Cyber Insights 2023: Cyberinsurance

About SecurityWeek Cyber Insights | *At the end of 2022, SecurityWeek liaised with more than 300 cybersecurity experts from over 100 different organizations to gain insight into the security issues of today – and how these issues might evolve during 2023 and beyond. The result is more than a dozen features on subjects ranging from AI, quantum encryption, and attack surface management to venture capital, regulations, and criminal gangs.*



CYBER INSIGHTS 2023

SecurityWeek Cyber Insights 2023 | Cyberinsurance – Cyberinsurance emerged into the mainstream in 2020. In 2021 it found its sums were wrong over ransomware and it had to increase premiums dramatically. In 2022, Russia invaded Ukraine with the potential for more serious and more costly global nation state cyberattacks – and Lloyds of London announced a stronger and more clear war exclusions clause.

Higher premiums and wider exclusions are the primary methods for insurance to balance its books – and it is already having to use both. The question for 2023 and beyond is whether the

cyberinsurance industry can make a profit without destroying its market. But one thing is certain: a mainstream, funds rich business like insurance will not easily relinquish a market from which it can profit.

It has a third tool, which has not yet been fully unleashed: prerequisites for cover.

The Lloyd's war exclusion clause and other difficulties

The Lloyd's exclusion clause dates to the NotPetya incident of 2017. In some cases, insurers refused to pay out on related claims. Josephine Wolff, an associate professor of cybersecurity policy at Fletcher, Tufts, has written a history of cyberinsurance titled *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*.

"Merck and Mondelez, sued their insurers for denying claims related to the attack on the grounds that it was excluded from coverage as a hostile or warlike action because it was perpetrated by a national government," she explains. However, an initial ruling in late 2021, unsealed in January 2022, indicated that if insurers wanted to exclude state-sponsored attacks from their coverage they must write exclusions stating that explicitly, rather than relying on boilerplate war exclusions. Merck was granted summary judgment on its claim for $1.4 billion.

The Russia/Ukraine kinetic war has caused a massively increased expectation of nation state-inspired cyberattacks against Europe, the US, NATO, and other west-leaning nations. Lloyds rapidly responded with an expanded, but cyberinsurance-centric, war exclusion clause excluding state-sponsored cyberattacks that will kick in from March 2023.

But “who gets to decide whether an attack is state-sponsored?” asks Wolff. “And what does it even mean for the attack to be state sponsored: that it was perpetrated by government employees? Or paid for by a government? Or even just tacitly permitted by a government? And state-sponsored cyberattacks are not rare occurrences – an exclusion for them is very different from a war exclusion that deals with a fairly well-specified and infrequent event.”

She is not alone with such concerns. “The issue here lies in the murky waters of attribution” explains Chris Denbigh-White, cybersecurity strategist at Next DLP. “Was the attack ‘state-conducted?’ Was it ‘state sponsored?’ Was it ‘state inspired?’ or was it simply a criminal organization piggybacking an existing conflict for financial gain?”

“Looking ahead,” continued Wolff, “I think insurers and their policyholders are going to find themselves mired in a lot of fights about attribution and how to define what makes a cyberattack state-sponsored or catastrophic or uninsurable.” Two things are certain: security defenders will have increased questions over the cost/return value of cyberinsurance, while insurers will be seeking new ways to ensure their market doesn’t disappear.

The insurers have one major advantage: insurance has been a staple part of business for centuries, and business leaders don’t seem inclined to exclude it from security. Joseph Carson, chief security scientist and advisory CISO at Delinea, notes that his own firm’s survey reveals 33% of IT decision makers applied for cyberinsurance due to a requirement from their board and executive management.

He also notes that 80% had subsequently called upon that insurance with more than half doing so more than once. “As a result of more cyber insurance policies being introduced, and ultimately many businesses needing to use them,” he comments, “the cost of cyber insurance is continuing to rise at alarming

rates. I expect to see this continue in 2023.”



Jerry Caponera

The insured’s concern over a falling return on investment is not the only worry for the insurers – whether we are in a defined recession or not, the world is certainly suffering an economic downturn. This is already having affecting security budgets. “Companies spent massively during the pandemic, and now that the economy has cooled, spending will go back to 2019/2020 levels,” explains Jerry Caponera, GM at ThreatConnect.

“A very likely outcome of this,” he continued, “is that more companies will fall below the cybersecurity poverty line (CPL). With inflation currently [at the time of writing] over 8% – measuring 4x higher than the central bank’s target rate of 2% – companies who hadn’t planned for increased costs will find themselves with less money to spend on cyber, thus falling further below the CPL and finding themselves facing the hard decision on where to spend their next investment dollar.”

Firms will increasingly need to choose between cybersecurity mitigations or cyberinsurance – and neither of these options on their own will benefit the insurance industry.

Insurers’ response

2023 is a watershed moment for cyberinsurance. It will not

abandon what promises to be a massive market – but clearly it cannot continue with its makeshift approach of simply increasing both premiums and exclusions to balance the books indefinitely.

One option would be to become more granular in the cover it offers. Instead of a single cybersecurity policy with a long list of exclusions, it could offer coverage in specific areas only. This would allow coverage to be more tightly defined with fewer if any exclusions. Further, suggests Chris Gray, AVP of security strategy at Deepwatch, it would "allow basic risk management into services while providing the ability to charge increased premiums for more upscale/impactful attacks."

This approach is not without precedent in other industries. The Food Liability Insurance Program (FLIP) provides Insurance designed for small food businesses with gross annual receipts under $500,000. The Forward Contract Insurance Protection (FCIP) plan is a supplemental insurance that provides an indemnity for farmers unable to deliver contracted volumes.

"Government intervention in the form of sanction insurance programs – a la TRIP, FLIP, FCIP, etcetera – is likely to evolve, with a significant discussion regarding coverage areas and their impact on national security," suggests Gray.

One of the strongest likelihoods over the coming years, however, is the growth of cybersecurity requirement impositions; that is, insurers will decline coverage unless the insured conforms to a specified security posture. This is the final option – when you can no longer increase premiums and exclusions, you have to reduce claims. And this is best achieved by helping industry prevent cyber incidents.

It may still not be enough. Chris Denbigh-White, cybersecurity strategist at Next DLP, argues, "The notion of 'insuring away cyber risk' will become (and arguably always was) somewhat unrealistic. Insurance premiums, prerequisites and policy

exclusions will no doubt continue to increase in 2023 which will have the effect of narrowing the actual scope of what is really covered as well as increasing the overall cost."

Nevertheless, the expansion of 'prerequisites' would be a major – and probably inevitable – evolution in the development of cyberinsurance. Cyberinsurance began as a relatively simple gap-filler. The industry recognized that standard business insurance didn't explicitly cover against cyber risks, and cyberinsurance evolved to fill that gap. In the beginning, there was no intention to impose cybersecurity conditions on the insured, beyond perhaps a few non-specific basics such as having MFA installed.

But now, comments Scott Sutherland, VP of research at NetSPI, "Insurance company security testing standards will evolve." It's been done before, and PCIDSS is the classic example. The payment card industry, explains Sutherland, "observed the personal/business risk associated with insufficient security controls and the key stakeholders combined forces to build policies, standards, and testing procedures that could help reduce that risk in a manageable way for their respective industries."

He continued, "My guess and hope for 2023, is that the major cyber insurance companies start talking about developing a unified standard for qualifying for cyber insurance. Hopefully, that will bring more qualified security testers into that market which can help drive down the price of assessments and reduce the guesswork/risk being taken on by the cyber insurance companies. While there are undoubtedly more cyber insurance companies than card brands, I think it would work in the best interest of the major players to start serious discussions around the issue and potential solutions."



Bob Ackerman

Bob Ackerman, MD and founder of AllegisCyber, agrees with Sutherland about the way forward for cyberinsurance, but is damning about its progress so far. “Unfortunately, insurers have struggled to take advantage of the opportunity, writing policies with numerous exclusions, high deductibles, and low coverage caps, and showing massive losses in the process. The market opportunity will require insurers to become proactive in defining performance thresholds in order to be ‘insurable’.”

He believes a PCIDSS-style model could be the solution. “By setting standards and measuring related performance, insurers can help define ‘cyber secure’ and build a profitable book of business in the process.”

Mark Lance, VP of DFIR and threat intelligence at GuidePoint Security, even suggests what it might look like. “We’ll continue to see an expansion from traditional questionnaires to actual validation, which will not only include a baseline of standard security solutions (EDR, PAM, MFA), their associated and current configurations (ASM) but also the presence of standard policies (IR Plans, Playbooks), and execution capabilities (Proof of User Awareness Training and Tabletop validation).”

Mike McLellan, director of intelligence at Secureworks, adds, “The requirements on organizations wishing to obtain cyber insurance will become more and more stringent, and organizations that are unable or unwilling to comply will find

coverage is declined."

Whether a PCIDSS style cyberinsurance standard can work is a separate question. While PCIDSS is a well-respected security standard, it has not eliminated the criminal theft of payment card details. GDPR has not eliminated the theft of PII. Put simply, successful cyberattacks cannot be eliminated by cybersecurity tools.

But to even reach the stage of a defined cyberinsurance standard, the insurance industry will either have to get into bed with existing security vendors or become a cybersecurity company itself. The former is worrying – depending on the closeness of the relationship and the degree to which the vendor seeks to satisfy the insurance industry rather than its own customers – while the latter is doomed to failure. The more mature security vendors have been working for more than two decades on eliminating cyber threats with varying but ultimately little success.

Whether or not a full cyberinsurance security standard emerges, there will be increasing cooperation if not collaboration between insurers and security vendors in 2023. "The borderless nature of networks, coupled with a threat landscape that is less predictable, necessitates the need for true risk quantification of companies' security controls now more than ever. With that, I expect to see more investment into quantifying cyber risk. This will drive better collaboration and data sharing between security companies," explains Jason Rebholz, CISO at Corvus Insurance. "Cyber insurance carriers will lean into partnerships with technology companies to fuse security data with insurance and risk modeling insights. The net result is more accurate risk quantification, which will in turn help keep policyholders safer."

There is no silver bullet for cybersecurity. Breaches will continue and will continue to rise in cost and severity – and

the insurance industry will continue to balance its books through increasing premiums, exclusions, and insurance refusals. The best that can be hoped for from insurers increasing security requirements is that, as Norman Kromberg, MD at NetSPI suggests, “Cyber Insurance will become a leading driver for investment in security and IT controls.”

An interesting comment comes from Jennifer Mulvihill, business development head of cyberinsurance and legal at BlueVoyant: “The underwriting process and the completion of an underwriting application are excellent ways to self-assess and consider the protection of assets from a cyber perspective. The information gleaned from these exercises is valuable information, not only for the CISO, but for the Board and CFO, and augments financial investments and regulatory compliance.” Insurers could charge for the right to apply for insurance, but if a prospective customer must pay, that customer could simply pay a cybersecurity consultant for the same service and ignore insurance altogether.

Summary

It is unlikely that the insurance industry will be able to balance its books through raising premiums and reducing payouts through increasing exclusions, nor yet eliminate claims through a required cybersecurity standard. The threats are too varied and too extreme.

“Obtaining or maintaining a policy is a challenge at scale,” comments Corey O’Connor, director of products at DoControl. “The bigger your business grows, the more challenging it will be to meet these requirements. More and more organizations were being dropped by providers throughout the last year, and going into 2023 there will likely be a trend of organizations being unable to receive coverage.”

It may be that government will be dragged into the equation. “I think there’s going to be pressure on governments to

clarify under what circumstances they'll provide some sort of backstop for coverage of catastrophic cyberattacks, pressure on insurers to not exclude too many types of attacks, and pressure on policyholders to challenge these exclusions in court if their claims are denied," suggests Josephine Wolff. "Rising premiums don't seem to have deterred businesses from buying cyberinsurance, so I don't know that these new types of exclusions will either, but I wonder how well they'll hold up in the face of a major cyberattack."

"Will Cyber insurance become an expensive 'tick in a box' or will it deliver real value?" asks Denbigh-White. "Will it even remain a viable offering from insurance companies in 2023? While carrying cyber insurance is rapidly becoming a 'security prerequisite' for many organizations, its benefit in relation to cost and cover remain uncertain as we move into 2023."

But "Rule no.1," warns Mark Warren, product specialist at Osirium. "Insurance always wins!" Insurance will get more expensive, more difficult to get, and less likely to pay out. "As a result, more organizations may decide not to take out insurance at all, instead focusing on ploughing resources into protection. If this happens, we can expect to see insurance companies partnering with big consulting firms to offer joined up services."

He fears that buying cyberinsurance may simply become a cost of doing business. "Pointless it may be, if insurers are never going to pay out… but buying cyber insurance may simply become a necessary cost of doing business – a box that must be ticked to demonstrate to shareholders that all steps are being taken to protect the business and ensure resilience and continuity."

Related: The Case for Cyber Insurance

Related: The Wild West of the Nascent Cyber Insurance Industry

Related: Cyber Insurance Firm Coalition Raises $250 Million at $5 Billion Valuation

Related: Cyber Insurance Firm Cowbell Raises $100 Million

About SecurityWeek Cyber Insights | *At the end of 2022, SecurityWeek liaised with more than 300 cybersecurity experts from over 100 different organizations to gain insight into the security issues of today – and how these issues might evolve during 2023 and beyond. The result is more than a dozen features on subjects ranging from AI, quantum encryption, and attack surface management to venture capital, regulations, and criminal gangs.*



CYBER INSIGHTS 2023

Cyber Insights 2023: Cyberinsurance