TOKIO MARINE HCC

CYBER STRONG®

2023 Cyber Report

CYBER & PROFESSIONAL LINES GROUP

CONTENTS

INTRO

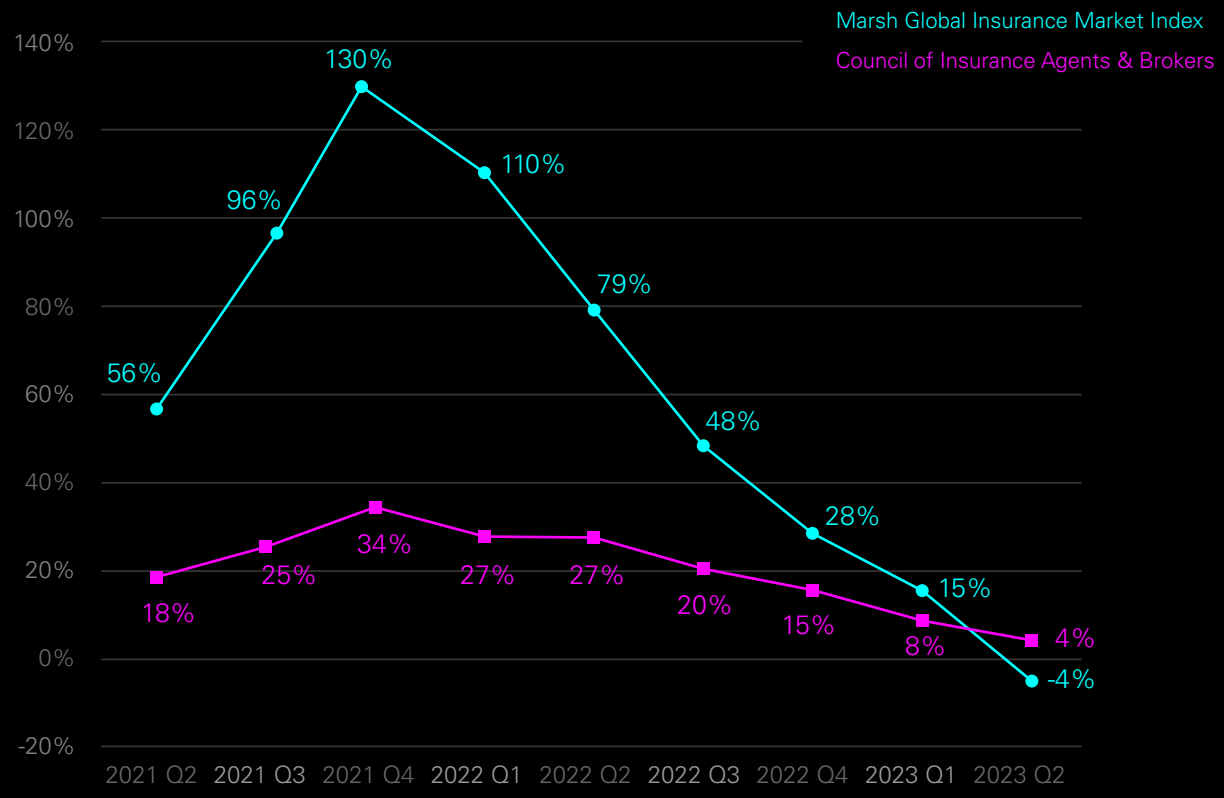
Over the past three years the cyber insurance market has experienced both unprecedented growth and substantial changes to its underwriting approach in an effort to respond to the changing cyber threat landscape. While some may have hoped that the drop in ransomware and decelerating rate increases were a sign of market stabilization in 2022, cyber-attacks are once again back in the headlines in a big way. This year could set a new record for financially motivated cyber-attacks, with several widespread cyber events adding to mounting attritional cyber losses. The increase in cyber losses comes at a time when the cyber insurance market's apparent return to profitability coincides with the emergence of softening market conditions. It could, once again, find itself at an inflection point if the current trends continue.

Cyber risk is unpredictable in nature and continues to deliver new challenges to insurers. In this report we will delve into the insurance cyber market's performance throughout the past couple of years, offering an overview of noteworthy cyber loss trends, placing special emphasis on ransomware.

State of the Market: Rapid Cyber Market Growth & Profitability Improvement

With the onset of the ransomware wave in 2019, the cyber insurance market has spent the last three years adjusting pricing and underwriting to a new reality. While those years coincided with a hard market in most P&C lines, cyber insurance saw the most significant correction of any line of insurance business. At the peak of the hard market in the fourth quarter of 2021, the leading insurance market rate indexes reported cyber price change of 130% and 34%, as shown in Figure 1.

Figure 1: Quarterly Cyber Rate Change



Marsh Global Insurance Market Index tracks price change in major P&C lines based on its own client portfolio while The Council of Insurance Agents & Brokers (CIAB) collects price information through a survey of its members.

Source: Marsh Global Insurance Market Index Q1 2021-Q1 2023, Council of Insurance Agents and Brokers P/C Market Survey Q1 2021 to Q1 2023

Price change has been a major component of the cyber market's response to the ransomware epidemic, but changes to insurers' underwriting approach have been equally impactful. Tightened eligibility criteria, modifications to application forms, use of cyber threat intelligence and targeted vulnerability scanning are among the efforts undertaken by insurers to improve profitability.

The increase in both rates and demand for coverage has resulted in dramatic growth in written cyber premiums, making cyber the fastest growing commercial insurance product in both 2021 and 2022. From 2019 to 2022 direct written cyber premiums in the US market grew from $2.2 billion to $7.2 billion based on statutory reporting (Figure 2). The top five cyber insurers accounted for about a third of the total written premiums in 2022. While statutory reporting captures most US cyber premiums, the US and Global cyber insurance markets are estimated to be $9 billion and $14 billion, respectively (1).

Figure 2: 2021-2022 Cyber Insurance Market Premium and Loss

Rank 2021	Rank 2022	Company Name	2021 DPW	2022 DPW	2021-22 DPW Change (%)	Market Share (%)	% of Cyber DPW Standalone	% of Cyber DPW Packaged	2021 Loss & DCC Ratio	2021 Loss & DCC Ratio	Est. UW Exp	Est. Comb Ratio
01	01	Chubb INA Grp	473.1	604.9	27.9	8.4	0.0	100.0	76.9	53.8	23.7	77.5
02	02	Fairfax Financial (USA) Grp	436.4	563.0	29.0	7.8	100.0	0.0	51.9	54.0	28.6	82.6
03	03	XL America Cos	421.0	527.4	25.3	7.3	100.0	0.0	86.5	66.2	24.3	90.5
04	04	Tokio Marine US PC Grp	249.8	367.6	47.2	5.1	79.7	20.3	43.8	57.8	28.6	86.4
09	05	Arch Ins Grp	171.2	346.4	102.3	4.8	93.3	6.7	9.2	52.3	28.4	80.7
06	06	Travelers Grp	232.3	315.3	35.8	4.4	82.8	17.2	72.7	34.8	30.9	65.7
05	07	American Int'l Grp	240.6	299.0	24.3	4.1	99.8	0.2	130.6	47.6	23.3	70.9
08	08	Nationwide Grp	183.1	257.3	40.5	3.6	93.5	6.5	33.1	12.5	30.8	43.3
13	09	Zurich Ins US PC Grp	151.9	252.5	66.3	3.5	75.0	25.0	76.9	68.2	19.7	87.9
15	10	Sompo Holdings US Grp	133.5	248.0	85.7	3.4	100.0	0.0	54.3	50.1	25.5	75.6
09	11	CNA Ins Cos	181.4	228.9	26.2	3.2	12.1	87.9	87.5	26.5	26.9	53.4
11	12	Berkshire Hathaway Ins Grp	159.9	228.5	42.9	3.2	67.5	32.5	-22.7	48.1	20.5	68.6
14	13	Liberty Mutal Ins Cos	141.5	208.2	47.1	2.9	49.8	50.2	92.1	57.5	32.8	90.3
19	14	Swiss ReIns Grp	103.8	207.0	99.4	2.9	100.0	0.0	32.7	19.6	33.2	52.8
12	15	AXIS US Operations	159.1	195.7	23.1	2.7	85.7	14.3	105.2	85.9	25.7	111.6
07	16	Beazley USA Ins Grp	200.9	174.6	-13.1	2.4	94.4	5.6	38.7	19.6	24.2	43.8
22	17	Ascot Ins U.S. Grp	64.3	166.6	158.9	2.3	44.3	55.7	19.0	30.2	31.8	62.0
32	18	Randall Grp	25.1	161.7	545.3	2.2	98.6	1.4	0.2	10.7	36.8	47.5
27	19	Markel Corporation Grp	46.9	152.9	226.2	2.1	75.1	24.9	90.6	40.1	30.1	70.2
26	20	Hartford Ins Grp	123.2	152.3	23.7	2.1	15.0	85.0	16.3	15.5	30.0	45.5
		Top 5*	1751.5	2409.3	37.6	33.3	66.0	34.0	78.4	57.1	26.4	83.5
		Top 10*	2531.5	3781.5	40.4	52.3	60.8	39.2	75.9	51.9	26.3	78.2
		Top 20*	3737.5	5657.9	45.1	78.2	59.0	41.0	70.8	46.3	27.2	73.5
		Total Standalone	3152.0	5090.8	61.5	65.3	0.0	0.0	0.0	43.1	27.6	70.8
		Total Package	1676.8	2146.0	28.0	34.7	0.0	0.0	0.0	47.9	26.4	74.3
		Total P/C Industry	4828.8	7236.7	49.9	100.0	65.3	34.7	67.6	44.6	27.3	71.9

Source: Reprinted from "US Cyber: First Hard Market Cycle Brings a Return to Profitability," June 13, 2023, AM Best Market Segment, Copyright 2023 by AM Best.

The price and underwriting changes introduced by insurers during the hard market have led to significant improvements in cyber market loss ratio performance. While 2020 and 2021 most likely produced an overall market loss in stand-alone cyber insurance, the 2022 year shows a remarkable recovery with 23 points reduction to 44.6% in total cyber loss ratio (Figure 2)*.

*It's worth noting that the approach to statutory reporting of cyber loss ratios may vary among insurers. Modeled loss development (the difference between the initial reserve and the final loss amount) may not be included in some insurers' reported losses. The ultimate loss ratio can be as much as 50 percent higher than the sum of initial loss payments and case reserves in a given accident year.

Profitability improvements are not exclusively attributed to changes implemented by cyber insurers. As ransomware became the leading driver of cyber insurance losses, there have also been notable fluctuations in attack activity, even on a quarterly basis. The second and third quarters of 2022 saw a dramatic reduction in ransomware levels which also contributed to improved performance in the cyber market.

The reduction in ransomware levels in 2022 combined with price improvements over the past three years, fueled very competitive cyber market conditions in the first half of 2023. Although the Marsh and CIAB cyber rate reports demonstrate positive rate change in the cyber market in the first quarter of 2023, Aon reported negative rate change in its client portfolio as early as November 2022, with rates hitting-26% in March 2023 (2). At the same time ransomware appears to have returned to levels observed in 2020 and 2021 and concerns about cyberwar and systemic cyber events are at an all time high.

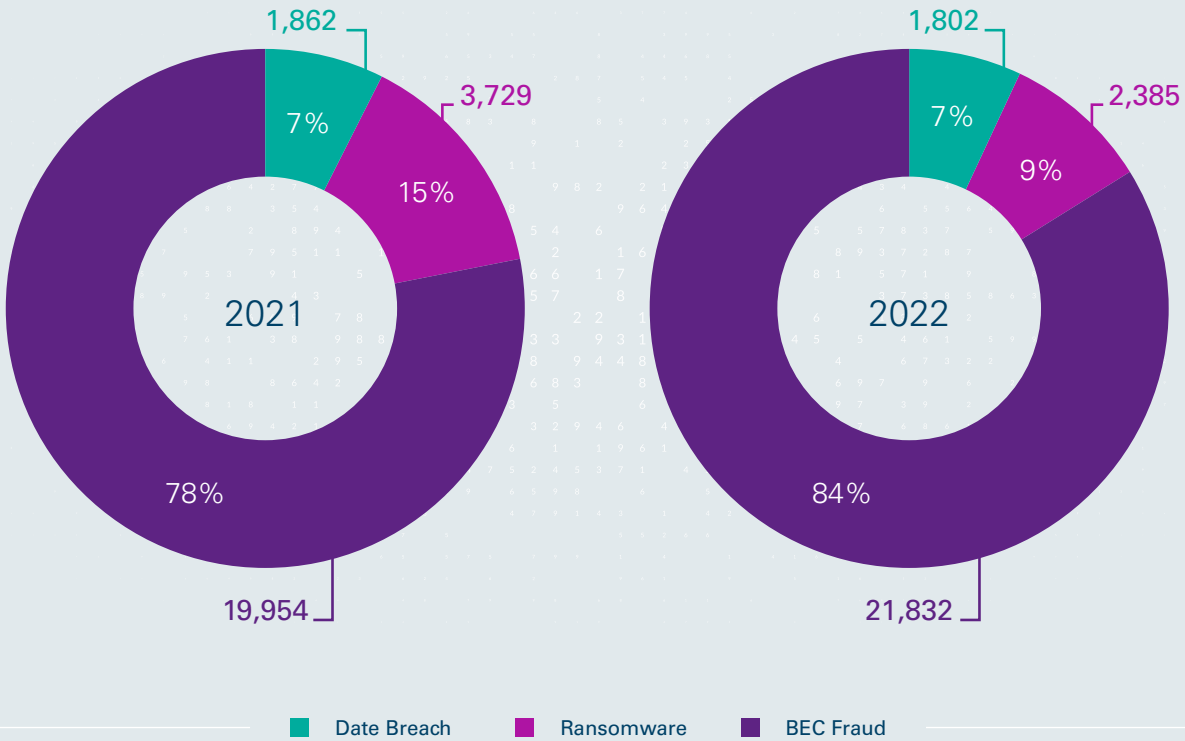
Cyber Loss Drivers: The Ransomware Roller Coaster Continues

The three main drivers of loss in the cyber insurance market are: ransomware, business email compromise (BEC) fraud and data breaches. While that configuration remained the same in 2022, there were notable changes in cyber loss trends compared to recent years. Ransomware remains the main contributor to cyber losses, but the ransomware curve broke unexpectedly in 2022, and, by all indications, both the frequency and severity of attacks dropped significantly. At the same time, a category of cyber claims that has been underway for some time, started to gain traction: privacy violations through unlawful collection of private information.

Ransomware Groups Were Disrupted in 2022

Accurate cyber incident tracking remains challenging as data breaches are still the only type of cyber incident that is subject to mandatory reporting to the US authorities. In 2022 data breaches remained relatively flat at 1,802 reported breaches vs 1,862 in the prior year (Figure 3). Although the FBI estimates that only 20% of ransomware attacks are reported to the authorities, the FBI IC3 report provides some level of insight into year over year changes in incident frequency in the US. The report shows that BEC fraud incidents increased 9% and ransomware incidents dropped 36% from 2021 to 2022. For comparison, our own (Tokio Marine HCC – Cyber & Professional Lines Group) portfolio of insureds saw a 58% reduction in ransomware incidents and a 35% reduction in BEC fraud incidents.

Figure 3: Reported Cyber Incidents 2021-2022



Source: FBI IC3 Report 2021-2022, Identity Theft Resource Center 2021-2022 Data Breach Report

We believe that the 2022 reduction in frequency of ransomware losses in the US can be attributed to multiple underlying causes:

- The Russia-Ukraine conflict, which caused disruption to many of the ransomware groups operating out of these territories.
- Although temporary, the takedown of one of the most prolific ransomware groups (Conti) contributed to a drop in ransomware attacks.
- Leading threat actors may have transitioned to attacking organizations outside the US to avoid attention from US government agencies.
- Many US organizations have adopted better security standards, especially due to concerns over ransomware attacks.
- Organizations are required to have certain cybersecurity controls when they purchase cyber insurance coverage. This may have resulted in a more significant drop in ransomware frequency compared to uninsured organizations.

The Most Expensive Cyber Loss is Still Ransomware

While BEC fraud is the most common cyber threat to organizations, ransomware attacks result in much higher average costs to victims based on cyber loss data reported by the insurance industry. The average BEC fraud loss was $125,000 in 2022, up 4% vs 2021 (Figure 4). By comparison, average ransomware losses are three to four times that amount. Figure 5 shows the aggregated average ransomware loss cost from the NetDiligence Cyber Claims Study compared to our own portfolio average ransomware loss for the 2021 and 2022 years. Both data sets show a significant drop in average ransomware loss amounts in 2022.

Figure 4: Average BEC Fraud Loss 2021-2022

Figure 5: Average Ransomware Loss 2021-2022

Figure 4 Source: FBI IC3 Report 2021-2022, Tokio Marine HCC Cyber & Professional Lines Group Loss Data 2021-2022.
Figure 5 Source: NetDiligence Cyber Claim Study 2021-2022, Tokio Marine HCC- Cyber & Professional Lines Group Loss Data 2021-2022 (Organizations <$2 billion revenue)

Sharp Increase in Attack Activity in H1 2023

Although reporting of ransomware attacks is not required, it is highly encouraged. Victim organizations hesitate to report attacks out of fear that public knowledge could tarnish their reputation. Even with the lack of ransomware reporting, certain data sources can validate attack activity in practically real time. Data collected from extortion sites, government agencies, hacking forums and news publications by Recorded Future show a dramatic uptick in ransomware in the second quarter of 2023 (Figure 6). This aligns with changes in ransomware frequency observed in our own portfolio during the same period.

Figure 6: Monthly Ransomware Activity Based on Extortion Sites

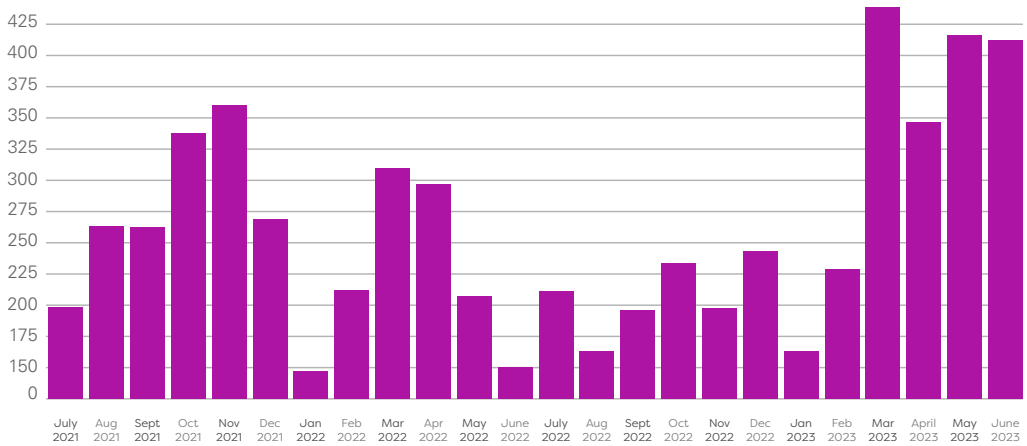


Figure 6 Source: The Record, Recorded Future News

Research by Chainalysis shows that ransom payments through June of this year are nearly at 2021 levels based on illicit crypto wallets monitored by the firm (*not representative of all ransom payments). Ransomware groups collected at least $449 million through the first six months of 2023 compared to $939 million for the full 2021 year (11).

Despite the occasional takedown of leading threat actors, the ransomware business is resilient. Cyber extortion has quickly evolved from ransomware to double extortion attacks combining both encryption and exfiltration of data. However, in the first half of 2023 cyber extortion attacks involving only data exfiltration have become more prevalent. This has contributed to a 70% increase in reported data breaches in the first half of 2023 compared to the same period in 2022 (12).

The ransomware ecosystem continues to prove how agile it is in adjusting to security improvements and government actions. With ransomware seemingly nearing or exceeding previous highs, it could once again cause significant changes in the cyber insurance market.

Privacy Litigation on the Rise

Another trend that may cause major impact to the cyber insurance market is the new wave of litigation aimed at privacy violations for the collection of private information through website tracking and biometric scanning.

Website tracking litigation has been around for well over a decade with class action lawsuits targeting companies using so-called zombie cookies (tracking unique user IDs and browser habits) as early as 2010. This time, litigation is focused on the use of website tracking technology known as Meta Pixel, developed by the parent company of Facebook. Meta Pixel is used on more than 30% of the top 100,000 websites, which has led to hundreds of class action lawsuits against US corporations (3). The latest wave of litigation has been aimed at the healthcare sector, to prove violation of state and federal laws protecting the privacy of healthcare information. However, the entertainment sector has also been impacted with alleged violations of The Video Privacy Protection Act. It will take months or years for many of these lawsuits to reach dismissal or settlement, while legal expenses continue to accrue.

On the biometric information side, a recent ruling by the Illinois Supreme Court decided that the $1,000 damages per violation under the Biometric Information Privacy Act (BIPA) accumulate each time biometric data is collected or transmitted, and not just the first time. In a separate case the court also held that a five-year statute of limitations could apply. This could lead to an enormous increase in settlement amounts. In combination, these two decisions have led to a 65% increase in BIPA lawsuit filings over the past few months (4).

Leading Ransomware Attack Vectors

While ransomware continues to be the number one driver of cyber insurance losses, it also presents insurers with an opportunity to help customers mitigate losses. Tracking of leading ransomware attack vectors allows insurers to develop prevention strategies that can be deployed to reduce the frequency of attacks. We continuously perform analyses and review of ransomware claims to ensure our policyholders are aware of some of the most widely leveraged vulnerabilities exploited by ransomware groups. Our CTI (Cyber Threat-Intelligence) team tracks current attack patterns and exposures by scanning customers' external networks, observing honeypot activity and malware logs, and by monitoring sales and chatter in underground markets.

Ransomware operators continue to take advantage of previously discovered and well-recognized tactics, techniques, and procedures (TTPs), such as: phishing, Remote Desktop Protocol (RDP) brute-forcing, and exploitation of remote code execution vulnerabilities. Proactive detection and alerting about critical vulnerabilities and exposures in customers' internet facing assets can substantially reduce the incidence of ransomware attacks.

Figure 7: Leading Ransomware Attack Vectors

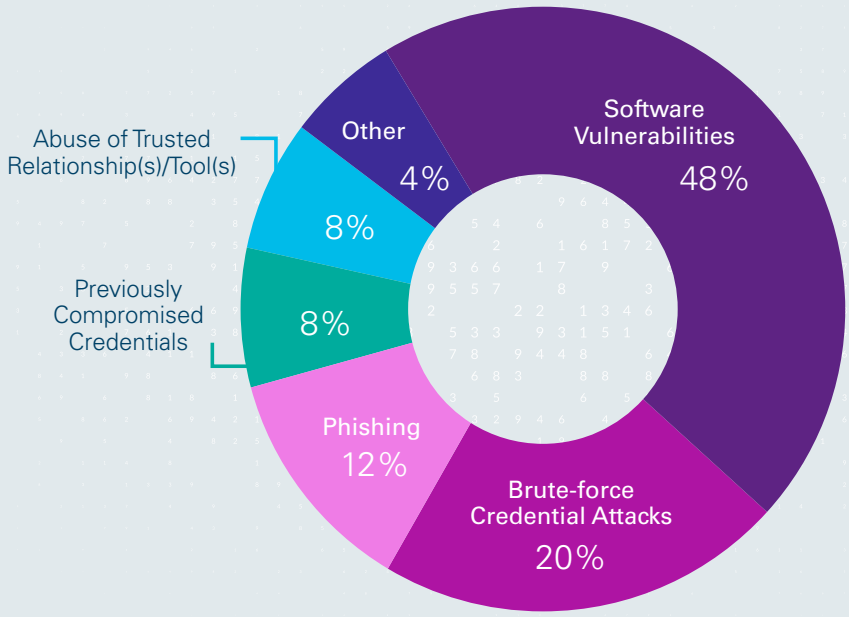
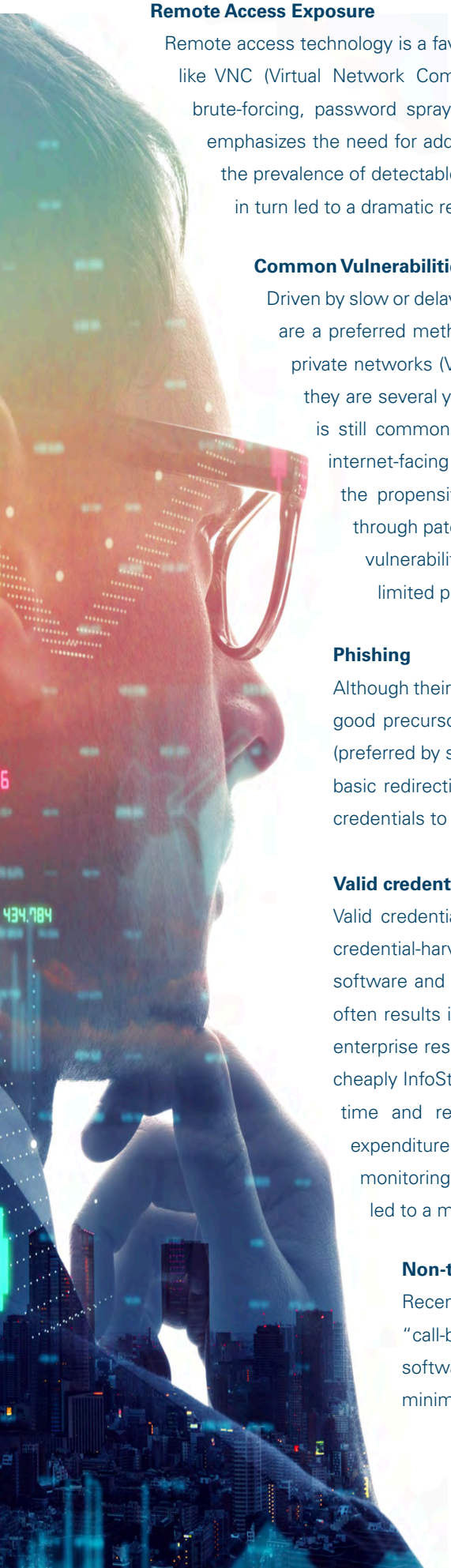


Figure 4 Source: Palo Alto Unit 42 2022 Incident Response Report



Remote Access Exposure

Remote access technology is a favored initial access vector of many ransomware groups. RDP, other remote access services like VNC (Virtual Network Computing), and VPNs (Virtual Private Networks) continue to be highly targeted through brute-forcing, password spraying, or by using valid credentials collected through other means. This continued trend emphasizes the need for additional layers of protection necessary to secure these services. Through proactive alerting, the prevalence of detectable RDP in our portfolio has been reduced by 94% to a rate of just 0.4% of insureds. This has in turn led to a dramatic reduction in RDP driven ransomware losses.

Common Vulnerabilities and Exposures (CVEs)

Driven by slow or delayed patching and widespread availability of exploit code, critical internet-facing vulnerabilities are a preferred method of initial access. Remote code execution CVEs affecting exchange servers and virtual private networks (VPNs) are widely targeted by initial access brokers and ransomware operators, even when they are several years old. For example, CVE-2018-13379, a Path Traversal vulnerability in FortiGate SSL-VPN, is still commonly targeted due to its trivial complexity of exploitation and the widespread presence of internet-facing vulnerable devices. This indicates either a general lack of an effective patching cadence or the propensity for organizations to favor temporary mitigations instead of addressing vulnerabilities through patching. Our targeted vulnerability scanning covers approximately 100 remote code execution vulnerabilities associated with ransomware attacks. As a result of these efforts CVEs make up a very limited portion of identified attack vectors in our ransomware incident intake.

Phishing

Although their prevalence appears to have recently diminished, successful phishing campaigns still remain good precursors of ransomware activity, with well-established modular malware payloads, like Qakbot (preferred by some ransomware threat-actors). Using phishing for the delivery of infostealer malware and basic redirections to credential harvesting pages also remain very effective methods of gathering valid credentials to corporate networks. Phishing prevention remains a significant challenge.

Valid credentials

Valid credentials remain a leading root point of compromise, whether obtained through phishing and credential-harvesting pages or captured in InfoStealer logs. InfoStealer malware is often found in torrented software and trojanized free downloads, making widespread infection a growing concern. The infection often results in exfiltrated browser data and provides an ideal method for capturing login credentials for enterprise resources like VPNs and team-collaboration applications. This problem is compounded by how cheaply InfoStealer logs can be purchased in underground markets, allowing threat-actors with available time and resources to extract valuable access with limited log processing-time and monetary expenditure. While there is no silver bullet when it comes to prevention of valid credential attacks, monitoring for info-stealer infections and intercepting corporate access for sale in dark web forums has led to a meaningful reduction in frequency.

Non-technical Exploitation

Recently, a non-technical exploitation resulting in easy access used by threat actors has been "call-back" phishing campaigns. Victims are persuaded to install legitimate remote management software on work computers, allowing attackers remote access to corporate networks, while minimizing the risk of detection by avoiding the use of malware.

Widespread Cyber Events Are Back

When it comes to widespread cyber events, the pattern looks similar to what we've seen in ransomware: somewhat of a lull in 2022, followed by a more recent return to a broader offensive from threat actors.

With the exception of the spillover effect from 2021's widespread log4j vulnerability, 2022 was relatively quiet for large-scale cyber events, and log4shell didn't have the impact the industry expected. Many observers also anticipated a major cyberattack in connection with the Russia-Ukraine war, but, so far, there have been no related incidents outside of Ukraine. However, as noted earlier, widespread attacks are on the rise again in 2023, with threat actors exploiting numerous recently discovered vulnerabilities.

Triple File Transfer Software Exploit

At the end of May, it became clear that users of the file sharing service MOVEit were being targeted at-scale, in what appeared to be an automated attack resulting in the installation of a webshell. The zero-day, now categorized as CVE-2023-34362, allowed threat actors to successfully target and exfiltrate data from hundreds of organizations before the industry could respond with a cohesive remediation and patching strategy. The ransomware group responsible for that attack, known as Cl0p, is also responsible for two prior large-scale compromises involving zero-days earlier this year. In February, Cl0p successfully carried out attacks against GoAnywhere MFT, and in March they were responsible for exploiting PaperCut. The similarities in previous targeting are indicative of the group's focus on file-sharing software. Compromising these systems allows the attacker to extend the extortion to any of the victim organization's clients as a third-party leak exposure.

The use of zero-days made detection and mitigation difficult and has allowed Cl0p to maximize profit due to the speed and scope of those attack. Although there is limited defense against zero-day exploits, the supply chain attacks against file transfer software is a reminder for companies to revisit data hygiene best practices and consider which contractual protections are available to shield them from vendor breaches. (5)

Hypervisor Vulnerability

In early February, the industry also witnessed wide-scale exploitation of VMWare ESXi instances, a hypervisor that manages virtual machines. This attack was not leveraging a zero-day, but two older vulnerabilities (CVE-2021-21974 and CVE-2020-3992) in OpenSLP (Open Service Location Protocol). This resulted in remote code execution and successful compromise of over 3,800 servers worldwide (6). Dubbed "ESXiArgs," the wide-scale attack was not originally attributed to a particular group, though it is now believed the exploit is leveraged by Alphv and Lockbit (7).

Attack Against a Major Cloud Service

In early January, cloud service provider Rackspace suffered a compromise that forced them to shut down their Hosted Exchange environment. Although only 27 of Rackspace's several thousand Hosted Exchange customers were ultimately affected directly by this attack, Play Ransomware operators were able to leverage CVE-2022-41080 to compromise the Outlook Web app (OWA). The exploit was dubbed "OWASSRF" by Crowdstrike, and it revealed a similar methodology of exploitation as ProxyNotShell. However, in this case the attack targeted OWA and proved capable of bypassing all previous ProxyNotShell mitigations. Rackspace had applied mitigations for ProxyNotShell, but had decided not to install the November patches due to possible operational risk (8).

Nation State Hits Crypto, Again

Another widespread attack involved a supply-chain compromise of 3CX's DesktopApp by North Korea, which successfully targeted cryptocurrency companies (9). This attack also highlighted the risk of a potential increase in financially motivated, at-scale cyberattacks from nation states, especially as geopolitical relations between major powers worsen due to current conflicts.

Updated Cyber Catastrophe Estimates

While none of these events are likely to meet the threshold, the estimates associated with hypothetical losses from a major catastrophic cyber event are sobering. In their recent study modeling potential cyber catastrophe, Guy Carpenter concluded that a 1-in-200-year cyber event could result in ground up economic losses ranging from $16 billion to $33 billion (1). By comparison, the largest actual catastrophic cyber event to date was the 2017 NotPetya widespread malware attack that resulted in estimated ground up economic loss of $10 billion (10). The prospect of these damaging large-scale attacks serves to remind us that in addition to alerting customers of critical exposures on their network, it is equally important to provide clear remediation guidance and the tools to sustain a level of awareness of best practices to help mitigate future methods of exploitation.

2023 and Beyond

Although the storyline for 2022 was one of significant reduction in the frequency and severity of ransomware attacks, 2023 in many ways marks a return to what we have unfortunately come to regard as cyber normalcy. Based on what we've observed in the first half of 2023, these are our predictions for the rest of 2023 and beyond:

- Ransomware levels are likely to continue to increase throughout 2023.
- Artificial intelligence is going to lead to more sophisticated attacks.
- Cyber pricing levels will stabilize and may increase again, but not to the levels the market has experienced in the past two years.
- Premium growth in the cyber insurance market will slow to 20-25%, following three record years.
- The MOVEit attack will re-open the debate about systemic risk restrictions or exclusions.
- Insurers' efforts to assist insureds with mitigation of ransomware and other cyber threats will continue to evolve as a key differentiator in the cyber market.

They say, history repeats itself; however, it's been tough to predict what happens in the cyber market. It really encompasses the term emerging risk as there are always new exposures and devised tactics. While the cyber insurance market seems to have relaxed both its pricing and security control requirements following last year's profitability improvements, the return of significant ransomware activity and several widespread cyber events in 2023 should be a wakeup call.

Sources

(1) Guy Carpenter Report "Through the Looking Glass: Interrogating the Key Numbers Behind Today's Cyber Market," May 31, 2023, https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Guy_Carpenter_Cyber_(Re)insurance_Market_Report_Publish_rev%20.pdf

(2) Aon Report "Buyer-Friendly Cyber and E&O Market: How to Take Advantage," May 2023, https://www.aon.com/insights/articles/2023/buyer-friendly-cyber-and-e-and-o-market-how-to-take-advantage

(3) Julia Angwin. The Markup. August 20, 2022, https://themarkup.org/newsletter/hello-world/facebooks-pervasive-pixel.

(4) Stephen Joyce and Skye Witley. Privacy and Security Law. Bloomberg Law at Bloomberg Industry Group, May 2, 2023, https://news.bloomberglaw.com/privacy-and-data-security/illinois-biometric-privacy-cases-jump-65-after-seminal-ruling

(5) Dan Goodwin. "Casualties keep growing in this month's mass exploitation of MOVEit 0-day." arsTechnica. Condé Naste at Wired Media Group, June 27, 2023, https://arstechnica.com/security/2023/06/casualties-keep-growing-in-this-months-mass-exploitation-of-moveit-0-day/

(6) Cybersecurity & Infrastructure Security Agency "ESXiArgs Ransomware Virtual Machine Recovery Guidance," February 8, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-039a

(7) "Hypervisor Jackpotting, part 3: Lack of Antivirus Support Opens the Door to Adversary Attacks." CrowdStrike Blog. CrowdStrike, May 13, 2023, https://www.crowdstrike.com/blog/hypervisor-jackpotting-lack-of-antivirus-support-opens-the-door-to-adversaries/

(8) Eduard Kovacs. "Play Ransomware Group Used new Exploitation Method in Rackspace Attack." SecurityWeek. Wired Business Media Publication, January 5, 2023, https://www.securityweek.com/play-ransomware-group-used-new-exploitation-method-rackspace-attack/

(9) Jeff Johnson, Fred Plan, Adrian Sanchez, Renato Fontana, Jake Nicastro, Dimiter Andonov, Marius Fodoreanu, Daniel Scott. "3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible." Madiant, April 20, 2023, https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

(10) Elizabeth Blosfield. "Cyber Lessons for the Insurance Industry Continue After Three Years After NotPetya." Insurance Journal News, August 12, 2023, https://www.insurancejournal.com/news/national/2020/08/12/578788.htm

(11) Chainalysis Team. "Crypto Crime Mid-year Update: Crime Down 65% Overall, But Ransomware Headed for huge Year Thanks to Return of Big Game Hunting." Chainalysis Blog, July 12, 2023, https://blog.chainalysis.com/reports/crypto-crime-midyear-2023-update-ransomware-scams/

(12) ID Theft Center Resource. "H1 2023 Data Breach Analysis." ID Theft Resource Center, 2023, https://www.idtheftcenter.org/publication/h1-2023-data-breach-analysis/

TOKIO MARINE HCC

2023 Cyber Report

tmhcc.com/cyber

Cyber... With Confidence.

Tokio Marine HCC has been innovating in Cyber Liability Insurance worldwide, for over 20 years. Our dedicated global team is made up of cyber insurance and in-house claims experts with deep industry knowledge and a wealth of cyber security experience. We promote active knowledge exchange, making us a global leader when it comes to cyber risk, while keeping you at the forefront of emerging threats on the ever-evolving Cyber landscape. From offices in the U.S., our cyber team insures US-domiciled businesses, with a focus on the small- to mid-sized segment, as well as individuals concerned with protecting their family, home and privacy from cyber threats. From Europe and the U.K., our team concentrates on mid- to large-sized businesses domiciled anywhere outside of the U.S. In addition, we leverage our in-house Cyber expertise to enhance other Tokio Marine HCC insurance coverages, letting you take on risk with confidence.

Learn more about Cyber at Tokio Marine HCC by visiting tmhcc.com/cyber

Follow us on LinkedIn: #TMHCC_Cyber
