TOKIO MARINE HCC

2024

Cyber Market Report

The U.S. cyber insurance market, lauded for its rapid expansion and record growth between 2020 and 2022, is now undergoing a pivotal transformation. After years of consistently high annual growth rates, the landscape has shifted in 2023, with annual growth of just 1.6% as a result of declining premium rates and limited growth in new policyholders. Meanwhile, there has been a notable rise in cyber extortion activity in the past 18 months and as fewer organizations feel pressured into paying extortion demands, threat actor groups have turned to more aggressive tactics and high value targets.

As we delve into the data and analysis, including past and current extortion activity, it becomes clear that the industry is confronted with both immediate and long-term hurdles.

US Cyber Market: Modest Growth

Following triple digit growth in the 2020 to 2022 period and achieving the highest growth of any commercial insurance product, the US cyber insurance market is facing a new reality. In 2023, domestic stand-alone cyber premiums experienced a slight contraction of 2%, while domestic package cyber premiums saw a moderate 5% increase. With stand-alone cyber premiums comprising 69% of written premiums and package cyber policies accounting for 31%, the overall domestic written premium growth was just 0.2% to $7.25 billion. Premiums written by alien surplus lines insurers, primarily Lloyd's, fared slightly better as they increased by 7% to $2.59 billion. In total the US cyber market grew a modest 1.6% to $9.84 billion (NAIC Cyber Report 2024)[1].

Declining Rates and Limited New Policyholders

The stagnation in market growth observed in 2023 can be attributed to a combination of declining premium rates and limited growth in policy count. While the hard market saw significant growth by premium rate increases, policy count growth remained comparatively modest. From 2020 to 2023, the number of US domestic policies increased just 10%, whereas premiums grew by 142% during the same period (NAIC Cyber Report 2024).

[1] Report on the Cybersecurity Insurance Market. National Association of Insurance Commissioners, Oct. 2024, https://content.naic.org/sites/default/files/cmte-h-cyber-wg-2024-cyber-ins-report.pdf

Without significant influx of new buyers entering the US cyber market, growth will continue to predominantly depend on price change and the market will likely fail to reach long term growth projections and necessary market diversification. Although 2023 data suggests a positive trend in policy count growth, some of this increase may be attributable to previously unreported package policies. For instance, one insurer reported an increase in policies from 96,300 to 349,500 while another saw growth from 198,300 to 284,600 (AM Best Cyber Report 2024).[2]

Figure 1: Cyber Market Rate Change 2020-2024 Q3

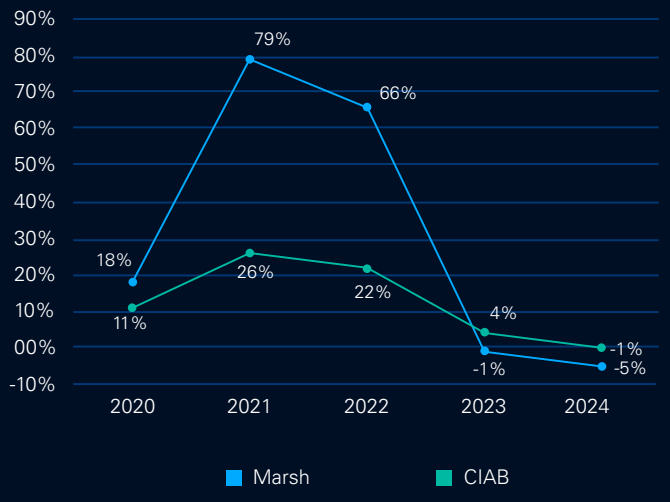
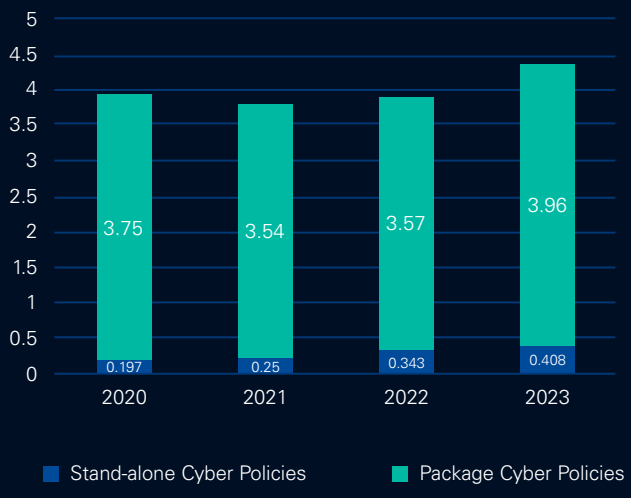


Figure 2: U.S. Domestic Policy Count 2020-2023



[2] *"Global Cyber Insurance," June 24, 2024, AM Best Market Segment, Copyright 2024 by AM Best*

Figure 1: 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: Reprinted Marsh Global Insurance Market Index 2020 to 2024 H1, Council of Insurance Agents and Brokers P/C Market Survey 2020 to H1 2023

Figure 2: The National Association of Insurance Commissioners collects premium, policy count and loss data from US Insurers.

Source: NAIC 2024

In 2024, premium rate change in the US cyber insurance market has fallen to below zero, marking the onset of a soft market. In addition to price reductions, insurers have also rolled back eligibility criteria, expanded coverage and reduced deductible levels over the past 12 months. Insurance market cycles typically shift following a few years of price hikes, and given the significant tightening between 2020 and 2022, it is not surprising that the market has transitioned into a soft phase. Hard markets, on the other hand, typically happen after several years of elevated loss activity, falling premium rates and/or one or several catastrophic events. The question is how long the soft market phase will last and what can be inferred from the 2023 year loss performance and the loss activity we've observed in 2024 so far. It's possible that cyber insurance will see more rapid shifts in market cycles than traditional lines of insurance given the dynamic nature of the risk.

Continued Profitability Improvement?

While premium growth stagnated in 2023, so did loss ratios based on the NAIC's reported loss figures. The reported loss ratio for stand-alone cyber increased by just over one point to 44.3% with package cyber loss performance improving 12 points to 35.5%. The combined result was a 3-point reduction in cyber market loss ratio to 41.6%.

Figure 3: 2022-2023 US Domestic Cyber Insurance Market Premium and Loss

Top 20 Cyber Insurers
($ millions)

Rank ###	Rank ###	Company Name	2022 DPW	2023 DPW	2022-23 DPW Chg (%)	Market Share (%)	% of Cybersecurity DPW Standalone	% of Cybersecurity DPW Packaged	2022 Loss & DCC Ratio	2023 Loss & DCC Ratio	Est. UW Exp Ratio	Est. Comb Ratio
1	1	Chubb INA Grp	604.9	573.6	-5.2	7.9	0.0	100.0	53.8	39.1	23.6	62.7
3	2	XL America Companies	527.4	487.2	-7.6	6.7	100.0	0.0	66.2	62.6	24.2	86.8
2	3	Fairfax Financial (USA) Grp	563.0	463.0	-17.8	6.4	100.0	0.0	54.0	51.0	33.7	84.6
6	4	Travelers Grp	315.3	384.9	22.0	5.3	84.7	15.3	34.8	22.4	33.8	56.2
4	5	Tokio Marine US PC Grp	367.6	377.9	2.8	5.2	78.0	22.0	57.8	44.6	29.0	73.6
12	6	Berkshire Hathaway Insurance Grp	228.5	289.3	26.6	4.0	40.3	59.7	48.1	47.1	26.5	73.6
5	7	Arch Insurance Grp	346.4	282.1	-18.5	3.9	88.6	11.4	52.3	58.1	30.0	88.1
7	8	American International Grp	299.0	274.4	-8.2	3.8	100.0	0.0	47.6	79.3	23.3	102.6
10	9	Sompo Holdings US Grp	248.0	262.9	6.0	3.6	100.0	0.0	50.1	44.9	25.5	70.4
208	10	Starr International Grp	0.0	260.0	NA	3.6	47.8	52.2	0.0	0.0	16.0	16.0
11	11	CNA Insurance Companies	228.9	228.4	-0.2	3.2	13.1	86.9	26.5	36.2	28.4	64.6
8	12	Nationwide Property & Casualty Gr	257.3	226.5	-12.0	3.1	93.8	6.2	12.5	27.6	32.8	60.4
9	13	Zurich Insurance US PC Grp	252.5	199.2	-21.1	2.8	72.8	27.2	68.2	63.5	20.0	83.5
15	14	AXIS US Operations	195.7	181.3	-7.4	2.5	88.5	11.5	85.9	73.2	28.7	101.9
13	15	Liberty Mutual Insurance Cos	208.2	178.3	-14.4	2.5	45.6	54.4	57.5	74.0	46.7	120.7
20	16	Hartford Insurance Grp	152.3	174.8	14.8	2.4	14.1	85.9	15.5	11.3	30.5	41.9
17	17	Ascot Insurance U.S. Grp	166.6	174.5	4.8	2.4	52.6	47.4	30.2	30.1	31.9	61.9
24	18	AMTrust Grp	115.9	170.0	46.7	2.3	87.8	12.2	7.6	4.9	36.4	41.3
16	19	Beazley USA Insurance Grp	174.6	149.6	-14.3	2.1	93.7	6.3	19.6	18.3	28.4	46.7
22	20	Intact US Insurance Grp	123.9	144.6	16.7	2.0	87.4	12.6	32.9	18.6	39.1	57.6
		Top 5*	2,378.3	2,286.4	-3.9	31.6	68.7	31.3	54.9	43.5	28.4	71.9
		Top 10*	3,500.2	3,655.2	4.4	50.5	71.1	28.9	53.3	46.4	26.9	73.2
		Top 20*	5,376.2	5,482.4	2.0	75.7	68.6	31.4	47.4	42.2	28.6	70.7
		Total Standalone	5,090.8	4,986.5	-2.0	68.8			43.1	44.3	28.8	73.1
		Total Package	2,146.0	2,257.4	5.2	31.2			47.9	35.5	36.3	71.8
		Total P/C Industry	7,236.7	7,243.9	0.1	100.0	68.8	31.2	44.6	41.6	31.1	72.7

Ranked by 2023 total standalone and packaged cybersecurity direct premiums written (based on premium reported as of June, 10 2024).

At first glance, the numbers appear encouraging, but a deeper analysis of the NAIC data uncovers some significant discrepancies in loss reporting:

- Package cyber policy losses require reporting on a loss payment and case reserve basis. However, loss development in the cyber line after the close of an accident year can add 50% or more in additional losses on top of the initial payments and case reserves in that year. As a result, the reported 35.5% "loss ratio" for the 2023 is likely understated and could be over 50% on an ultimate loss basis. Stand-alone cyber requires loss reporting on an "incurred loss" basis but it's unclear whether insurers interpret that as estimated ultimate loss, incurred but not reported (IBNR) losses, or just paid loss and case reserves, as seen with package cyber policies.

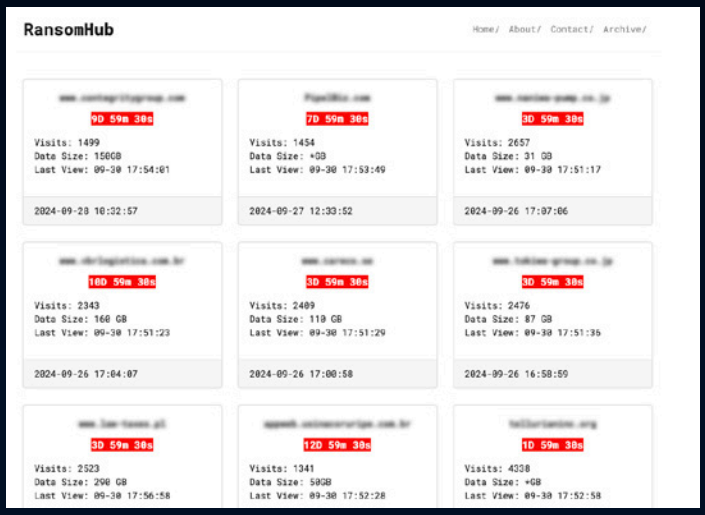
- One insurer reported zero losses on both its stand-alone and package cyber policies in 2023 and another reported just 4.3% loss ratio. These two insurers alone account for $430 million of written premiums, representing 6% of total premiums reported to the NAIC in 2023.

In addition to the challenges in statutory loss reporting for the cyber line, there are several reasons why some insurers may have a reserving lag following the 2023 year. Prior to the surge in ransomware attacks that began in 2019, cyber insurance was considered a medium tail line in terms of loss development. The primary loss drivers were data breaches and privacy litigation which typically take 2-3 years, or longer, to fully develop. The shift to ransomware as the main driver of loss in 2019 significantly altered the landscape of cyber insurance, transforming it to a shorter tail line of business. This was largely due to the fact that 85% of organizations paid the extortion demands which meant that losses matured very quickly, and the bulk of claims centered around the extortion payment itself. Over the past couple of years fewer organizations have opted to pay extortion demands and as a result incidents now much more frequently involve business income loss. Additionally, cybercriminals have turned to double extortion tactics (encryption and data theft) to increase their leverage. With most cyber extortion attacks involving data exfiltration, the complexity and scope of these events have driven cyber loss maturation back to a medium tail timeline, reflecting the extended periods required to fully resolve claims. The recent wave of privacy litigation involving website tracking tools has only added to that shift in loss development trends.

While the current NAIC data may not fully capture this reality, the 2023 cyber market's loss performance is expected to develop significantly worse than that of 2022. The spike in extortion incident activity observed particularly in the second half of 2023 is another strong indication of the potential reserving lag.

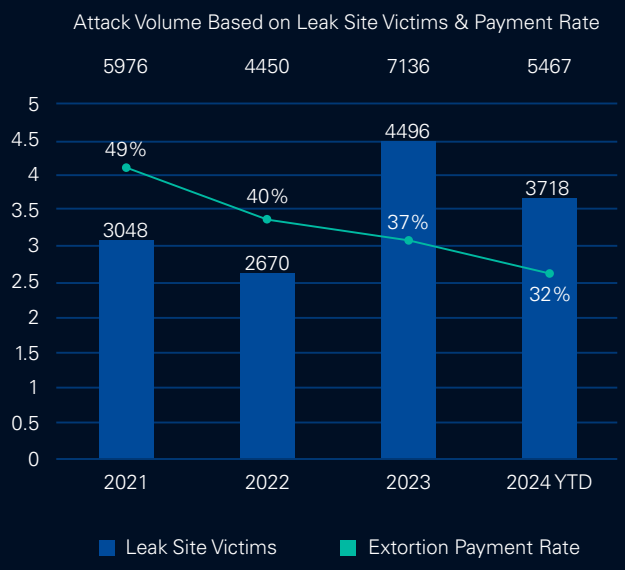
2023 Extortion Activity Likely Reached All-Time High

Since the change to double extortion tactics starting in the second half of 2020, leak sites have become a strong indicator of extortion activity levels. More than 90% of cyber extortion attacks involve data exfiltration either in combination with ransomware or in isolation. When extortion victims refuse to pay, the organization's name is leaked on what's commonly known as the "wall of shame".



TOR site of RansomHub group

Figure 4: 2022-2023 US Domestic Cyber Insurance Market Premium and Loss



Extortion payment rates have dropped steadily from a high of 85% at the beginning of the ransomware wave in 2019 to a record low of 32% in 2024. That's likely a result of improved backup resilience and victim organizations having better awareness of the pros and cons of paying extortion.

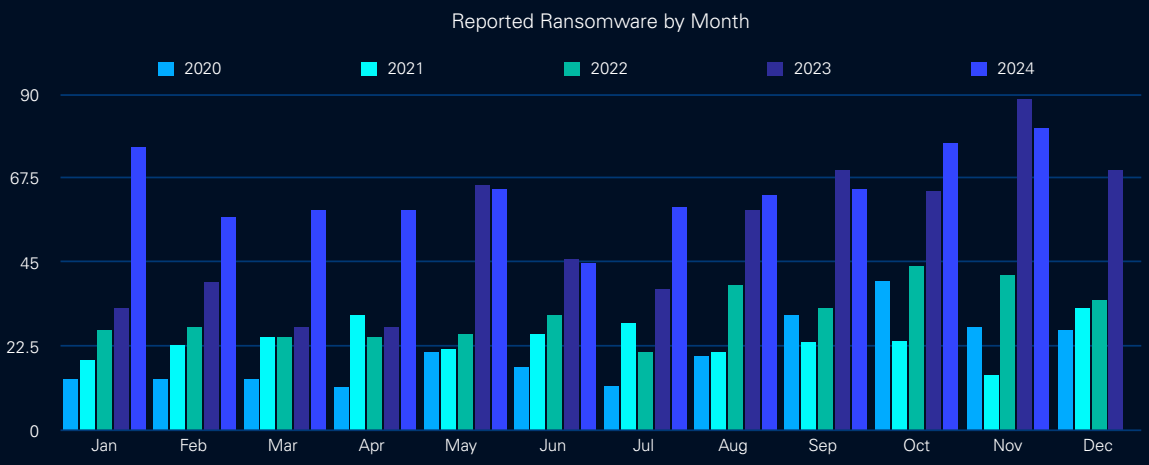
Extortion payment rates tracked by incident response firms and insurers can therefore be used to estimate changes in extortion activity by comparing those figures to the volume of organizations on leak sites[3]. The data shows that cyber extortion levels likely reached an all-time high in 2023 following the 2022 lull caused by the onset of the war in Ukraine and government actions against leading ransomware groups. This is further supported by the increase in total annual extortion payments from $567 million in 2022 to $1.1 billion in 2023[4] and a corresponding increase in publicly reported extortion incidents (Source: BlackFog).

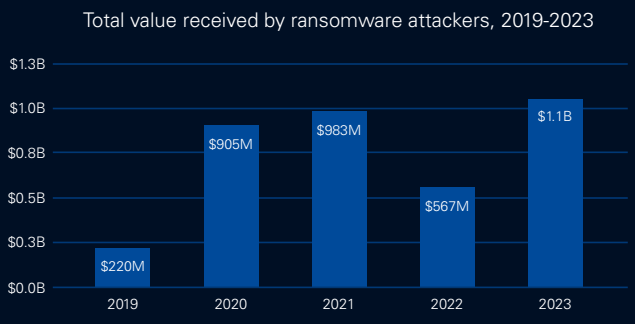
Figure 4 Source: "Coveware: Ransomware Recovery First Responders." Coveware: Ransomware Recovery First Responders, 30 July 2024, www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024. Accessed Sept. 2024.

[3]TOR site of RansomHub group

[4]Chainalysis Team. "Ransomware Hit $1 Billion in 2023." Chainalysis, 7 Feb. 2024, www.chainalysis.com/blog/ransomware-2024/.

Figure 5: Reported Ransomware Attacks 2020-2024





In addition to the overall increase in extortion incidents, last year saw some of the most unprecedented extortion attacks to date which included large corporate victims such as MGM Resorts, Caesars Palace, Clorox and Johnson Controls. Based on SEC filings, several of these attacks are likely to have resulted in losses in the nine-figure range.

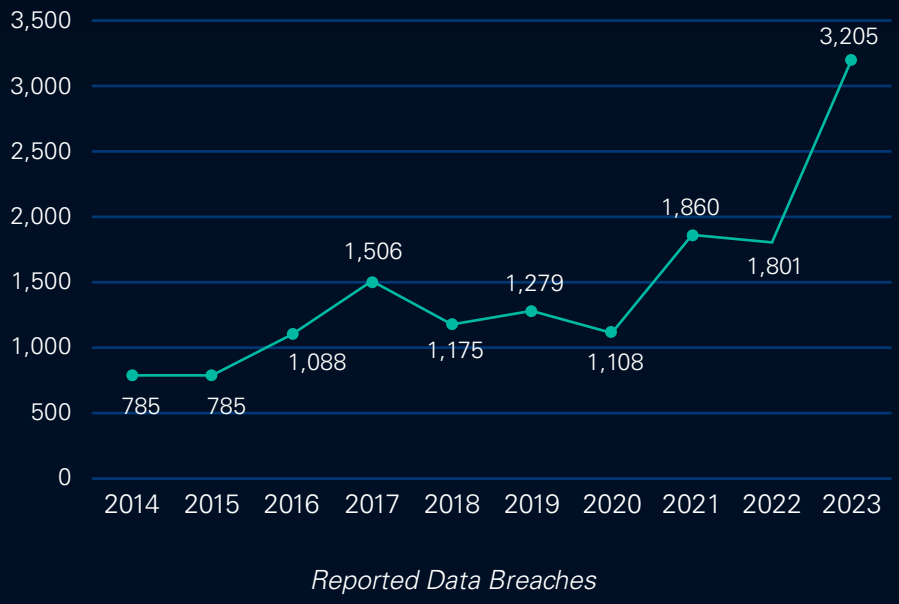
2024 has so far not seen any reduction in extortion activity and the most sophisticated ransomware groups seem to have now turned their attention to single points of failure with their attacks impacting not only the immediate target but also hundreds or thousands of their customers. This tactic is yet another change in strategy to apply additional pressure on organizations to pay up and, so far, it seems to be working. Both Change Healthcare and CDK Global paid very large ransoms following attacks in February and June ("Widespread Events").

Figure 5 Source: Reprinted from Chainalysis Team. "Ransomware Hit $1 Billion in 2023." Chainalysis, 7 Feb. 2024, www.chainalysis.com/blog/ransomware-2024/.

The Impact of Extortion on Reported Data Breaches

With the increase in extortion activity the number of reported data breaches has skyrocketed. 2023 saw the highest number of data breaches since reporting began: 3,205 - a 78% increase over 2022.

Figure 6: Reported Ransomware Attacks 2020-2024



Source: Identity Theft Resource Center. 2023 Data Breach Report. ID Theft Resource Center , Jan. 2024, p. 25, www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf. Accessed Sept. 2024.

About three quarters of the data breaches reported in 2023 were associated with cyberattacks with the rest resulting from system failures or human error. Although nearly every extortion attack now involves some level of data exfiltration, not all are reported as data breaches and there are several reasons why. Stolen data may not contain personally identifiable information, but sensitive corporate information instead. In other cases, the victim of an extortion incident is potentially unaware of the notification requirement or may assume that an extortion payment ensures that stolen data is forever suppressed, which is never guaranteed. Similar to extortion activity levels, data breach incidents have continued at the same high pace in the first half of 2024 with 1,571 reported incidents compared to 1,393 for the same period in 2023[5].

[5] *Identity Theft Resource Center. 2023 Data Breach Report. ID Theft Resource Center , Jan. 2024, p. 25, www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf. Accessed Sept. 2024.*

Shift in Initial Access Techniques

Ransomware groups continue to evolve their tactics. Initial access techniques used for cyber extortion attacks can still largely be grouped into phishing, remote code execution vulnerabilities and remote access exposure but 2023 saw a major shift to VPN compromise, a trend that's become even more apparent in 2024.

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. That intelligence effort is further augmented with forensic data collected from our Incident Response team.

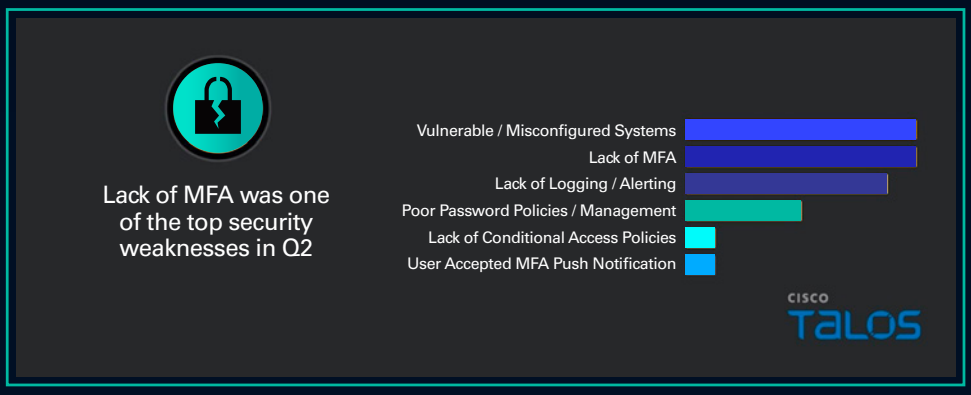
As vulnerability exploitation has decreased considerably, VPN exploitation via brute-forcing and valid credentials has become a leading attack vector for multiple ransomware affiliates[6] and perhaps the reason why extortion attacks remain at a high level. Prominent ransomware groups like Akira, have relied heavily on brute-forcing Cisco ASAs to gain initial access to their victims' networks. Although VPN is a necessary security solution for enterprise networks, when not properly managed, it can represent an exposure as severe as an internet-facing RDP (Remote Desktop Protocol) connection. This increased interest by threat-actors has also recently expanded to brute-forcing tools that include multiple SSL VPN providers, as well as other remote access solutions, including RD Web.[7]

This development highlights the importance of continuous auditing and management of VPN and other forms of remote access to corporate networks, as the lack of basic security controls, most notably MFA (Multi-Factor Authentication) has once again become a widespread factor in ransomware exploitation. The issue is not isolated to small organizations with several of the most high-profile and costly attacks of 2023 and 2024 involving VPN compromise and lack of MFA. VPN servers require thorough monitoring, patching and auditing. Customers with limited staffing and technical resources should consider a managed cloud solution, and ensure MFA is enabled on all accounts. This would decrease the risk of VPN compromise due to inconsistent patching or lack of brute-forcing prevention. If a managed solution is not possible, regularly audit VPN security groups to ensure access is provisioned only to accounts requiring VPN access, including local users on the VPN appliance. They should ensure default accounts are disabled, and default passwords are reset. Additional steps that would diminish the

[6] "Ransomware Tracker: The Latest Figures [March 2023]." Therecord.media, therecord.media/ransomware-tracker-the-latest-figures.
[7] "Large-Scale Brute-Force Activity Targeting VPNs, SSH Services with Commonly Used Login Credentials." Cisco Talos Blog, 16 Apr. 2024, blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/.

risk of a successful VPN brute-forcing attack include denying IP connection and authentication from anonymizing software like TOR (The Onion Router), and unauthorized VPN services and proxies. It is also critical to enforce password complexity and lockout policies, to prevent repeated brute-forcing attempts from succeeding. Implement "Impossible Travel" rules to deny consecutive login attempts to the same account from different IP ranges. Geolocation blocking alone is not effective. Ransomware operators easily circumvent this mitigation by using US-based proxies and VPN services.

Figure 7: Leading Security Weaknesses



Source: https://blog.talosintelligence.com/ir-trends-ransomware-on-the-rise-q2-2024/

Although wide scale weaponization of vulnerabilities as a method of initial access has declined, easily accessible Proof of Concept (PoCs) exploits have contributed to a sustained frequency of critical vulnerability exploitation for specific enterprise products. Widely available across GitHub and other repositories, PoCs of critical vulnerabilities affecting ConnectWise ScreenConnect, Cisco ASA and Citrix NetScaler saw persistent weaponization by multiple ransomware groups.

February was specifically marked by wide-scale exploitation of CVE-2024-1708, a path traversal vulnerability, and CVE-2024-1709, a critical authentication bypass vulnerability, both affecting ConnectWise ScreenConnect, a well-known remote access software solution. As a Remote Management and Monitoring solution (RMM), ScreenConnect is of strong interest to remote attackers. This became evident as working PoCs were shared after the vulnerabilities were announced, which was immediately followed by exploitation by multiple high-profile groups, including Black Basta and LockBit[8].

Dubbed "CitrixBleed", CVE-2023-4966, a sensitive information disclosure vulnerability affecting NetScaler ADC and Gateway, continued to be exploited this year. It can allow a remote, unauthenticated attacker to obtain session tokens from memory, and hijack existing authenticated sessions, bypassing multi-factor authentication, validating continued threat actors' interest. With thousands of vulnerable instances still detected worldwide, exploitation is expected to continue.

Cisco VPN vulnerabilities also remain widely exploited, in particular, CVE-2020-3259, a critical information disclosure vulnerability affecting Cisco ASA and FTD appliances that could allow an attacker to retrieve memory content from the Cisco device, including cleartext usernames and passwords. Another prevalent Cisco vulnerability, CVE-2023-20269, affects the separation of authentication, authorization, and accounting (AAA). Prior to its release as CVE-2023-20269, Akira was targeting corporate networks by simply exploiting this flaw via a publicly available Metasploit module published in 2022[9].

[8] "Threat Actor Groups, Including Black Basta, Are Exploiting Recent ScreenConnect Vulnerabilities." Trend Micro, 27 Feb. 2024, www.trendmicro.com/en_us/research/24/b/threat-actor-groups-including-black-basta-are-exploiting-recent-.html. Accessed Aug 2024.
[9] "Cisco ASA Clientless SSL VPN (WebVPN) Brute-Force Login Utility." Rapid7, 2024, www.rapid7.com/db/modules/auxiliary/scanner/http/cisco_asa_clientless_vpn/. Accessed Sept. 2024.

New Normal in Widespread Events

In 2023, the cyber landscape experienced a resurgence of widespread incidents, with several attacks exploiting vulnerabilities in widely used software products across various industry sectors. These high-profile breaches underscored the pervasive risks facing organizations reliant on critical digital infrastructure. For example, Cl0p's exploitation of a remote code execution vulnerability (CVE-2023-34362) in the MOVEit file sharing service impacted more than 2,700 organizations in multiple industries (Source: https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/). So far, this year's most prevalent widespread events have been the result of successful targeting of third-party software providers specific to the auto and healthcare industry. Moreover, three major events in the first seven months of this year- including one that seems to have caught catastrophe models off guard- marks a significant increase in widespread event activity compared to the past several years.

Change Healthcare

On Feb 21, 2024, Change Healthcare was the victim of a ransomware attack. Owned by UnitedHealth Group, the company provides billing services, prescription and insurance claims processing. As Change Healthcare provides services to 94% of US Hospitals, the attack resulted in interruptions in claims and prescription processing across the entire United States[10]. It was later revealed that 4 Terabytes of data were exfiltrated from the company's networks, possibly exposing the confidential data of 1 in 3 Americans.

It was revealed by the attacker that they had gained access to Change Healthcare's networks through the use of Citrix Remote Access portal credentials they discovered in an InfoStealer log. Since MFA was not enforced on that account, the attackers were simply able to bypass security controls through valid credentials, and gain access to internal resources within the network[11]. The attackers then moved laterally throughout the Change Healthcare networks, exfiltrating data and deploying encryption. As a preventative measure, services were shut down, to prevent encryption from spreading to the broader UnitedHealth Group networks[12]. And while Change Healthcare opted to pay $22 million to the ransomware group

[10]"Latest Alerts and Advisories | NJCCIC." Nj.gov, 2024, www.cyber.nj.gov/Home/Components/News/News/1299/214. Accessed 11 Oct. 2024.
[11]"Change Healthcare Hacked Using Stolen Citrix Account with No MFA." BleepingComputer, www.bleepingcomputer.com/news/security/change-healthcare-hacked-using-stolen-citrix-account-with-no-mfa/.
[12]Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack" May 1, 2024, Transcript of Proceedings, pp. 1-10, 2024 https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf

behind the attack to ensure exfiltrated data was deleted, the group (BlackCat) refused to pay the ransomware operator in possession of the data, who in turn decided to capitalize on the attack through another group, RansomHub[13]. RansomHub, demanded an additional ransom payment for data deletion. UnitedHealth Group estimated the event could reach a total monetary cost of over $2.3 billion.[14]

CDK Global, Inc.

On June 19, 2024, CDK Global experienced a ransomware attack at the hands of BlackSuit. As one of the largest Software-as-a-Service (SaaS) providers for the automobile dealership industry, CDK's software products streamline purchasing, leasing, and marketing for thousands of dealerships in the US and Canada.[15] As a result of the attack, and the vendor's critical role in daily operations, thousands of dealerships were forced to severely diminish their productivity.

Immediately after detecting the attack, the company shut down systems to limit the scope of the compromise, and attempted to restore services, but shortly after, they were forced to take systems offline again. Additional cause of concern was the use of an always-on-VPN connection associated with CDK's DMS (Dealer Management System) services, as these connections into customers' networks could have further exposed them during the compromise[16]. The company was forced to pay a $25 million ransom to BlackSuit for data deletion and decryption[17].

CrowdStrike

On Friday, July 19th 2024, CrowdStrike released an automatic update for its Falcon Sensor software as normally scheduled. However, this update contained code that conflicted with the normal operating procedure of the Microsoft Windows operating system. The result was 8.5 million Windows devices, both physical and in the cloud, unable to reboot, rendering them unusable. The nature of the issue left system administrators to manually remediate the issue on each individual machine, after CrowdStrike had created a fix for the release[18]. Due to the widespread nature of the issue and business urgency to return to a working state, this event was capitalized on by malicious actors. Social engineering attacks were launched to distribute malware via fake updates and remediation support services[19].

The outage caused by the CrowdStrike Falcon update resulted in roughly $5.4 billion in damages to Fortune 500 companies, and widespread outages in multiple industries, including over 46,000 flight delays and 5,171 flight cancellations.[20] Although the CrowdStrike outage was not the result of an attack, this event is a reminder of the catastrophic consequences that can result from a widespread non-malicious attack across multiple industry verticals.

[13]"Latest Alerts and Advisories | NJCCIC." Nj.gov, 2024, www.cyber.nj.gov/Home/Components/News/News/1299/214.
[14]Alder, Steve. "UHG: Substantial Proportion of US Population May Be Affected by Change Healthcare Cyberattack." HIPAA Journal, 23 Apr. 2024, www.hipaajournal.com/change-healthcare-responding-to-cyberattack/.
[15]"CDK Global." Cdkglobal.com, 2024, www.cdkglobal.com/fixed-ops/service/cdk-service. Accessed Sept. 2024.
[16]"CDK Global Outage: Everything You Need to Know." Sangfor Technologies, 2024, www.sangfor.com/blog/cybersecurity/cdk-global-outage-everything-you-need-know. Accessed Sept. 2024.
[17]"Ransomware Summer: Attacks Heated Up, but so Has the Global Response | TRM Insights." Trmlabs.com, 2024, www.trmlabs.com/post/ransomware-summer-attacks-heated-up-but-so-has-the-global-response. Accessed Sept. 2024.
[18]Djajapranata, Cliff. "CrowdStrike, Microsoft Outage: Is Tech Too Vulnerable?" Georgetown University, 25 July 2024, www.georgetown.edu/news/ask-a-professor-crowdstrike-outage/.
[19]Counter Adversary Operations. "Threat Actor Uses Fake Recovery Manual to Deliver Unidentified Stealer." Crowdstrike.com,
[20]Whitmore, Geoff. "The CrowdStrike Outage Is Still Impacting Airlines." Forbes, 22 July 2024, www.forbes.com/sites/geoffwhitmore/2024/07/22/the-crowdstrike-outage-is-still-impacting-airlines/.

The Outlook

As we look to 2025 it's worth revisiting some of the predictions in our 2023 report to see what we didn't get right. We estimated that growth in the US cyber insurance market would slow to 20-25% and that turned out to be too optimistic when in reality the market ended the year at just 1.6%. Another prediction that didn't come true was systemic risk concerns potentially leading to coverage restrictions in the wake of the MOVEit attack. In the end, the attack didn't have sufficient impact on cyber market loss performance to lead to any changes. We've since had three major widespread events and yet it doesn't seem like these events will lead to changes in market behaviors or coverage structures in the short term, if at all.

It's now clear that 2022 was an anomalous ransomware year and what we've seen in all other years since 2019 should be considered the norm in cyber extortion. On top of that, the market may have to contend with an average of three to four mini-CAT events per year in addition to the potential 50-year, 100-year and 200-year catastrophic events that some insurers are already pricing into their portfolios.

As the U.S. cyber insurance market enters a pivotal phase, it is clear that this is not just a period of stabilization but a moment requiring strategic adaptation and innovation. While hard market growth was fueled by rapid premium increases, the softening market of 2023-2024 signals that pricing alone can no longer drive expansion. The future will depend on attracting new policyholders, portfolio diversification and working even more closely with policyholders to address increasingly sophisticated cyber threats.

The long-term success of the cyber insurance market hinges on its ability to balance profitability with robust risk management, adapt to regulatory changes, and create a greater cybersecurity investment. In an increasingly volatile landscape, only insurers who innovate and embrace a dynamic approach to risk will thrive. The question is whether the industry can seize the opportunity or be blindsided by the very threats it seeks to mitigate.

TOKIO MARINE HCC

2024

Cyber Market 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.

Follow us on LinkedIn: #TMHCC_Cyber