PARKER SMITH & FEEK

An IMA Company

COMMERCIAL INSURANCE

EMPLOYEE BENEFITS

PERSONAL INSURANCE

RISK MANAGEMENT

SURETY

CYBER

Markets in Focus

Insurance Pricing & Market Update

Q1 2023

OVERVIEW

The underlying theme of Cyber risk remains volatility – for both insured and insurer. While Cyber insurance has been available for over twenty years, it has only come into mainstream focus in the past five years due to the prevalence of ransomware attacks. Prior to that, Cyber insurance was seen as mainly an instrument to manage data breaches and privacy. Ransomware has demonstrated that Cyber risk is not limited to theft of data and is truly an enterprise risk. Areas of concern now extend to operational disruption; business interruption, data re-creation and supply chain. Symptomatic of that perspective, according to Allianz's 2023 Risk Barometer, Cyber risk ranked as the top issue facing businesses around the world in 2023 for the second year in a row. A key driver of that concern is that Cyber risk is that it is also a remarkably fluid category that presents an unknown quantity. Cyber insurance has been instrumental in assisting impacted organizations and provided a critical financial backstop for many companies in the face of catastrophic ransomware attacks. The industry has been at the forefront of diagnosing the underlying issues and prescribing necessary controls on how to mitigate future attacks. As we look forward, there are no shortage of emerging Cyber risks that will impact organizational balance sheets and Cyber insurance will need to continue to help manage that volatility. We will delve further into these trends and how the Cyber insurance marketplace is responding.

CYBER RISK TRENDS

PRIVACY

Privacy will continue to be a point of emphasis within public policy and Plaintiff bar. There is still not a federal law to address consumer data rights and we continue to see a hodgepodge of state laws. The most notable example remains the California Consumer Privacy Act (CCPA), which has been in place since 2018 and has been amended further. CCPA regulates the collection, possession, and sale of consumers' personal information by businesses. It gives consumers more control over the personal information that companies collect and provides consumers with a new remedy in the event of a data breach that results in the "unauthorized access and exfiltration, theft, or disclosure" of certain personal information. CCPA is unique in that it allows for a private right of action for any violation of the law – not just data breaches. To date, there have been over 270 CCPA – related actions filed. Damages available for a private right of action include a statutory amount between $100 and $750 per consumer per incident or actual damages, whichever is greater.

It also provides the attorney general with broad rule-making authority and the power to impose substantial penalties for violations. As an example, in September 2022 the beauty products retailer Sephora became the first company to be penalized under CCPA for not disclosing to consumers that it sells their personal information, failing to respect users' Global Privacy Control as an opt-out, and neglecting to correct these infractions by a deadline. The $1.2 million penalty is part of a settlement with the CA attorney general and the company must rectify its data sharing policy, avenues to opt out, and service provider agreements; and report on its progress to the attorney general.

California will remain the bellwether for consumer data privacy laws, but other states will follow their lead. Colorado, Connecticut, Utah, and Virginia are also implementing new data privacy laws in 2023.

In line with expanding consumer data laws, the enactment of biometric privacy laws is another growing trend across the country. Existing legislation, most notably the Biometric Information Privacy Act (BIPA) in Illinois, has led to a boom of class action litigation against employers, consumer-facing business, and technology companies for claimed violations of biometric privacy rights. Biometric privacy laws and regulations generally require businesses to track, inform employees or consumers of, and provide methods for employees or consumers to consent to, the collection of biometric information or biometric identifiers.

SETTLEMENTS

August 2022
Snap, the parent company of photo-sharing platform Snapchat, reached a $35 million settlement to resolve ongoing litigation which alleged that the company improperly collected biometric data in violation of BIPA through its Lenses feature.

September 2022
Google finalized its $100 million settlement to resolve alleged BIPA violations relating to its Google Photos service

October 2022
A jury found in favor of a class of Illinois truck drivers in the first BIPA class action to be tried to verdict in *Rogers v. BNSF Ry. Co*. After closing arguments, the jury needed less than an hour to return its verdict in favor of the class of truckers, which awarded $428 million in statutory damages.

December 2022
Par-A-Dice Hotel Casino and Boyd Gaming agreed to a $825,000 settlement to resolve claims that they violated biometric privacy law with video surveillance cameras.

Current states with a Biometric Law: AK, CA, CO, IL, NY, TX, VA, WA

States with proposed Biometric Law: MS, OK

TRACKING TECHNOLOGY

Tracking technology, such as the use of pixel and session replay, can be installed to analyze visitor activity on a website, measure effectiveness of advertising and support digital marketing efforts. What seems like an innocent way of gaining insight into your marketing practices has spurred class action litigation. A 2022 class action lawsuit resulted in a healthcare entity agreeing to pay $18 million for the use of the web tool collecting patient information without their permission.

Office for Civil Rights and HIPAA

Healthcare and other federally regulated entities should consider the privacy and regulatory implications of using this tracking technology.

"Office for Civil Rights (OCR) states that tracking technology vendors that receive PHI must sign a business associate agreement (BAA), which must include a description of the vendor's permissible uses and a guarantee of safeguarding PHI. OCR warns that the vendor must meet the definition of a business associate in order for a BAA to permit the disclosure."

For additional information please review the bulletin from the Office for Civil Rights at the U.S. Department of Health and Human Services.

Video Privacy Protection Act and State Wiretapping Statutes

Organizations beyond healthcare that are utilizing this technology have also been met with more regulatory risk. Class action lawsuits have been filed against companies using the tracking technology alleging they knowingly disclosed protected information by allowing Meta's embedded Pixel code to share a digital subscriber's viewing activity and unique Facebook ID with the social media platform. A Video Privacy Protection Act violation could result in $2,500 per class member.

August 2022, in *Popa v. Harriet Carter Gifts Inc.*, the Third Circuit Court of Appeals issued a decision that the session replay software used resulted in a transfer of consumers' data from the retailer's website to the provider of the software was "interception" under the statute.

INTERNET OF THINGS (IOT) AND INDUSTRIAL INTERNET OF THINGS (IIOT)

As our society becomes more reliant on connectivity the IoT exposure has continued to expand. Though most IoT devices don't collect, or store protected information they can be used as a gateway into other networks.

Common types of attacks:

+ **Privilege Escalation Attack** – gaining privileged user access through devices that are either unpatched, misconfigured or have weak security.

+ **Brute-Force Attack** – accessing an IoT device by targeting a device's weak password hygiene.

Potential implications that may result from an IoT compromise include a security breach, business interruption and risk of product defects.

SEC GUIDANCE

Due to the lack of a clear federal law on date security, varying enforcement agencies will step in to fill the void. The FTC has historically been the lead enforcement agency as related to consumer privacy; the SEC is now getting in the act on behalf of investors. Under rules first proposed in 2022 but expected to be finalized as soon as April 2023, publicly traded companies that determine a Cyber incident has become "material"—meaning it could have a significant impact on the business—must disclose details to the SEC and investors within four business days. That requirement would also apply "when a series of previously undisclosed, individually immaterial cybersecurity incidents has become material in the aggregate."

The SEC's rules will also require the boards of those companies to disclose significant information on their security governance, such as how and when it exercises oversight on Cyber risks. That information includes identifying who on the board (or which subcommittee) is responsible for cybersecurity and their relevant expertise. Required disclosures will also include how often and by which processes board members are informed and discuss Cyber risk.

SPOTLIGHT ON – OPERATIONAL DISRUPTION

Business Interruption has been a common yet often misunderstood insurance coverage available for Cyber risks for several decades. Business Interruption coverage will provide indemnity for the loss of income but for the insured having suffered a covered network interruption. Due to historical focus on data breaches, business leaders are less familiar with the concept of business interruption responding to a covered Cyber incident such as a ransomware attack or system failure. The duration and costs associated with managing a catastrophic Cyber event can be substantial. According to Cyber extortion incident response firm Coveware, the average days of downtime was ~25 days in Q4 of 2022, reflecting the amount of time an impacted company may experience some non-zero level of disruption from the attack.

CONTINGENT BUSINESS INTERRUPTION

Businesses today are more reliant on outsourcing IT operations than ever before. Gartner reported last year that almost two thirds of application spending will be directed towards cloud technologies by 2025, up from 57.7% in 2022. Businesses invest in cloud technology to more easily scale their operations and reduce IT infrastructure expense. From a risk perspective, it's important to consider that despite the perceived benefits of cloud technology, businesses are now more reliant on those uninterrupted services, or uptime, of their cloud service providers. In today's world, every organization is at least partially or entirely dependent on digital and internet infrastructure to maintain their operations.

It is conceivable that a system outage or breach affecting digital infrastructure such as a cloud service provider could affect a large segment of the economy at once. For example, cloud service providers such as Microsoft and Amazon Web Services own a large percentage of the market share so that a failure of their cloud technology could have massive consequences. The possibility that a single event on one small part of a digital system could cascade to other interconnected third parties sitting on that same system.

Cyber insurance markets are concerned that a major outage affecting a major cloud service provider could impact multiple insureds at once, thus creating potential systemic event for the insurers and reinsurers that backstop these losses. Several leading Cyber insurers are responding by adding policy language that limits their exposure to these potentially catastrophic events. Carrier rationale is that a market-wide effort to address systemic Cyber risk is necessary to manage capacity to pay claims, as volatility and demand for Cyber insurance continues to grow.

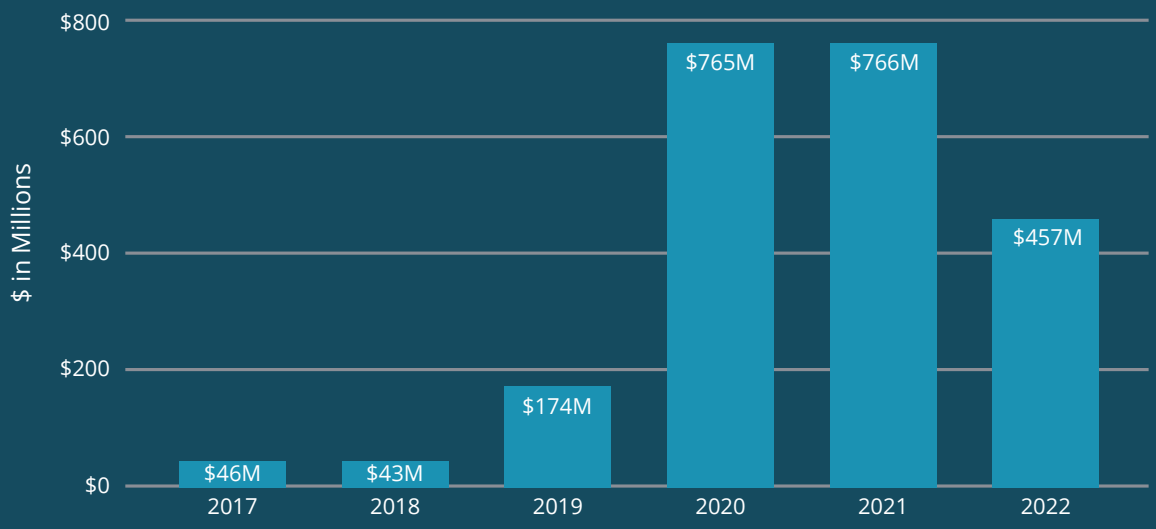
Supply chain disruption goes beyond cloud infrastructure providers. Many organizations are also reliant on Software as a service (SaaS) providers. There have been several high-profile events in this area and Gartner predicts that **by 2025, 45% of organizations worldwide will have experienced attacks** on their software supply chains—this is a three-fold increase from 2021. The Net Diligence 2022 Cyber Claims study shows an increase in average business interruption costs on Cyber claims from $340,000 from 2017-2021, to $707,000 in 2021.

Underwriters are also starting to evaluate an insured's third-party Cyber risk by evaluating the IT security controls of their insureds' supply chain. Business leaders should consider tools that can help measure the security of their IT vendors based on noninvasive scanning technology. There should also be emphasis on contractual provisions that require their vendors to maintain certain IT controls and procedures to protect their data and ongoing operations. Another point of emphasis is awareness of the cost of downtime. Cyber insurance provides a wealth of resources to help an organization get back up and running and access to forensic accounts to assist with the loss quantification.

CLAIM ACTIVITY

While the years 2019-2021 were particularly challenging for Cyber insurance companies due to severity of ransomware claims, 2022 was a more favorable experience. Ransomware attacks declined 61% in 2022 and the percentage of companies that paid a ransom dropped from 82% to 68%, according to a recent survey from Delinea.

TOTAL VALUE RECEIVED BY RANSOMWARE ATTACKERS
2017-2022



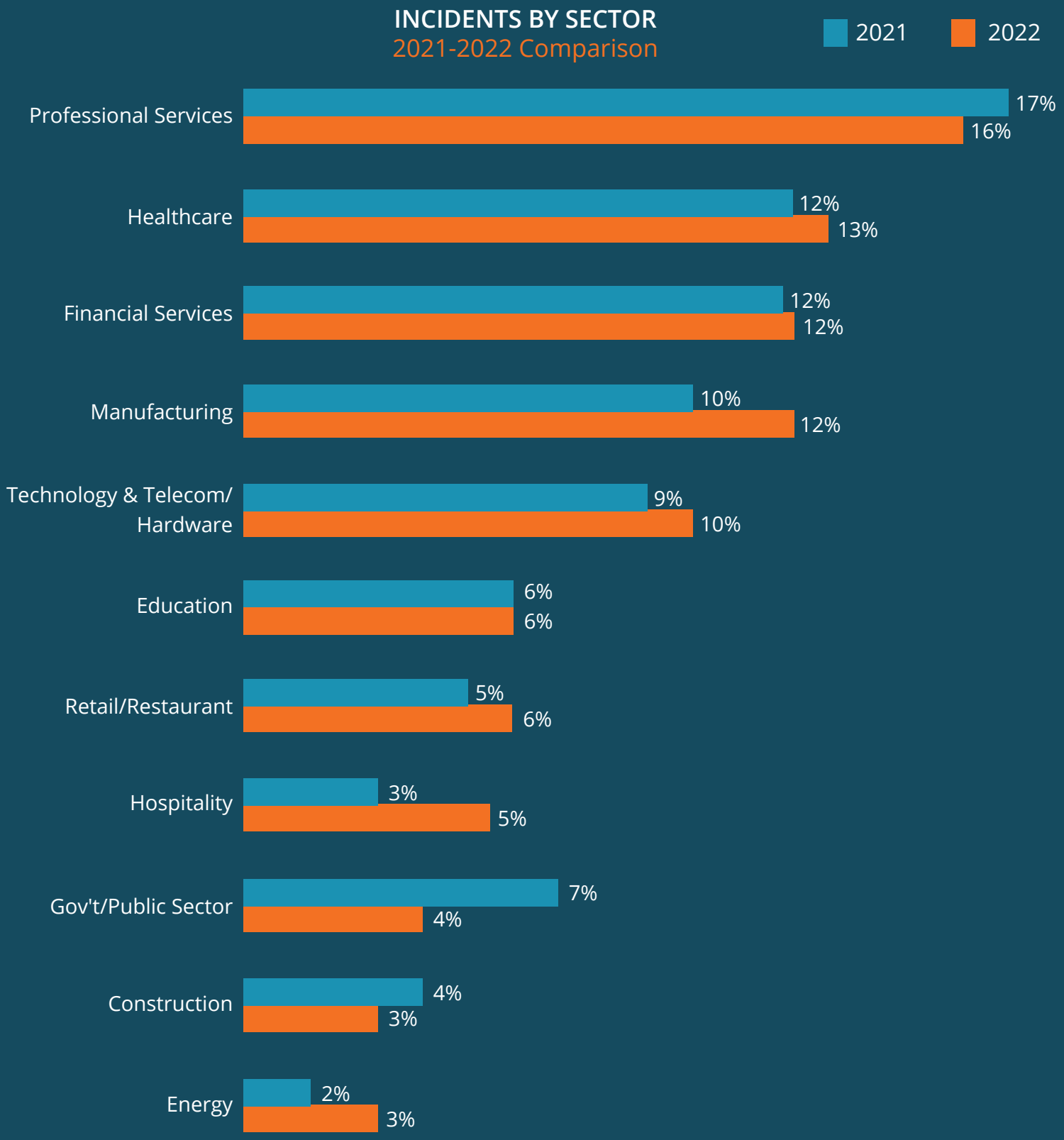
Source: Chainalysis

+ There are a wide range of variables why ransomware claims declined in 2022. One notable example was the improvement in data backups. The ability to restore data from backups allowed organizations to avoid extended downtime and having to pay extortions.

+ Extortionists have been forced to change their strategies and have now resorted to exfiltration of confidential data as a means of leverage. 48% of ransomware claims involved exfiltration 2022, an all-time high.

While the frequency of successful ransomware attacks is down, there are still attacks occurring. The attacks continue to increase in severity. According to Cypfer, ransom demands increased in Q4 2022 to an average of $710,000. The highest demand observed in December was $55 million and was the Royal ransomware variant.

The key to a successful ransomware is organizational vulnerability and poor hygiene. As noted in the below summary from Kroll, Cyber criminals do not discriminate by industry group.



As a corollary, Cyber claims related to Funds Transfer Fraud (FTF) and social engineering increased. A recent study from Cyber insurance company, Corvus, indicated that 28% of claims related to funds transfer fraud, their largest claims category for 2022.

+ Business Email compromise was the most common root cause of claims.

+ Claims concerning social engineering that compels an insured's vendor or client to wire money to a fraudulent bank account, known as invoice manipulation, is a more frequent occurrence.

Third-party Cyber risk, or losses stemming from breaches or failures of third-party providers affecting an insured, showed the fastest growth in proportion of overall claims.

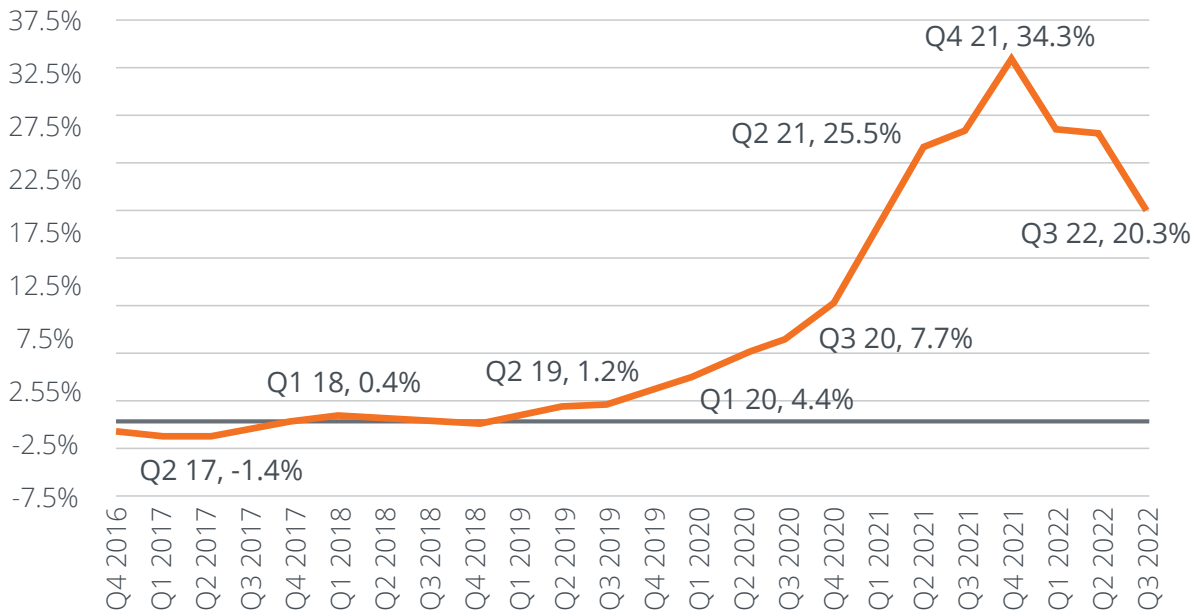
MARKETPLACE DYNAMICS

With the rise of ransomware there was also an increase in underwriting scrutiny for Cyber insurance coverage. Cyber insurance carriers have come to rely on external scanning technology to find high risk vulnerabilities and require immediate mitigation. They are also requiring mandatory security controls. As threat actors find more ways to bypass those security controls, underwriting requirements continue to shift in order to qualify for coverage.

The result of those underwriting controls and next-generation underwriting is resulting in more favorable loss ratios for insurance carriers. That loss ratio has direct implications on premium rates. Better loss ratios will result in more competitive premium rates.

Cyber premium rates have recently seen industry highs, from Q1 2020 to Q4 2021 CIAB reported an increase of 29.9%. We have started to see some stabilization as evidenced by the decrease in Q3 2022.

PREMIUM CHANGE FOR CYBER, Q4 2016 - Q3 2022



Source: https://www.ciab.com/download/35895/?tmstv=1668540348

Though loss ratios vary from carrier to carrier based on their business model, a standard gauge in the P&C market would be a carrier seeking a loss ratio between 50-55%. Based on this we can determine that during the 2021 poll of admitted carriers by NAIC the majority of carriers were seeing a negative impact to their Cyber books. Paying out more in claims than what they were requiring in premium. This led to a right sizing of rates and the underwriting environment we have seen over the past six quarters.

Exhibit 1: Top 20 Admitted Groups (Does Not Include Alien Surplus Lines)

2021 Rank	2020 Rank	Group Number	Group Name	Direct Written Premium	Loss Ratio w/DCC	Market Share
1	1	626	Chubb Ltd Grp	473,073,308	76.9%	9.8%
2	8	158	Fairfax Fin Grp	436,447,801	51.9%	9.0%
3	2	968	AXA Ins Grp	421,013,729	86.5%	8.7%
4	11	3098	Tokio Marine Holdings Inc Grp	249,785,218	43.8%	5.2%
5	3	12	American Intl Grp	240,613,748	130.6%	5.0%
6	*	3548	Travelers Grp	232,276,831	72.7%	4.8%
7	5	4942	Beazley Grp	200,877,555	38.7%	4.2%
8	7	218	CNA Ins Grp	181,382,785	87.5%	3.8%
9	*	1279	Arch Ins Grp	171,944,995	9.2%	3.6%
10	6	3416	AXIS Capital Grp	159,059,212	105.2%	3.3%
11	13	212	Zurich Ins Grp	151,865,004	76.9%	3.1%
12	14	111	Liberty Mut Grp	138,216,723	95.2%	2.9%
13	12	3219	Sompo Grp	133,519,577	54.3%	2.8%
14	10	23	BCS Ins Grp	132,043,119	80.1%	2.7%
15	*	91	Hartford Fire & Cas Grp	123,163,166	16.3%	2.6%
16	*	361	Munich Re Grp	119,989,106	69.0%	2.5%
17	20	181	Swiss Re Grp	103,827,837	32.7%	2.2%
18	*	501	Alleghany Grp	88,554,222	20.5%	1.8%
19	*	98	WR Berkley Corp Grp	81,249,260	36.9%	1.7%
20	16	31	Berkshire Hathaway Grp	71,365,401	-0.5%	1.5%

NAIC Report on the Cyber Insurance Market, October 18 2022
https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf

MARKET EVOLUTION

As noted, one of the lessons learned from the increase in loss activity was a need for more security specific underwriting scrutiny beyond static annual questionnaires. This has led to the rise of "insurtechs". An insurtech is a company that combines the use of technology and an insurance product. These companies approach Cyber risk with the idea that security and insurance go hand in hand. Taking a proactive approach to how they underwrite risk using analytics as well as how they look to prevent incidents from happening with their extensive pre-breach service offerings and real time monitoring. Using security engineers and data scientists, insurtechs have disrupted the Cyber marketplace through innovation and more intuitive solutions.

The market size, measured by revenue, of the Cyber Insurance industry was $3.5 billion in 2022. The market size of the Cyber Insurance industry is expected to increase 7.7% in 2023. S&P Global Ratings noted in a 2022 report that while the demand for Cyber risk protection is growing, the capacity for reinsurance in this sector is not keeping the same pace. This void in the marketplace poses an issue for Cyber carriers looking to grow and keep up with demand. Carriers will have the option to rely less on re-insurance and maintain this volatile class of business on their balance sheet or explore alternative means to spread the risk. As an example, Beazley, a specialist Lloyds of London insurer, recently launched the market's first Cyber catastrophe bond. This is the first time that a liquid Insurance-Linked Securities (ILS) instrument has been created for Cyber catastrophe risks. The $45 million bond gives Beazley indemnity against all perils more than a $300 million catastrophe event. To increase the risk transfer marketplace, the standard insurance will need to collateralize risk pools like other lines of insurance (ex. Property insurance). This is a substantial milestone and will bring more participants to the market place.

LOOKING FORWARD

The rate increases and enhanced underwriting scrutiny have had the desired effect and carrier loss ratios have improved to target ranges. This is in combination with the number of new market entrants will result in a more favorable environment for buyers. We expect that rates will likely be at or close to flat over the coming twelve months. There will be notable exceptions based on certain industry groups that have had poor loss ratios in the past five years. While the rate environment will be competitive, we do expect carriers to maintain discipline on policy terms and conditions. We also emphasize that underwriters will continue to insist on "must have" controls in order to qualify for the insurance. There will also be heightened scrutiny of the identified emerging risks that will inevitably lead to more loss activity and subsequent volatility within the marketplace.

KEY TAKEAWAYS

- Cyber risk will continue to pose an unknown source of volatility for organizations
- Unforeseen risks within the Cyber realm will increase in magnitude
- Increased competition and innovation have had positive effect within the industry
- Cyber insurance carriers have returned to profitability and will provide more competitive terms but will also be cautious in outlook
- Cyber insurance will continue to be an essential tool for both risk identification, pro-active remediation and a financial backstop

MORE THAN JUST INSURANCE

Based in North America, Parker, Smith & Feek is an integrated financial services company focused on protecting the assets of its widely varied client base through insurance, risk management and wealth management solutions. As an employee-owned company, Our 1,800-plus associates are empowered to provide customized solutions for their clients' unique needs.

PARKER SMITH & FEEK
An IMA Company

MARKETS IN FOCUS CONTRIBUTORS

TIM BURKE, Executive Vice President, Head of Cyber

ALEX FULLERTON, Marketing Specialist

JIM MILLAR, Account Executive, Cyber Risk Solutions

AUTUMN STONE, Account Executive, Cyber Risk Solutions

www.psfinc.com