CYBERSCOUT®

Cyberscout Shares Top Cyber Insurance Industry Predictions for 2021

Cyber insurance will go mainstream to address spike in cyber risk for individuals and small businesses

> We anticipate that 2021 will be a turning point for many insurers who have remained too narrowly focused on underwriting and not claims management in the growing cyber risk sector. Cyber insurance will go mainstream in 2021, cyber insurance professionals will be in high demand and the complexity of cyberattacks will demonstrate the need for co-mingling of expert services with claims handling.
>
> - Matt Cullina, Managing Director, Global Markets, Cyberscout

1.

Standard insurers will get a wake-up call about cyber insurance

In a recent report from Allianz, the number of cyber insurance claims has steadily risen over the last few years, up from 77 in 2016, when cyber was a relatively new line of insurance, to 809 in 2019. In 2020, there were already 770 claims in the first three quarters. The outbreak of cyberattacks that impacted hospitals, manufacturing companies, schools, small businesses, social media accounts and more following news of the COVID-19 outbreak, should serve as a wake-up call for insurers across the spectrum. Regardless of the industry, every organization has moved from having an increased reliance on digital technologies to being uber reliant, and as a result even more vulnerable to cyberattack. Even farm insurance policies are starting to include cyber coverages as a standard offering. Insurance companies and brokers need to understand the risks and threats that cybercrime poses to businesses of all shapes and sizes and offer appropriate coverages across their portfolio.

2.

Personal cyber insurance will become a "must-have" in personal lines insurance packages

COVID-19-related phishing attacks increased 667%, according to a recent study by data security company, Baracuda. Consumers are becoming more aware that a breach of personal information or financial fraud resulting from a cyberattack won't always be covered by someone else – like a business or their financial institution. As cybercrime continues to proliferate our daily lives, consumers will seek policies that accurately reflect the risks they encounter – and they won't want to seek out a standalone policy – they'll expect to see cyber cover in home, auto or even life insurance policies.

3. Cyber insurance brokers will be in high demand

Due to the highly specialized nature of cyber risks and insurance intelligence, insurers will be scrambling to fill these positions as cyber insurance continues increasing in demand. The talent shortage in cyber insurance will lead many insurers to outsource specialty work to partners that can fill that gap.

4. Remote work will continue to blur the lines between personal and commercial security risks

When the pandemic is over, one in six workers is projected to continue working from home or co-working at least two days a week, according to a recent survey by economists at Harvard Business School.

While global vaccine distribution is on the horizon, many knowledge workers will continue working remotely through much of 2021. Attacks on remote learners using their parents' business computer, phishing campaigns sent to a personal email that infiltrates a business network, and, the general distraction of living, learning and working from home will continue to complicate cyber insurance market coverages. These conditions highlight the gaps in many cyber policies, which were designed for commercial lines or large corporate risks and not small business and personal lines where much cybercrime is occurring.

5. Complexity of double extortion ransomware attacks will require crisis management, not just coverages

2020 saw increases in double-extortion ransomware in which attackers are not only capturing and encrypting sensitive data and demanding ransom for decryption, but they are now also first exfiltrating data from the victim and threating to post it publicly unless the ransom is paid. Today's victims now have three significant concerns around ransomware – regaining access to critical business data and systems, identifying what data might have been exfiltrated and reporting obligations after the attack. Ransomware claims are increasing in both dollar value and complexity, and insurers will increasingly need expert forensic investigation and breach support services to support their clients through an attack and help manage the crisis, not just clean-up the aftermath.

6. Social engineering scams—including business email compromise—will outpace ransomware

Ransomware can be lucrative, but it's time-intensive. Cyber criminals are looking for the quickest and easiest return. We will see criminals continue to take advantage of the disinformation age and try to monetize victims faster and more efficiently than ever before. Education will continue to be an important defense, but organizations will need to consider investing in tools for security. Deploying multi or two-factor authentication, conducting phishing simulations, using geo filters and creating a zero (or less) trust environment will need to become standard practice to protect business networks.

7. The role of cyber risk management services will increase to offset claims

that traditional liability insurance policies and other cyber coverages did not properly price for today's cyber risk exposures. With the frequency and severity of claims on the rise, cyber insurers across the globe have started to tighten their risk appetites, underwriting guidelines and take rate. Offering services, like a 24/7 Fraud Center helpline for policyholders can address their cyber problems before it results in a claim.

8. A cyber capital capacity crisis will emerge

Poor performance of mid-market commercial cyber policies and a failure to diversify downwards into small business and personal lines risks will force secondary capacity to exit the market. Fewer brands in the market will make it impossible for all existing specialty insurance brokers to find capacity to continue trading, some direct full-stack brands will find it hard to reinsure against these risks and exit the market.

9. East will outpace west

Consistent with their progressive moves on data privacy regulations, we are seeing faster growing market appetite for personal and commercial cyber lines in emerging markets in Asia-Pacific. We anticipate adoption rates in Asia will overtake Western Europe and challenge North America before the turn of the next year. Also look out for cyber insurance launches geared towards SME commercial & personal lines insureds in the Middle East, Africa and Latin America as those markets will also start to heat up.

10. Cyber Insurance solutions will be deployed via alternate distribution strategies

Telcos, employee benefits brokers, mobile phone providers, SAAS companies, large retailers and banks are just a handful of verticals that will start to deliver cyber insurance solutions to their customers, members and employees.

About Cyberscout

Since 2003, Cyberscout has been a leader in protecting businesses, individuals, and families against hackers, thieves, and human error. We deliver unrivaled cyber risk education, identity protection, and fraud resolution services, as well as swift cyber incident response services around the world. From ransomware attacks to identity theft, email scams, to privacy data breaches, Cyberscout provides advanced tools and expert support services that educate and empower people around the globe. Cyberscout solutions are available in more than 45 countries, with offices in Galway, Ireland, Montréal, Canada, and Scottsdale, Arizona.