2023 U.S. Cyber Market Conditions Outlook Report

Gallagher

Insurance | Risk Management | Consulting

January 2023

THE CYBER INSURANCE MARKET BEGINS TO STABILIZE

By: John Farley
Managing Director, U.S. Cyber Practice

After three years of hardening conditions, the cyber insurance market has finally begun to show signs of stabilization. From a premium perspective, cyber insurance buyers are seeing smaller rate increases and, in some cases, even flat renewals.

There are, however, clear signs that we will not be reverting to the soft market conditions from a few years ago. First, the offered products cover less with new restrictive policy wording imposed by several carriers in 2023. Secondly, the strict underwriting control requirements mandated last year will persist while the demand for capacity appears to continue to outpace supply. Finally, there is a growing concern among cyber insurance markets around systemic cyber risk, where the focus remains on quantifying a potentially catastrophic cyber event and estimating the probability of one occurring. This underlying concern will likely persist through 2023 and work to support the current conditions that will maintain the tenants of a challenging cyber insurance marketplace.

WHAT WE SAW IN 2022

In the first quarter of 2022, the FBI released its 2021 Internet Crime Report detailing all 2021 losses. The FBI reported potential ransomware losses exceeding $6.9 billion. Also in the report were the most commonly reported incidents: business e-mail compromise ("BEC"), and the criminal use of cryptocurrency. Of note, while ransomware made headlines, the FBI reported that BEC schemes resulted in 19,954 complaints with an adjusted loss of nearly $2.4 billion.

In February of 2022, we saw the conflict between Ukraine and Russia erupt, which stoked fears of a larger global cyber conflict that could potentially impact organizations exposed to collateral damage, if not targeted directly by Russia. Fortunately, those concerns never did manifest, and the cyber market breathed a sigh of relief. As 2022 progressed, the frequency and severity of ransomware attacks leveled off and, by some estimates, trended downward. According to one report,[1] ransomware attacks in the first nine months of 2022 declined by 31% year-over-year — a considerable factor in 2022s slowing the dramatic upward climb in rates from the year before.

We also noted some long-awaited good news for the market in the Fitch Ratings report that was released in June. Specifically, Fitch noted robust growth in the cyber insurance market and improved cyber loss ratios amongst carriers.

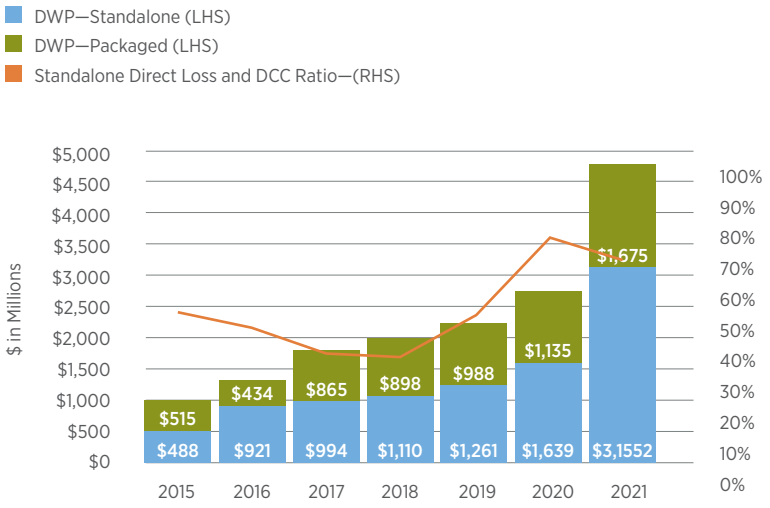
"A sharp increase in 2020 cyber loss ratios promoted substantially higher prices and rapid premium growth in 2021 that exceeded incurred losses, leading to surprising improvement in the cyber direct loss ratios versus the previous year."

Some key findings in the Fitch report reflected the fact that cyber underwriting profits improved while there was a noted increase in cyber insurance adoption amongst insurance buyers:

- Losses increased by over 300% since 2018. Still, 2021 premium growth exceeded the change in incurred losses and the standalone cyber loss ratio improved to 65% from 72% a year earlier.
- Fitch estimates that standalone and packaged cyber statutory direct written premiums increased by 74% in 2021 to nearly $5 billion compared with 9% growth for the P/C industry overall.
- Standalone cyber coverage increased by 92% in 2021.

P/C Industry Aggregate Standalone and Packaged Cyber Risk

Standalone Cyber Coverage loss Ratios improved to 65% from 72% in 2020



Standalone Direct loss and DCC ratios: 2015–48%, 2016–43%, 2017–35%, 2018–34%, 2019–47%, 2020–72%, 2021E–65%.

Statutory Cybersecurity and Identity Theft Coverage Supplement Data. DCC—Defense and cost containment incurred.

Source: Fitch Ratings, S&P Global Market Intelligence.

[1] SonicWall: Ransomware down this year, but there's a catch—*The Register*

Regulators made their voices heard in 2022. According to the SEC's Statement on Proposal for Mandatory Cybersecurity Disclosure issued on March 9, 2022, all publicly traded companies must adhere to two mandates, among other requirements.

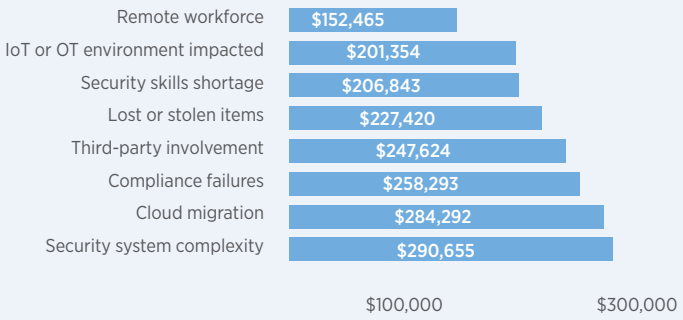
- **Mandatory cybersecurity incident disclosure.** Material incidents must be reported on an 8-K form within four business days of the incident. Organizations would also be required to provide periodic updates about previous incidents. In addition, they would be required to report when "a series of previously undisclosed, individually immaterial cybersecurity events has become material in the aggregate."
- **Required disclosures of company policies to manage cyber risks.** Annual reports would have to outline a firm's policies for identifying and managing cyber risks and document whether any member of its board of directors has expertise in cybersecurity.

Regulatory lawsuits and enforcement also made headlines in 2022. We witnessed the first jury verdict involving Illinois' Biometric Privacy Act, which regulates the collection use and storage of biometric identifiers, resulting in a $228 million plaintiff's verdict.[2] We also saw U.S. regulators impose a $391.5 million fine against one of the largest global technology companies that allegedly tracked the location of users who opted out of location services on their devices. This was the largest privacy-related multi-state settlement in U.S. history.[3]

A comprehensive summary of recent losses related to cyber incidents was summarized in the Ponemon/IBM Security 2022 Cost of a Data Breach Report. They highlight several factors that could mitigate the cost of a data breach and others that may amplify them. Underwriters have continued to monitor these and other control factors and remain focused on them in assessing their willingness to write policies for prospective insureds.

Key Cost Amplifiers

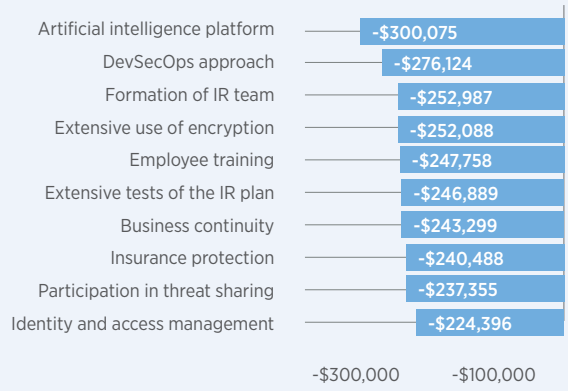
Measured in U.S. $ millions



SOURCE: PONEMON/IBM SECURITY 2022 COST OF A DATA BREACH REPORT

Key Cost Mitigators

Measured in U.S. $ millions



SOURCE: PONEMON/IBM SECURITY 2022 COST OF A DATA BREACH REPORT

[2] Biometric privacy award sparks reactions in insurance market—*Business Insurance*

[3] Google to pay record $391m privacy settlement—*BBC News*

WHAT WE ARE WATCHING: KEY PLAYERS THAT WILL SHAPE THE 2023 MARKET

We see the 2023 cyber marketplace reaching a level of maturity that we had not seen previously. A general understanding of expected cybersecurity controls has been established, and that expectation will be reinforced in 2023. After working through two or three policy renewal cycles in the hardening market, carriers have gained a greater comfort level in the risks they prefer to write moving forward. Several key players in the marketplace ecosystem will play crucial roles this year as this market continues to mature and grow. Their actions will profoundly impact the landscape that the cyber insurance buyer will ultimately need to navigate.

Underwriters: Underwriters remain laser-focused on several controls, including multifactor authentication, endpoint detection and response, privileged access management, employee training, incident response planning along with other key cybersecurity controls. The application process, however, is still viewed as widely inefficient, time-consuming and prone to errors and miscommunication between underwriters, insureds and brokers. As a result, there will be an increased effort to streamline the process. This may be accomplished, at least in part, via an agreed upon third-party vendor solution that validates key controls are in place to a reasonable degree before underwriting decisions are made. We also expect some of the markets to modify policy wording to address concerns surrounding systemic cyber risk. This will include a focus on constricting coverage where multiple losses may result from a cyber-warfare event, losses stemming from a key player in the IT supply chain, or other attacks on critical infrastructure that lead to wide-ranging cyber losses.

Reinsurers: The reinsurance community has taken center stage on the important topic of capacity as it is viewed as imperative to the growth of the cyber insurance market. It is widely believed that it may come from both reinsurers and key capital markets via insurance-linked securities. However, before any meaningful progress can be made, there will be a need for improvements in cyber catastrophe modeling tools. Unlike those used for property insurance, cyber models do not have the luxury of analyzing multiple billion dollar losses over a significant time frame, are challenged by a quickly shifting peril as the threat landscape evolves, and are using recently developed systems and software whose functionality and capabilities will likely have room for improvement.

Cyber Risk Management Vendors: We will see a continued trend of convergence of cybersecurity vendors with the insurance carrier and brokerage community. This may be accomplished through both strategic partnerships and acquisitions. The focus will be on leveraging key vendors to improve cyber loss quantification from both a single insured and a large number of insureds stemming from a wider systemic type of cyber loss event. In addition, cybersecurity vendors will have a continued and growing role in helping underwriters assess the risks of applicants and to provide ongoing cyber risk services for insureds throughout their policy terms.

U.S. Regulators: Heightened regulatory risk will permeate the 2023 cyber marketplace and contribute to the concerns of the underwriting community. Several U.S. government agencies are considering, legislating or starting to enforce new rules that would require companies to report cyber incidents. The current focus will be on critical infrastructure industries such as financial services, energy, health care and communications and will extend to several other sectors. In addition, we expect several states to follow California's lead in enacting comprehensive privacy laws that extend to emerging privacy threats including, but not limited to, biometrics.

At the federal level, all eyes will be on SEC enforcement of non-compliance to the proposed cybersecurity disclosure requirements. Finally, from an international perspective, we will continue to see global privacy regimes empowering data subjects that reside in their respective countries with regulations based on the core concepts introduced by the EU's General Data Protection Regulation.

U.S. Government: Government will continue efforts to assist the general public with emerging threats and resiliency advice through alerts provided by Cybersecurity and Infrastructure Security Agency ("CISA"). In addition, the U.S. Department of State recently formed its first Bureau of Cyberspace and Digital Policy ("CDP") which may establish national cybersecurity control regulations.[4] We will also be watching recent initiatives introduced by the U.S. Government Accountability Office. In their recent report[5] to Congress, they urged both the Treasury and Homeland Security to address the possibility for a potential government backstop to support the cyber insurance market, similar to the TRIA program that stabilized the property insurance market after 9/11.

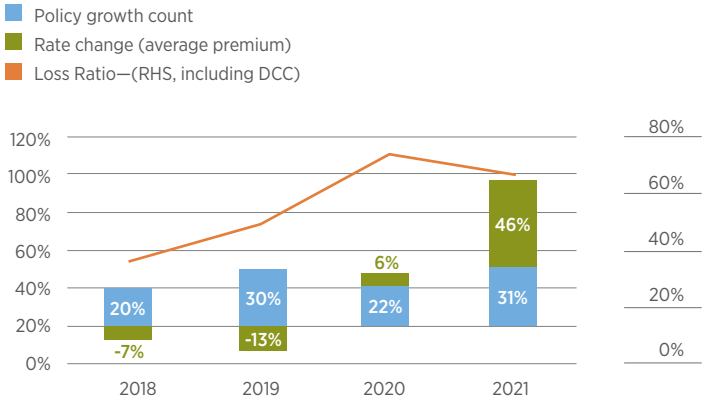
[4] State Department Announces First Bureau of Cyberspace and Digital Policy—*Nextgov*

[5] Cyber growth more about rate adjustments than contracts."— S&P Global Ratings—*Reinsurance News*

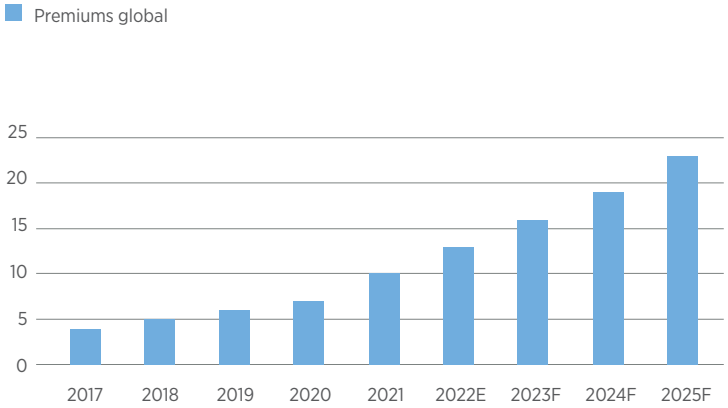
LOOKING AHEAD

Figure 5

U.S. standalone loss ratio and rate and exposure growth



Global cyber insurance premiums, USD bn, Swiss Re estimates



Source: National Association of Insurance Commissioners, S&P Global, Swiss Re Institute calculations

There is a growing consensus that the cyber insurance market is poised to grow exponentially in the near and far term. According to one estimate,[6] cyber insurance premiums reached $10 billion in 2021 and are projected to grow 20% year-over-year until 2025. That premium level, coupled with an estimated annual global cyber loss estimate of $945 billion,[7] leaves a vast majority of predicted cyber losses uninsured.

This reality will play against an evolving threat landscape with a looming concern of a future catastrophic cyber event. The market will certainly expand, but will do so carefully with dynamic cyber insurance policy terms and creative efforts for capacity expansion. Underwriters will partner with vendors from the cybersecurity and compliance arenas while keeping a close eye on how the U.S. government may play a part in its overall growth. In summary, we see the potential for significant growth in the cyber insurance market in 2023 and in the years to follow. As the cyber insurance marketplace continues to mature, it will follow a path to form a more cohesive alliance with both cybersecurity and government sectors as cyber threats evolve.

[6]Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks, Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks | U.S. *GAO*

[7]Swiss Re Institute Cyber insurance: strengthening resilience for the digital transformation McAfee. op. cit. from Swiss Re Institute Cyber insurance: strengthening resilience for the digital transformation