Global Cyber Market Update

Mid-Year 2021

Gallagher

Insurance | Risk Management | Consulting

As we began 2021 we were bracing for what was widely expected to be a turbulent and difficult cyber insurance market. Those predictions came true, and by some measures, the market conditions that unfolded in the first half of 2021 were more challenging than many expected. Cyber claim frequency and severity continued their upward trend. This led to a swift response from the cyber insurance market as they imposed significant limitations of capacity, narrowed the scope of coverage terms, heightened underwriting scrutiny and significantly increased rates.

Ultimately, most cyber insurance buyers in 2021 so far have felt the impact via time consuming and complex renewals, with many obtaining less coverage at a higher cost.

The Current Threat Landscape

The ransomware trends we saw in 2020 continued to plague the cyber insurance market throughout the first half of 2021. Through the first quarter of 2021 the U.S. saw extortion demands rise to $220,298 on average, with the average downtime extending to 23 days. Moreover, 77% of ransomware attacks involved threats to publicize data that was ex-filtrated in the attack, commonly known as a "double extortion" tactic[1].

This rise in attacks was not a localized trend; it was felt around the globe. According to one report, EMEA countries (Europe, the Middle East and Africa) experienced a 36% increase in cyberattacks, the U.S. followed with an increase of 17%, while those in the Asia-Pacific region saw a 13% increase since the beginning of the year[2].

Notably, hackers continued to focus on key targets in the supply chain, where a successful attack on one could impact thousands of other victims. A global software company, an international food distributor, and a U.S.-based fuel supplier are just a few examples of crippling cyberattacks that impacted victims in the supply chain over the first half of the year. Ultimately, these sophisticated and well-planned attacks gave cyber criminals leverage to increase extortion demands while providing a gateway to many more victims.

While ransomware threats made headlines, social engineering losses also continued to mount. According to the recently released FBI *IC3 2020 Internet Crime Report*, 2020 saw a record 69% increase in cybercrime from the prior year's report, with Business Email Compromise ("BEC") losses accounting for half of all losses. In fact BEC losses amounted to a staggering $1.8 billion in losses alone[3].

[1]Coveware Q1 2021 Marketplace Report
[2]Check Point 2021 Cyber Security Report
[3]FBI IC3 2020 Internet Crime Report

The Government's Role and Global Regulatory Developments

Governments around the world became more focused in the fight against cyberattacks in 2021, and have made deliberate efforts to coordinate with the private sector to prevent further attacks. Meanwhile, international regulators are now paying especially close attention to individual privacy rights and data collection compliance requirements.

U.S.

- The Biden administration has directed federal agencies to develop voluntary cybersecurity goals for companies that operate U.S. critical infrastructure.
- Following the passage of the Illinois BIPA and California's CCPA, there has been an uptick in litigation allowing for private rights of action and statutory damages—ultimately increasing cyber claims payouts even further.
- In July, a global web conferencing platform settled a class action in U.S. District court for $86 million, where the plaintiffs alleged failure to comply with basic data security requirements[4].

UK

- Recent EU privacy and security law updates have had a common theme: enabling a far greater right of action for the individual that allow law firms to prosecute entities on behalf of impacted individuals[5].
- In July, Luxembourg regulators issued a $886 million fine against a leading global online retailer for alleged failure to comply with GDPR requirements[6].

CANADA

- Royal Canadian Mounted Police recently began a pilot program in increase cyber crime reporting in an effort to increase information sharing with the private sector. It is intended to be fully operational in 2022[7].
- Canada's proposed Consumer Privacy Protection Act (CPPA), if passed, would be comparable to regulation in the U.S. and EU. It would allow similar rights and greater control for data subjects. Penalties for non-compliance could be as high five percent of an organization's annual revenue or $25 million Canadian dollars[8].

AUSTRALIA

- Late last year, Australia introduced a bill to extend the Critical Infrastructure Act to expand to more sectors and enhance the existing framework with additional security obligations.
- In June, another bill was introduced to make it mandatory for all Australian businesses and government agencies to notify the Australian Cyber Security Centre before paying a ransom to a ransomware attacker. Failure to notify can lead to a penalty of up to $220,000.
- Australian government authorities are considering additional cyber security compliance responsibilities for directors of large Australian companies, potentially holding directors personally responsible for cyber attacks.

[4]Zoom settles US class action privacy lawsuit for $86M — BBC News
[5]Market Knowledge
[6]Amazon hit with $886M fine for alleged data law breach — BBC News
[7]The National Cybercrime Coordination Unit (NC3) | Royal Canadian Mounted Police (rcmp-grc.gc.ca)
[8]Coming Soon: Canada's New Privacy Law – What You Need to Know | Epiq — JDSupra

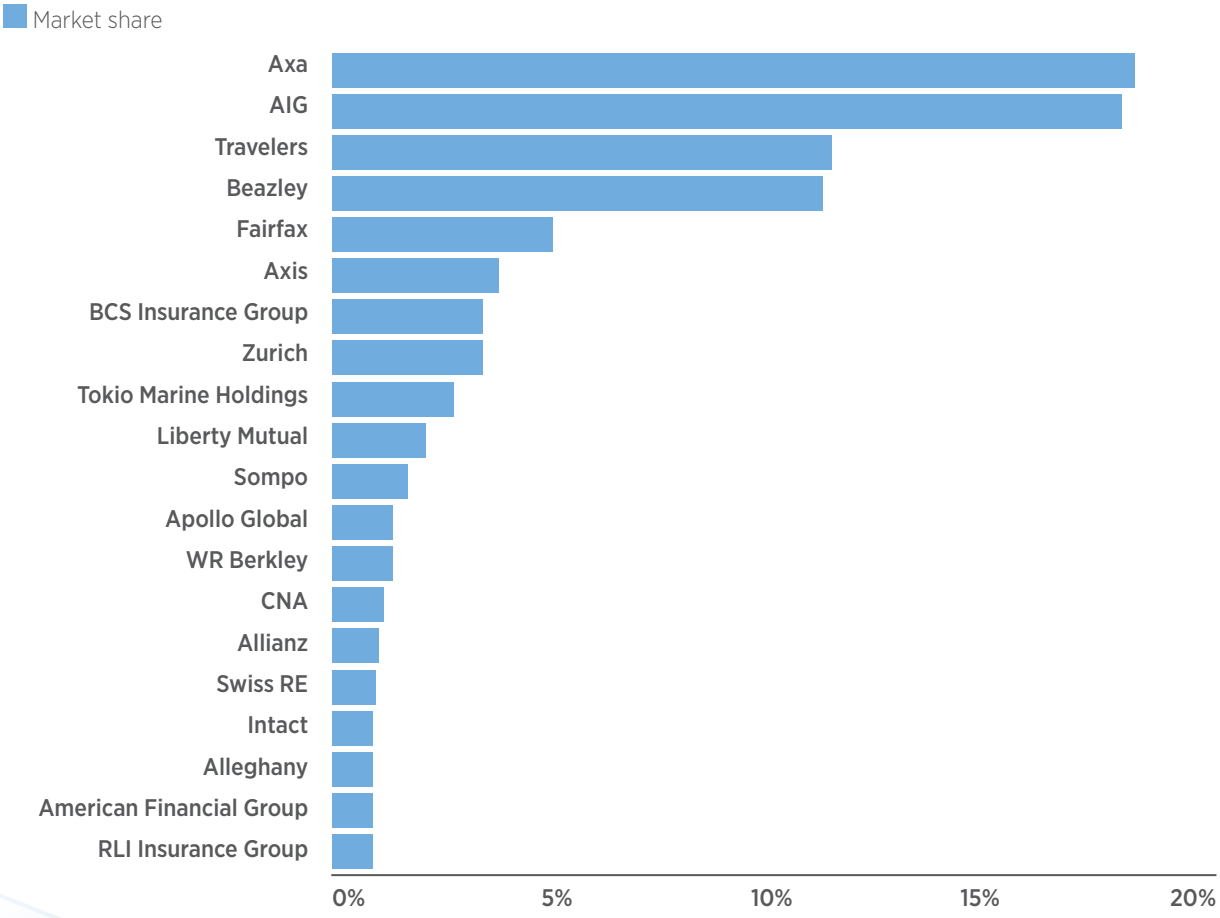
The State of the Cyber Insurance Market

According to the Best Market Segment Report that was published in June, 14 of the top 20 cyber insurer's loss ratios increased in 2020[9]. After compiling last year's loss data and seeing these cyber claims trends deteriorate through the first half of 2021, the cyber underwriting community has responded with a laser focus on data security controls when evaluating risks. Virtually every carrier will require attestation of at least some preventive controls, which likely include multifactor authentication ("MFA"), Remote Desktop Protocol ("RDP"), data backup practices, segregation of networks, encryption, patch management, Privileged Account Management ("PAM"), employee training and a host of others. Applications often require additional ransomware supplemental applications that may involve dozens of questions around controls specifically designed to prevent or mitigate the effects of ransomware attacks.

Without some of these controls in place, many carriers are refusing to quote. Those that do will likely demand significant rate increases in the 100% to 200% range, and in some cases as high as 300%. Even the best in class risks that comply with all underwriting required security controls are seeing increases in the 40% to 60% range.

Biggest Players

Axa, AIG are the U.S.'s biggest underwriters of standalone cyber policies[10]



[9]Best Market Segment Report: Ransomware and Aggregation Issues Call For New Approaches To Cyber Risk, June 2, 2021

[10]National Association Of Insurance Commissioner's Data, Bloomberg

Many cyber insurance policies offered in the 2021 marketplace are restricting coverage in a number of ways, including:

- Sublimits and coinsurance requirements imposed for ransomware claims.
- New exclusionary language related to the use of end-of-life software and the use of at-risk software or email platforms that have not been remediated.
- Coverage limitations related to what triggers coverage for regulatory investigations.

Additional challenges are being seen in the insurance market as we continue to see capacity constriction. Many insurance markets are offering significantly lower policy limits, while others are exiting the market for larger, more complex risks altogether.

We have also seen risk appetites decrease for specific industry classes, including municipalities, education and manufacturing. Newer entrants are beginning to feel pressure to obtain additional financial backing while many of the longstanding cyber carriers are now subject to significant rate increases from the cyber reinsurance markets. In fact, 62% of all cyber insurance is ceded to reinsurers[1]. We therefore expect the cyber reinsurance treaty market to take affirmative steps to maintain profitability and reduced systemic risk that may affect their exposure, putting further pressure on rates.

[1]https://www.swissre.com/reinsurance/property-and-casualty/reinsurance/casualty-reinsurance-underwriting/cyber-reinsurancein-the-new-normal.html

Strategies to Navigate the Cyber Insurance Market

While much of the news throughout 2021 has been bad for both carriers and their insureds, there are strategies that organizations can follow to prevent and mitigate attacks and to place themselves in a better overall position as they navigate the cyber insurance market. Going through the cyber insurance application process, as complex and time consuming as it is, often has the effect of improving the applicants overall cyber security maturity level. The natural outcome includes both the identification of security vulnerabilities and taking steps toward remediating them. Once the cyber policy is in place, most cyber insurance carriers will offer a variety of free and discounted cyber risk management services. These include employee training, incident response planning, technology to scan for known vulnerabilities, identify intrusions and, in some cases, the resources for correcting security flaws. That take-up rate for these services had been remarkably low in prior years. However, we are seeing a welcome reversal in that trend as more insureds are taking advantage of these valuable cyber risk management tools.

The Second Half of 2021: What To Expect

We expect even greater underwriting scrutiny of cyber security controls in the cyber insurance market throughout the remainder of 2021 while capacity will almost certainly continue to shrink. Insurance products will reflect decreasing carrier appetites to fully cover ransomware costs, as they push for cost-sharing in the form of ransomware coinsurance and sublimits. Rate hikes show no real signs of leveling off in the near term. This will likely force insureds to offset these costs by assuming greater self-insured retentions and taking an even greater role in actively managing cyber risk.

Contributors

John Farley
US Cyber Lead

Robyn Adcock
Australian Cyber Lead

Tom Draper
UK Cyber Lead

Brian Dagg
Canada Cyber Lead

Gallagher

ajg.com **The Gallagher Way.** Since 1927.