite the appearance of being a healthy market, though, the cyber insurance industry has reached a crossroads. Carriers are still making money, but it's not what it used to be. As ransomware and business email compromise have spiked, insurers have seen higher losses across both stand-alone cyber policies and those packaged with other types of insurance. For every dollar of coverage they offer, insurers now lose about 65 cents.

That's more than double the loss ratios seen in 2017, which stood at 27.5 cents for packaged and 35.4 cents for stand-alone policies, according to research from AM Best.[2] Loss ratios of 65 cents on the dollar are far above the comfort level of most insurers.

To keep pace with the evolving risk profile and protect their profits, insurers are dramatically overhauling their underwriting models.

"Insurance, as it's currently practiced, is usually heads they win and tails they win, too," says Eric Gyasi, a cybersecurity expert and vice president at Stroz Friedberg, an Aon company, **in an exclusive interview** with Tanium's online cybersecurity news magazine *Focal Point.* "Cyber has upended that model quite a bit."

Cyber insurance risk is not as easily diversified as other coverage types. Consider flood insurance. If a major flood strikes one state, income generated in states without heavy flooding helps offset an insurer's losses.

But cyberattacks are rarely confined to one place. When widespread attacks such as NotPetya hit critical infrastructure, any organization with vulnerable hardware or software can be affected. Insurers can't diversify themselves out of that kind of risk.

And most policies exclude coverage for acts of war. But such "war" clauses can be tricky to enforce. For instance, adversarial nation-states rarely, if ever, take credit for cyberattacks on foreign governments and enterprises. Also, nations such as Russia and North Korea shelter cybercriminal syndicates and hacktivists, whose attacks, even if aligned to the motherland, are not considered acts of war.

Insurers are not taking any chances. Many are drafting new clauses, looking to hedge their risks by expanding the number of coverage exclusions. "Chubb has gone public with their strategy of limiting coverage for widespread events," Monica Tigleanu, senior cyber underwriter at the German reinsurance giant Munich Re, **recently told *Focal Point.***

"There is a lot of sensitivity in the insurance market to systemic risk," she explains, "and exclusions are another way to manage that risk."

That should put policyholders on alert.

Why is a war exclusion in your cyber insurance policy?

War exclusions first appeared in insurance contracts in the 1930s in response to the Spanish Civil War. They may seem like a cop-out to some, just another way for insurance companies to get out of paying clients. But the real aim of these exclusions is to safeguard insurers from events so catastrophic that they'd go bankrupt trying to pay all the claims. That protects the rest of us, too. There's no point in having insurance if your insurance company will be drained of funds.

But insurers drafted the original war clauses during an actual war, when damage to people and property was physical. Cyberwar is harder to spot.

It's also harder to define. In 2013, former CIA Director Michael Hayden called a rash of state-sponsored cyberattacks originating from China "akin to Hiroshima[3]." A year later, Sen. John McCain, R-Ariz., said the North Korea hack of Sony Pictures Entertainment was "a new form of warfare." Not so, said President Obama, who called the Sony breach "cybervandalism" and "not an act of war."[4]

Three years after that, the NotPetya cyberattack, which affected businesses worldwide and wreaked $2 billion to $10 billion in damages, was also deemed vandalism, even though both the U.S. and U.K. governments attributed the attack to the Russian military.

NotPetya had targeted Ukraine's financial sector. But it went viral and global thanks to the world's interconnected computer networks. Pharmaceutical giant Merck & Co. claimed it suffered $1.4 billion in losses in the attack. But its nearly three dozen insurance companies rejected the claim, citing war exclusion.

Merck sued its cyber insurance providers—and won

In December 2021, a New Jersey judge sided with the pharma giant. The judge ruled that the war exclusion clause related to armed conflict.[5] The judge further noted that if the insurers had wanted to avoid paying for such cyberattacks, they should have changed the wording to define those events.

Merck's policy was what's known as an all-risks policy. As Michael Bahar, a litigation partner at Eversheds Sutherland and a former deputy legal adviser to the National Security Council, wrote in a recent report, "All-Risks policies are designed to provide cover against physical damage to property, yet many pre-2018 policies do not explicitly or implicitly exclude cyber risk and thus may provide cover, termed 'silent cyber' by the insurance industry."[6]

Bahar advised that in light of the Merck case, and because of the new geopolitical instability and heightened risk of cyberattacks, companies should closely examine their insurance policies "to ensure sufficient coverage."

Today, companies frequently rely on cyber-specific insurance policies. In fact, businesses with such policies did not have their NotPetya claims denied.

But insurers are worried. Ransomware attacks continue to soar. And insurance rates are rising — 130% in the U.S. and 92% in the U.K. in the fourth quarter of 2021, according to Marsh, a leading insurer.[7]

"If cyber criminality continues unchecked, [insurance] will become unaffordable," noted Adrian Cox, CEO of the London-based insurer Beazley, in the *Financial Times.*

What other ways are insurers dodging cyber claims payouts?

Cyber insurance coverage is already challenging enough to get and keep in these days of constant ransomware attacks. Now, companies apparently need to worry about insurers taking them to court to rescind their policies — as if they never existed.

In late August, Travelers Property Casualty Company of America and International Control Services (ICS) reached an agreement in an Illinois federal court to approve the cancellation of ICS's policy and any claims for coverage following a recent ransomware attack. Travelers alleged in its suit that when ICS filled out its application for cyber-risk insurance, it misrepresented having multifactor authentication (MFA), which most such policies currently require. (Travelers and ICS did not respond to requests for comment.)

The fact that a major insurer sought to avoid paying a claim isn't surprising. Insurers do that all the time. But challenging the validity of an already issued policy is highly unusual for any coverage type and should send a warning to companies seeking cyber-risk insurance to proceed carefully.

Why pick a fight?

While policyholders shouldn't expect such lawsuits to become commonplace, there will probably be more of them, according to Scott Godes, a partner and co-chair of the insurance recovery and counseling practice at Barnes & Thornburg, a national law firm that represents companies in insurance recovery cases.

"Carriers have quietly been threatening to use policy rescission as a 'nuclear option' for some time," **he told *Focal Point.*** "It's super disappointing to see it. It's a model, in my opinion, of blaming the policyholder as opposed to engaging in more careful loss control. It's a model of using ambiguous and cleverly worded application questions against policyholders."

Godes is referring to a practice of putting the onus on companies to regularly attest to the actions they've taken to strengthen cybersecurity instead of partnering closely with policyholders to ensure they are meeting security posture expectations. After an attack, insurers put a policyholder's cybersecurity readiness under particular scrutiny. A forensic investigator is often assigned to verify the accuracy of the cybersecurity practices a company reported on its insurance application.

Insurers should work more collaboratively with policyholders to head off cyberattacks and to avoid any confusion that could lead to disagreement, Godes told *Focal Point.* Some carriers already do this for other forms of insurance. For instance, some insurers advertise that they could provide discounted rates to motorists who are willing to place a device in their cars to monitor their driving habits. Insurers could employ a similar "loss control" strategy when writing cyber-risk policies, rather than use answers to applications as "trapdoors," Godes argues.

However, many businesses are hesitant to share detailed information about their cybersecurity practices. They worry about insurers sticking their noses where they might not belong or about the potential legal implications of divulging security practices.

Tackling tedious applications

Given these difficulties and the growing spate of ransomware and other cyberattacks, many cyber insurers are requiring applicants to complete lengthy and unwieldy questionnaires to qualify for coverage, says Josephine Wolff, an associate professor of cybersecurity policy at the Fletcher School at Tufts University and author of *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks.*

"These applications have gotten so long now," Wolff explained, in an exclusive interview with Focal Point, "that some companies put teams of three or more people into rooms and tell them, 'Answering this questionnaire is your job for the next month.'"

Of course, devoting that much time takes away from other work. A more common practice is for someone in the office of the CISO, CIO, CFO, or treasurer to fill out insurance paperwork.

The problem: It's unlikely that one person will have the background or time to answer every technically detailed question accurately and completely. As a result, errors, omissions, and misrepresentations happen and spur insurers to deny claims or, as Travelers demonstrated with its precedent-setting case, rescind coverage.

"I think the biggest thing you will see is, as people misrepresent things on their policies, either intentionally or unintentionally, insurance companies will push back," says Gerry Glombicki, senior director at Fitch Ratings, a top credit-rating agency, in a recent ***Focal Point* article.**

> **"I think the biggest thing you will see is, as people misrepresent things on their policies, either intentionally or unintentionally, insurance companies will push back"**
>
> **Gerry Glombicki**
> Senior director, Fitch Ratings

Picking their battles

But even if others follow Travelers' lead, industry observers maintain they will probably do so sparingly. *Focal Point* recently asked three **experts to weigh in** on the possibility of taking cyber insurance policyholders to court. The optics, they concur, aren't great.

"It really doesn't serve the insurance companies well to get wrapped up in a whole bunch of litigation where they're trying to void coverage based on technicalities," says David Anderson, U.S. head of cyber at reinsurance broker McGill and Partners.

"I'm surprised that this kind of litigation occurs in the first place," agrees Sean O'Brien, visiting fellow at the Information Society Project at Yale Law School. "It's a horrific strategy because it's going to result in nobody having faith in these products. They have enough difficulty selling cyber insurance."

"It's a slippery slope," adds Gerry Kennedy, principal at Charles River Insurance. "You're purporting to provide coverage to policyholders when they need it. But then you pull the rug out from underneath them [by rescinding contracts] when that time comes? Most people would say, 'It would have been nice to know there was that possibility before you denied my claim.'"

Strengthen your coverage with cyber hygiene

While no security expert can guarantee a future free from cyberattacks (or the litigation that may spring from them), there are some basic cyber hygiene practices that business and tech leaders can take to lower their risk.

A cyber risk score identifies an organization's level of exposure to cybercrime and the liabilities that stem from IT vulnerabilities. A risk score report communicates the strength of an organization's IT asset management program internally and externally.

LEARN MORE

- **Practice cyber hygiene.** This is not just enthusiastic advice to be ignored like those shout-outs from your Peloton instructor. According to a recent Fitch Wire Post, cyber insurance companies are now demanding "better cyber hygiene requirements for policyholders, such as multifactor authentication."

  Good hygiene practices typically include having MFA, endpoint protection, robust AV, up-to-date redundant and offline backups, and security awareness and training programs. The rising number of cyber-hygiene prerequisites can be frustrating for executives, but the constraints provide an opportunity for CISOs to talk to their C-suite about the need to fund more cybersecurity upgrades across the organization.
- **Evaluate your cyber risk.** A cyber-risk score can alert you to weaknesses in your cybersecurity strategy and spotlight preventable errors, like failing to install software updates or manage configurations. Risk scoring also shows off your strengths. Like a calling card or marketing tool, it's a way to announce your organization's cyber attributes to insurers, executive boards, and supply chain partners. Even a poor risk score is useful, giving security leaders the precise and necessary data to set new priorities and increase IT budgets.

- **Automate wherever you can.** This can't be repeated enough. IT departments are understaffed. Workers are burned out. Automation tools reduce the risk of human error; they bolster your security squad, replacing manual provisions with scripts and configuration files managed by machines. They can handle a host of low-level tasks, from password resets to patch management to identifying and mitigating threats. They can improve incident response by consolidating threat information from multiple sources, and the fact that *hackers* are also using these tools (hello, NotPetya) speaks volumes.

  Automation tools also communicate to insurance underwriters, demonstrating that despite a small staff or limited budget, your security systems are configuring, patching, and password resetting quickly and regularly.

- **Make friends with your cyber insurance policy underwriter.** Insurers are asking more of clients. Literally, questionnaires used to set rates are getting lengthier and more detailed. Don't take that the wrong way. "If you feel like you're being grilled … it's because we need to get as good an understanding [of your business] as possible," Paul Gooch, a cyber underwriter with Tokio Marine Kiln, said on Dale Peterson's *Unsolicited Response* podcast. "Try not to see it as adversarial."

That last bit of advice holds true in times of war or peace. As easy as it is to imagine underwriters as out to extort as much money from clients as possible, the reality is less colorful.

If underwriters rejected all clients and denied all claims, the market wouldn't exist.

Cyber underwriter Monica Tigleanu, of Munich Re, agreed. "It's important that the community educates underwriters [as to] why they made certain decisions," she told ***Focal Point.*** "We just need to understand the controls in place that will make those asset owners resilient."

> "It's important that the community educates underwriters [as to] why they made certain decisions."

Monica Tigleanu
Cyber underwriter, Munich Re

Reducing your legal risk

No one likes unpleasant surprises. So *Focal Point* recently asked industry observers how to best take precautions. They recommend the following.

Take the questionnaire seriously

As cumbersome as these applications have become, they are legally binding statements of fact. Litigation can arise anytime there's ambiguity. Before filling out an application, Anderson from McGill and Partners recommends forming a cross-functional risk-management team to gather all the operational and technical detail that will be needed to supply the most complete and accurate answers.

Lawyer up

Anderson also suggests getting an attorney involved early on to help guide the process and review questionnaire responses. "Everything you put in writing to insurance companies is a representation, whether your signature is on it or not," he says. "Hiring an attorney is an expensive process, and not a lot of companies, especially mom-and-pop shops, can do it. But if you can, it's advisable."

Map your exposure

During the application process, it's important to remember that cybercriminals often attack third parties. It could become an issue down the road if a company represents that it has MFA but doesn't make sure its affiliated partners and vendors use it as well, notes Kennedy of Charles River. He suggests communicating with the insurer to understand if third-party risk management is one of its expectations and, if so, pinning them down on its requirements.

Know what you're attesting to

The buck stops with whoever signs on the dotted line of a cyber insurance application. If an issue occurs later, that's the person who will be in the crossfire of any legal proceedings. For that reason, Fitch's Glombicki stresses that the signatory, who is ideally a senior leader, should know what they are attesting to —for their own protection as well as the organization's.

Be forthcoming

Wolff of Tufts notes that the worst thing a company can do is gloss over the truth. Though they don't need to overdo it with details, executives should be as forthcoming as possible to avoid accusations of misrepresentation. For example, if a company has deployed MFA in some places but not others, executives should identify where it exists and where it does not.

Understand what's in the policy

When applying for cyber insurance, don't assume your policy protects against every imaginable scenario. Insurance doesn't work that way. It's extremely important, therefore, to understand what's in a policy and pay particular attention to stated exclusions, warns Eric Gyasi, an attorney and vice president at Stroz Friedberg, an Aon company.

"That may sound a little trite, but organizations tend to set it and forget it," he says. "In fact, a policy may not cover what you thought it was covering."

Don't assume your policy protects against every imaginable scenario. "In fact, a policy may not cover what you thought it was covering." Eric Gyasi, Attorney & VP, Stroz Friedberg, an Aon company.

Insurers aren't yet lining up to rescind policies they've issued. But observers believe more suits like Travelers v. ICS will almost certainly follow as the industry seeks to refine its risk models and rules.

As Godes of Barnes & Thornburg warns: "Companies should be mindful that carriers are taking more aggressive and strict constructionist views on their applications — and react accordingly."

Conclusion

The pressure on business, tech, and cybersecurity leaders has never been greater. They must spot and mitigate digital risks and educate their workers on the value of proper cyber hygiene, all while calculating exactly what their insurers will and won't pay for when an inevitable breach occurs.

Get started by understanding your cyber risk. Sign up for **Tanium's risk assessment** and get a comprehensive view of your risk posture at no cost.

Endnotes

[1] https://www.gao.gov/products/gao-21-477

[2] https://www3.ambest.com/ambv/sales/bwpurchase.aspx?record_code=320999&altsrc=

[3] https://www.usnews.com/news/articles/2013/02/20/former-cia-director-cyber-attack-game-changers-comparable-to-hiroshima

[4] https://www.washingtonpost.com/news/post-politics/wp/2014/12/21/obama-north-korea-hack-cyber-vandalism-not-act-of-war/

[5] https://www.insurancejournal.com/news/national/2022/02/04/652272.htm

[6] https://www.jdsupra.com/legalnews/merck-and-international-indemnity-v-ace-4184468/

[7] https://www.marsh.com/us/services/international-placement-services/insights/global_insurance_market_index.html

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.