Gallagher

Insurance | Risk Management | Consulting

Cyber Market Conditions

JANUARY 2022

The Cyber Insurance Market Struggles With Continued Hardening Market Conditions

By John Farley

As we look back on the 2021 cyber insurance marketplace, we see all the hallmarks of a hardening market, with no signs of relief as we move into 2022. We are in a place and time where difficult questions are being asked about systemic cyber risk, cyber underwriting practices and where hackers may hit next. Debates between brokers and underwriters rage on exactly what cyber insurance policies should cover and to what extent an insured's cyber risk management maturity requirements need to adapt to the 2022 threat landscape. Capacity questions have not been settled, and exactly how much will be available in the U.S. and global cyber markets in 2022 remains an open question.

WHAT WE SAW IN 2021

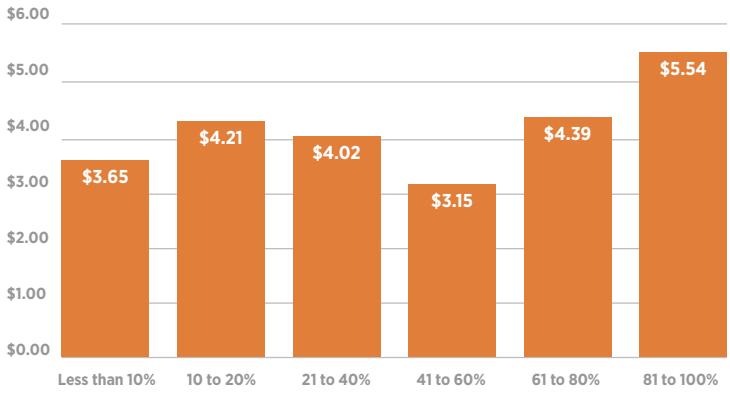
Last year was a stark reminder that hackers are pivoting — and are succeeding — in deploying new attack strategies. There is clear evidence that they now favor targets in the supply chain that could provide a gateway to multiples of additional victims, providing efficiencies to their methods. There were a wide variety of victims that ranged from global software providers, email platforms, the largest U.S. meat supplier and a fuel supplier that provides nearly half the fuel to the east coast of the U.S. Threat actors have found this vast system of interdependencies to be fertile hunting grounds.

Ransomware attacks continued to ravage the bottom lines of both their victims and insurance carriers. In fact, during the first six months of 2021 we saw $590 million paid in ransom payments, as opposed to $416 million paid in all of 2020.[1] Increased payment amounts may be due, at least in part, to the fact that hackers now routinely threaten to publicize their victim's most sensitive data if their six and seven figure ransom demands are not met. However, extortion payments are just one piece of the cyber claim. The latest studies revealed that over the past year the average downtime from a ransomware attack was 23 days with average business interruption losses and other costs increasing from $761,106 to $1.85 million in 2021.[2]

The impact of heightened cyber risk due to COVID-19 was also apparent last year. Organizations were forced to continue to operate in remote working environments while cyber threat actors continued to exploit inherent data security weaknesses there. This challenge was reflected in the 2021 Ponemon-IBM Cost of a Data Breach Study, which showed a correlation between increased remote workforce and the increased cost of a data breach.[3]

Average cost of a breach based on share of employees working remotely

MEASURED IN U.S. $ MILLIONS



Source: 2021 Ponemon-IBM Cost of a Data Breach Study

Social engineering schemes continue to plague victims, as documented in 2021 when the FBI released their 2020 Internet Crime Report. The FBI reported that organizations lost $1.8 billion due to Business Email Compromise (BEC) social engineering attacks.[4]

Regulatory risk continued to evolve as privacy laws around the U.S. and international arenas expanded. Data subjects and the regulators that represent them are more empowered than ever by the California Consumer Privacy Act, the Illinois Biometric Information Privacy Act, Europe's General Data Protection Regulations, and many other rules. These regulations follow a common theme that holds organizations to specific standards as they collect, store, process and transfer consumer data. In some cases, noncompliance can lead to regulatory investigations, lawsuits, fines and settlements and may provide a path for plaintiffs to pursue private rights of action.

Gallagher

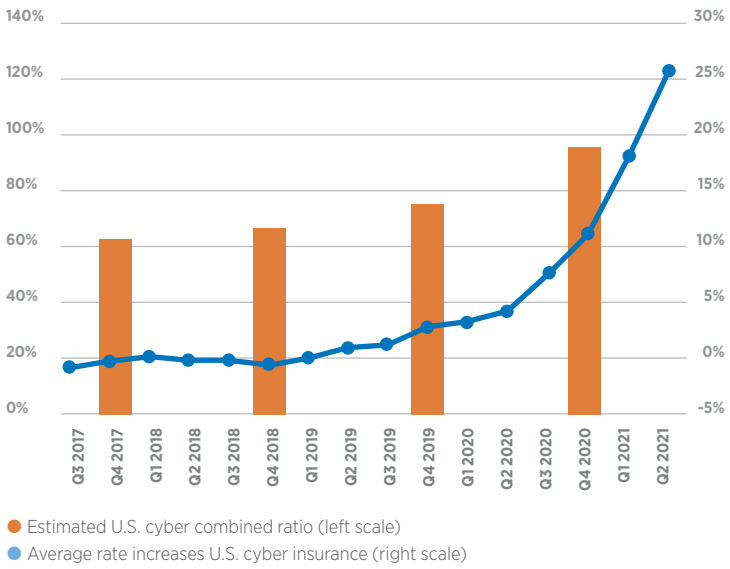
Insurance | Risk Management | Consulting

Cyber Market Conditions

JANUARY 2022

As losses multiply, cyber rates ramp up

Significant rate increases did not offset combined ratio deterioration.



Source: Standard & Poor's Financial Services LLC

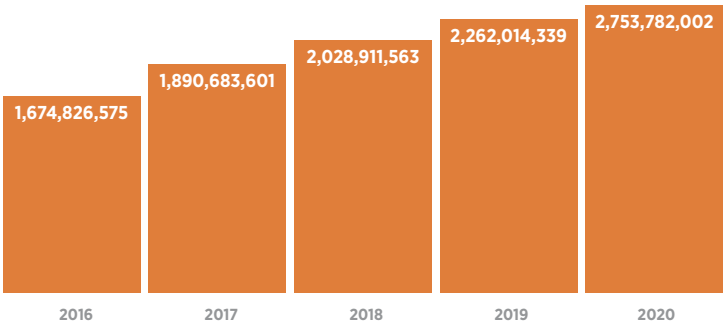
The cyber insurance market took four deliberate steps to combat increasing loss ratios in an effort to protect its bottom line.

- **Rate increases:** Cyber premiums increased across the board, regardless of the industry sector or size of the organization. We saw some of the best-in-class risks subject to 50% and higher rate increases in some cases. Others that lacked specific data security controls saw rates as high at 100% to 300%, if the cyber insurance applicant were provided a quote at all. We saw cyber underwriters being cautious or even moving away from specific industries, including municipalities, higher education, technology and manufacturing.
- **Coverage limitations:** Many carriers imposed sublimits and coinsurance provisions specific to ransomware claims. This often resulted in limiting coverage to 50% of the policy limit or less. We saw certain carriers add exclusionary language to specific known vulnerabilities; failure to remediate these could lead to a denial of coverage for losses attributed to them. Others revised coverage terms specific to regulatory claims with language that constricted risk transfer for regulatory risk.
- **Capacity constriction:** While we did not see any mass exodus from the market, there were clear indicators that carriers wanted to limit their exposure through limiting capacity. The policy limits offered during prior renewals were routinely cut to half of that amount during the 2021 renewal cycle, both at the primary and excess layer level.
- **Greater underwriting scrutiny:** Almost all carriers asked for more details around data security control efforts. Not surprisingly, many questions focused on ransomware prevention and mitigation, with several carriers requiring ransomware supplemental applications consisting of dozens of questions to see how well insureds managed the threat.

The overall cyber insurance market grew in the U.S. to $4.1 billion in direct written premiums in 2020, representing an increase of 29.1% from 2019.[5] And with continued challenges faced in the cyber insurance marketplace, we expect the trend to continue in 2021 and throughout 2022.

Total direct written premium combined stand-alone and package[6]

(does not include Alien Surplus Lines Market)



Source: National Association of Insurance Commissioners (NAIC). 2021 Report on the Cybersecurity Insurance Market

Cyber Market Conditions

JANUARY 2022

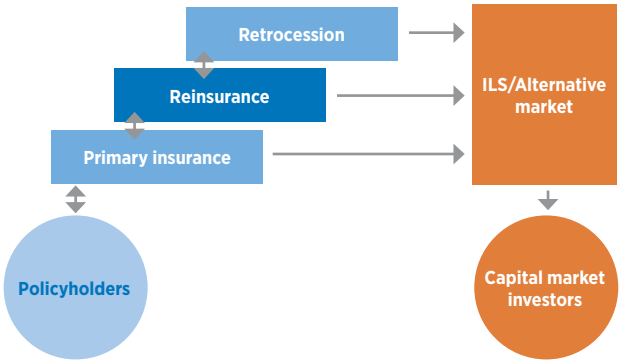
WHAT WE ARE WATCHING; KEY PLAYERS THAT WILL SHAPE THE 2022 CYBER MARKET

We see the 2022 cyber marketplace at a crossroads. Several key players in the marketplace ecosystem will play crucial roles this year, and their actions will profoundly impact the landscape that the cyber insurance buyer will ultimately need to navigate.

Cyber Insurance Underwriters: It has become clear that rate increases alone will not be able to solve the 2022 cyber market challenges. The trend of greater underwriting discipline will continue with the least attractive risks facing non-renewals and left with few viable options. Any carriers offering coverage without some of the core controls that the majority of the other carriers are demanding will run the risk of adverse selection, as the least attractive risks flock to them. We are also focused on changing coverage terms, which are trending to restrict coverage for systemic risk, where a single vulnerability may impact a majority of a carrier book of business. Carriers are beginning to address this in their policy forms by imposing sublimits and/or exclusionary language for these global cyber incidents, and it may impair the buyer's ability to transfer cyber risk in the comprehensive way it did in prior years.

Reinsurers: With as much as 45% of primary cyber insurance market premium ceded to reinsurers, we expect capacity constraints to continue impacting underlying market pricing alongside an evolving cyber threat landscape.[7] (Re)insurers' ability to generate capacity will be an important factor in 2022. We expect markets to seek support from outside the traditional rated capacity market via collateralized reinsurance and Insurance-Linked Securities (ILS) transactions with the capital markets. This could also take the form of looking to different reinsurance structures and product development. We also expect continued cyber loss modeling tool development as the market pushes for further insights into the far-reaching threats of systemic cyber risk.

The cyber re/insurance value chain



ILS—Insurance-linked securitization. Source: S&P Global Ratings.

Cyber Risk Management Vendors: The service providers that help prevent and mitigate the effects of cyber incidents play a role of growing importance and have become a fixture in today's cyber marketplace. Buyers of cyber insurance will need to leverage these services one way or the other, and the vendors that can provide efficient and cost-effective solutions for the needs of specific risk profiles will continue to emerge as a necessity.

Government: We are watching an increased effort by both the U.S. and international governments to work with and provide insight to the private sector in managing cyber threats, with a particular focus on the ransomware epidemic. Efforts to enhance threat intelligence sharing and a priority of protecting critical infrastructure will be apparent in 2022. Guidance around OFAC compliance, specific to whether or not ransom payments can legally be made, was provided in 2021, with aggressive action in sanctioning at least one cryptocurrency exchange. The private sector may be subject to severe penalties for noncompliance to government-mandated OFAC requirements and a close watch on enforcement efforts in 2022 is warranted. We also expect law enforcement to become more proficient at helping victim organizations recover ransom payments to threat actors, using a combination of cryptocurrency experts, computer scientists, blockchain analysts and crypto-tracers in this effort. Finally, we expect law enforcement to embark on a more aggressive offensive strategy in disrupting Ransomware as a Service (RaaS) affiliates.

LOOKING AHEAD

Now more than ever, we are working to prepare our clients for some uncertain and choppy waters in the 2022 cyber insurance marketplace. Certain industry sectors will struggle more than others. But regardless of industry or organizations size, we certainly will see a continued disciplined underwriting approach that remains laser-focused on data security controls, with rates continuing their upward trend. The cyber insurance buyer needs to be wary that rates alone should not be the barometer by which they measure the hardness of the 2022 market. They will need to maintain a wide lens view of other factors, including more restrictive coverage terms, mandatory sublimits and exclusionary language specific to certain global and widespread cyber incidents.

Gallagher

Insurance | Risk Management | Consulting

Cyber Market Conditions

JANUARY 2022

To effectively manage the underwriting process, we will maintain a detailed working knowledge of the latest cyber insurance products and the requirements to qualify for them. We will also need to balance renewal timelines with required data security control remediation efforts amidst potential budget limitations.

Because of the highly nuanced nature of the cyber insurance market, it is imperative that you are working with an insurance broker who specializes in your particular industry or line of coverage. Gallagher has a vast network of specialists that understand your industry and business, along with the best solutions in the marketplace for your specific challenges.

Please note: A client's risk profile is the primary variable dictating renewal outcomes. Loss experience, industry, location and individual account nuances will also have a significant impact on these renewals.

Sources:

[1]https://www.Insurancejournal.com/news/international/2021/11/19/642947.htm

[2]Allianz Global Corporate & Specialty (AGCS) report https://www.insurancejournal.com/magazines/mag-features/2021/11/01/639581.htm

[3]Ponemon 2021 Cost of a Data Breach Study

[4]FBI 2020 Internet Crime Report 2020_IC3Report.pdf

[5,6]National Association of Insurance Commissioners (NAIC). 2021 Report on the Cybersecurity Insurance Market

[7]SP Global: Cyber Risk In A New Era: Reinsurers Could Unlock The Cyber Insurance Market https://www.spglobal.com/ratings/en/research/articles/210929-cyber-risks-in-a-new-era-reinsurers-could-unlock-the-cyber-insurance-market-12118547

AUTHOR

John Farley
Managing Director
Cyber Practice
John_Farley@ajg.com

John leads Gallagher's Cyber practice in the U.S. and works closely with our teams in across the world in our Global Cyber practice. He provides thought leadership on a variety of cyber risk management best practices. He assists clients across all industries in navigating the dynamic cyber insurance markets as a means to cyber risk transfer while providing guidance on emerging regulatory risk, cyber attack techniques, cyber risk prevention and data breach cost mitigation strategies.

During his 30 years in the insurance industry, John forged strategic relationships with cyber insurance underwriters, privacy attorneys, IT forensics investigators, and law enforcement. His extensive experience earned him a seat on an advisory board for the U.S. Treasury.