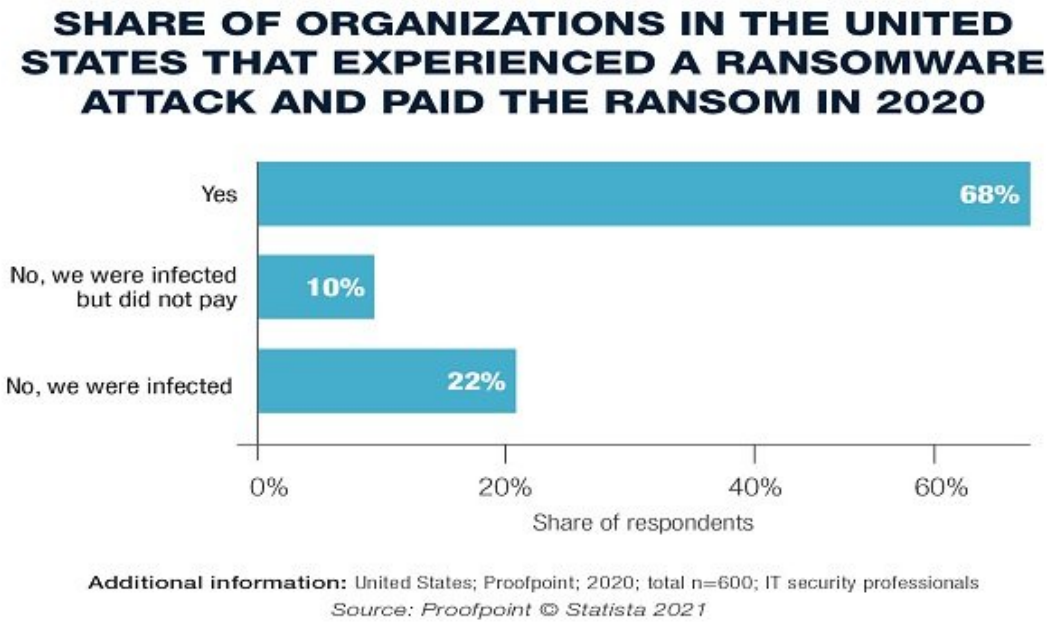
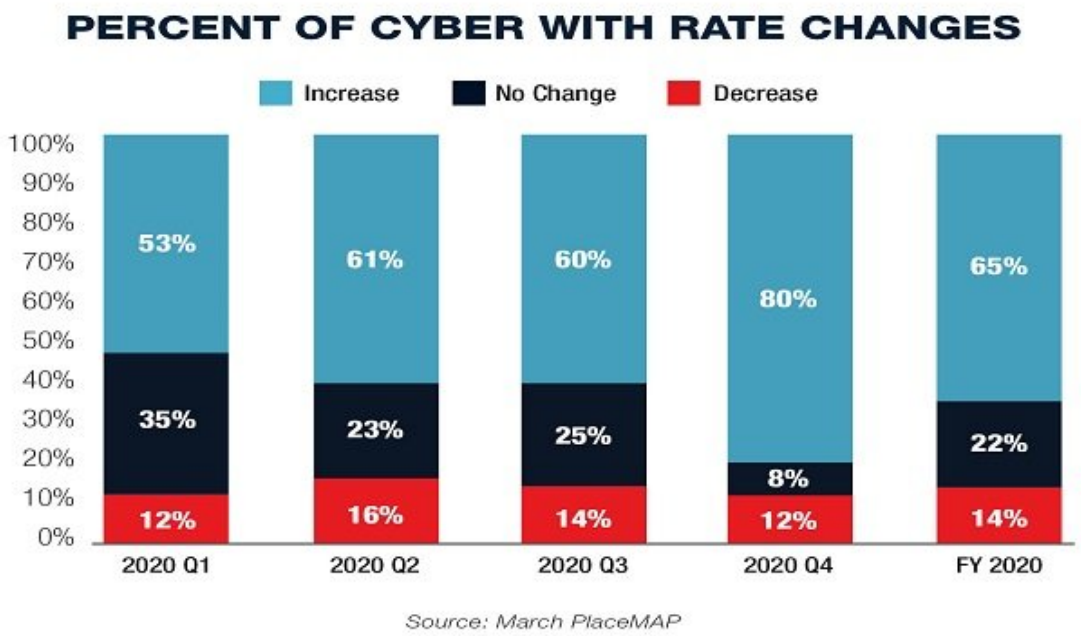
2021 Cyber insurance market update

Web of Risks: Cyber insurance rates swell and capacity tightens as digital threats and losses become more frequent and severe.

By Steve Hallo | July 30, 2021



The cyber insurance market is beginning to see sub-limits, particularly for ransomware losses. (Graphic by Statista)



Cyber insurance premiums have been increasing — even doubling in some cases. (Graphic by Marsh PlaceMAP)

Cyber risks are growing in frequency (https://www.propertycasualty360.com/2021/07/28/personal-cyber-risks-working-smart-in-a-hybrid-environment/), severity, and complexity, making them among the biggest threats of our time facing businesses and their insurers. Cybersecurity breaches are happening at a rapid pace because malicious actors continue to evolve their techniques while targeting new victims in an effort to stay one step ahead of today's best risk-mitigation strategies.

How does that translate into dollars? The collective additional cost and lost revenues companies face from cyberattacks could reach as much as $5.2 trillion during the coming three years, according to a report from Accenture plc. Meanwhile, the data and analytics company GlobalData has reported that gross written premiums for the cyber insurance market (https://www.propertycasualty360.com/2021/01/05/cyber-insurance-trends-to-look-for-in-2021/) are projected to reach $20.6 billion by 2025.

Mounting menace

In 2020, "we saw a series of significant cyber incidents and ransomware attacks, including the shopping platform Magento and the SolarWinds hacks," Kenneth Saldanha, Accenture's global insurance lead, explains. The latter alone impacted up to 18,000 companies, including multiple U.S. government agencies, and it has been estimated that it could cost cyber insurers $90 million."

As a result of growing cyber losses, coverage rates in the cyber insurance sector have ballooned year-over-year at a significant pace.

"There is a wide range of rate activity by segment, industry class and risk quality," says Thomas Kang, North American head of cyber, tech and media at Allianz Global Corporate & Specialty (AGCS). "However, the broader market is seeing premium increases (https://www.propertycasualty360.com/2021/04/29/how-revenue-data-influence-cyber-premiums/) between 20% and 50%."

Cyber insurance was previously considered an optional investment for companies with minimal sensitive data.

"The ubiquitous rise in cybercrime impacting all industries and market segments has since proven that being prepared to defend against existential cyber threats to a business is no longer optional," Kang says. "It is critical that companies — across all industry segments — understand the business risk presented by cyberattacks and ensure proper investment to manage the risk."

These issues are leading to supply and demand challenges in the cyber insurance market, Saldanha says. He notes the sector has a high ceiling for individual losses and potential for risk accumulation as well as large capital requirements. As a result, fewer insurers are writing these types of policies, and those that do aren't willing to hold too much of this risk.

"At the same time, cyber reinsurance capacity is finite," he says. "This rising demand has led to competition for capacity, hence increasing prices."

The market also is beginning to see sub-limits, particularly for ransomware losses. This hasn't historically been the case, according to Sandy Codding, head of cyber for Swiss Re.

Codding explains that while premiums have been increasing — even doubling in some cases — an unanswered question lingers: Are those increases adequate for the rate at which the exposure is increasing?

"My perception is all insurers are experiencing dramatic increases in losses, primarily due to ransomware," Codding says.

Cyber risks and ransomware events are now among the costliest risks to today's businesses. (Illustration by Shaw Nielsen)

Ransomware worries

Ransomware has become the face of cyber loss, says Timothy Zeilman, Hartford Steam Boiler vice of global product owner-cyber. Ransomware is also a major reason that organizations and businesses no longer consider cyber coverage to be optional.

"That thinking has changed," Zeilman says. "No one is safe from ransomware. It is a broad-based threat, and the awareness of that has increased."

But, he adds, "cybersecurity-threat awareness could still be better."

The eye-popping sums that hackers now demand are unfortunately driving cyber-risk cognizance. Accenture's Cyber Threatscape report found a 60% increase in the average ransomware payment between the first and second quarters of 2020.

"This is especially concerning for insurers as these saboteurs will often set the ransom based on the victim's level of cyber insurance coverage," Saldanha says.

The rise in ransomware incidents is leading many to ask if paying hackers is a prudent move. In fact, some suggest the industry is driving bad actors to ask for more money, knowing insurance will cover the loss.

Some industry players are starting to say "no more." In May 2021, French insurer AXA announced it would no longer write policies that included reimbursement coverage for ransomware extortion payments, according to the Associated Press, which noted it was an industry first. AXA's plan only applies to France and doesn't impact existing policies, nor does it affect coverage for recovering from a ransomware attack.

Swiss Re's Codding says the decision to pay a ransom or not is always tough.

"I feel, at least for today, that not allowing payment is going to create a lot of pain for companies because so many are unprepared for an event," Codding explains. "If they can't or don't pay to recover data, it can be months to restore operations. And that is a substantial problem. It is not ideal to pay it, but sometimes it is really the best choice."

This dilemma played out in headlines recently as the operator of the Colonial Pipeline Co. reportedly attempted to rebuff hackers' demands after they had shut down the country's largest fuel pipeline. However, those early reports were quickly proven false, and the company shelled out nearly $5 million to restore pipeline operations, Bloomberg reported.

Weak links

The past year also has shown vulnerabilities when it comes to third-party vendors, such as the aforementioned SolarWinds incident as well as the MS Exchange breach, leading to a spike in so-called "supply-chain attacks."

During the first quarter of 2021, nearly 140 organizations reported being impacted by a supply-chain incident. Such breaches saw an increase of 42% during that period compared with the prior quarter, according to the nonprofit Identity Theft Resource Center.

The real problem with supply-chain attacks is their potential for widespread damage. For example, a single breach of IT provider Blackbaud detected in May 2020 impacted more than 12 million individuals and 550 organizations.

Supply-chain attacks also can result in a spike in insurance claims, which is expected with the MS Exchange event, an incident that hit Microsoft's best-selling email service. The insurance and reinsurance industries are likely to see a "long-tail of attritional claims" stemming from the incident, according to cyber analytics firm CyberCube. Associated claims are likely to focus on legal, forensic and clean-up costs.

"The insurance industry is only just beginning to understand the scope of possible damage. It is too early to calculate potential losses from the theft of a corporation's intellectual property," William Altman, cybersecurity consultant at CyberCube, said in a release. "An accumulation of loss could result in multiple —

theoretically, tens of thousands — of companies making insurance claims to cover investigation, legal, business interruption and possible regulatory fines."

Regulatory picture

As a result of COVID-19, regulatory exposures in 2020 as well as into 2021 had less impact on the market than initially anticipated, according to Paul Needle, senior vice president and cyber treaty underwriter for Munich Re U.S.

However, this is unlikely to be the case for long.

"The Information Commissioner's Office (ICO), which is responsible for enforcing the U.K.'s GDPR (General Data Protection Regulation), publicly noted that corporate penalties — including fines issued to Marriott and British Airways — were significantly reduced due to the impact of the pandemic on the penalized entities," he says.

Of note, however, was the passage of the California Privacy Rights Act (CPRA), which updates and expands the state's cybersecurity laws and increases alignment between the CCPA and the GDPR, Needle explains.

"These regulations will likely have a major impact on the insurance market in the near future," he says. "For companies with significant PII (personal private information) concerns and/or those involved with selling data, in particular, the regulations have created additional underwriting scrutiny."

Risk management power

Although cyber challenges can seem insurmountable, mitigation tools exist. For example, the National Institute of Standards and Technology Cybersecurity Framework provides essential guidance regarding risk identification, protection and detection. It also has an incident response and recovery function.

Similarly, the National Association of Insurance Commissioners (NAIC) developed a model data security law. Most recently, it was used to create the Maine Insurance Data Security Act, which outlines standards for insurers licensed in the state, including requirements for developing, implementing and maintaining written information security programs that align with the size and complexity of a business based on a risk assessment. Such risk assessments are required to be conducted annually to assess the effectiveness of cybersecurity controls, information systems and other safeguards to manage threats.

"As most cyber policies provide coverage for regulatory fines and penalties, underwriting for cyber risks moves in lockstep with evolving data privacy and security regulations," AGCS' Kang says. "There have been material regulatory and consumer actions based on both CCPA and GDPR, and we are continuing to monitor the frequency and severity of claims under both."

New statutes and regulations have had a broader impact, as they shift conversations from "reasonable security of sensitive data to the protection of the privacy rights of consumers," he says. "As consumers exercise their new rights regarding their data, there are also operational requirements for companies that process or store such data to respond to consumer requests."

Pulling the growing risk and all the other threads impacting this market together, Accenture's Saldanha explains end-to-end cyber protection is made up of four critical elements: Complete and transparent cyber risk assessments; targeted pre-break services to reduce risk exposure, including near- and real-time threat monitoring; tailored insurance coverage and other products that keep risk aligned premiums and terms at their center; and breach responses services that should include developing a flexible and globally accessible team that can quickly restore companies to their pre-breach state.

"Despite this ever-evolving risk landscape and increasing attack surface, cyber risks remain profoundly uninsured, globally," Saldanha says. "According to McAfee, premiums are calculated to account for less than 1% of the estimated $600 billion annual cost of cybercrime."

Setting premiums

Many insurance companies base coverage rates on a policyholder's potential revenues and earnings. The bigger and more successful the company, the higher the premiums. Some insurers also use the number of employees as a determining factor, with higher headcounts resulting in larger premiums, according to the business consultancy AdvisorSmith.

The type of business can also play a role in costs, according to AdvisorSmith, which noted a company's risk can be segmented into low, moderate and high tiers.

Lower tiers, or those that don't deal much in third-party information and have fewer data records, enjoy the lowest premiums. Small manufacturers with few clients and little in the way of customer information fall into this category.

Moderate risk companies hold larger amounts of customer data but may not store highly sensitive details. These types of businesses include retailers that accept in-store credit card transactions.

The top-risk tier includes businesses that store sensitive information such as social security numbers, birth dates and other financial or personal information. Top-tier businesses include medical offices, accountants, universities and property management firms. Insurance carriers, which are attracting more attention from hackers, also fall into this category.

Additionally, location can play a factor as rates vary by state. For instance, businesses in Arizona faced steep premium hikes, with an increase of 39%, from 2019 to 2020, according to AdvisorSmith. The firm noted policies written in North Carolina saw premiums drop 12% during the same period.

Many insurance companies will also inquire about each potential policyholder's cybersecurity practices. This might include a look into data loss prevention procedures, multi-factor authentication systems and encryption practices. Additionally, how often and quickly a business can spot and patch software vulnerabilities and whether third-party vendors are used to monitor and assess security issues also come into play, according to AdvisorSmith.

Keep reading...

- **Does cyber insurance make ransomware worse? (https://www.propertycasualty360.com/2021/05/26/does-cyber-insurance-make-ransomware-worse/)**
- **The WFH impact on the cyber insurance market (https://www.propertycasualty360.com/2021/07/22/the-wfh-impact-on-the-cyber-insurance-market/)**
- **E&O in the world of cyber liability (https://www.propertycasualty360.com/2021/07/07/eo-in-the-world-of-cyber-liability/)**