2024 Q2

Cyber Market Update

Steve Robinson
National Cyber Practice Leader

"The clicks are getting slower."

That's what a senior VP in our Executive Lines Cyber practice said while we were discussing changes occurring in our industry. He didn't mean the clicks on a website — he meant the clicks the car on a roller coaster makes as it approaches the top of the hill. The clicks get slower, and then the view changes quickly as the car reaches the crest and begins its fast descent. It's a perfect way to describe where we are in this constantly evolving cyber insurance marketplace.

The past 18 months or so have seen the market completely flip from the pre-2023 days of significant rate increases, strict underwriting, capacity tightening, and coverage restrictions in the wake of significant losses, largely tied to the ransomware epidemic. From there, we witnessed a full-scale assault on common sense in the complete un-doing of many of the levers insurers pulled to ensure profitability in this growing coverage area.

Loss frequency in 2022 dropped significantly due to, among other things, the splintering and re-focusing of threat actor groups involved in the Russia/Ukraine conflict; increased governmental, law enforcement, and media focus on the perpetrators; and insurers' improved cybersecurity requirements for businesses to qualify for Cyber insurance coverage.

In reaction to these improved results, carriers reduced rates significantly, and some lowered the barriers to entry for coverage and began to again entertain classes of business once in their no-fly zone. We've covered this extensively in previous Cyber insurance market updates.

Today, however, the clicks are getting slower. Change awaits us on the other side of the hill. The only question is when and how drastic it will be.

HEADLINE-GRABBING CYBER EVENTS

On February 21, 2024, Change Healthcare — a healthcare technology company that processes as much as 50% of US medical claims — fell victim to a ransomware attack, causing significant disruption to hospitals and healthcare practices throughout the country. The enormous operational, financial, and reputational effects of the attack are still being felt and will continue for months to come.

This wide-scale event reminds us that despite a temporary slowdown in activity in 2022, ransomware attacks continue to be highly lucrative crimes. Groups like LockBit, Medusa, ALPHV/BlackCat, Black Basta, and others continue to evolve and grow and have led the list of active threat actor groups that have perpetrated publicized attacks so far in 2024.

As if we needed a reminder that data breaches aren't a thing of the past, AT&T disclosed last month that the personal information of 73 million current and former customers was stolen and shared on the dark web — including Social Security numbers, passwords, full names, email addresses and street addresses, phone numbers, dates of birth, and account numbers.

An artificial intelligence (AI)-assisted cybercrime that recently garnered significant media attention involved an AI heist at a multinational firm in Hong Kong.[1] In this made-for-Hollywood scenario, a finance worker was tricked into paying out $25.6 million to fraudsters who used deepfake technology to pose as the company's CFO in a video conference call. The worker attended the call with what he thought were several other members of staff, only to later find that all were deepfake recreations.

In the Cyber insurance and financial risk management world, we authenticate wire transfer requests by executing callbacks or verifying the authenticity of the request by a means other than the original mode received. In this instance, it's easy to see how that step was deemed unnecessary, as the victim thought he was receiving real-time instructions from a known person he could see in real time. The rules of the game are changing.

REGULATORY DEVELOPMENTS IN THE CYBER WORLD

As cyber threats continue to grow and cause economic and social disruption throughout the world, government intervention and information sharing increasingly become part of the conversation. Because cyber insurance policies generally provide coverage for regulatory liability — and, in most cases, fines and penalties associated with covered cyber incidents — it's important to stay abreast of the latest developments in this environment. Here's a summary of some of the more recent trends.

California

Civil and administrative enforcement of the California Privacy Rights Act (CPRA) went into effect in 2023 as an extension of the CCPA, introduced in 2018. CPRA offers enhanced privacy protections for consumers by expanding their rights regarding personal information and imposing obligations on businesses.

Connecticut

Passed in 2022, the Connecticut Data Privacy Act (CTDPA) went into effect on July 1, 2023. The law expands personal data privacy, establishes business obligations, and penalties for non-compliance.

Kentucky

The Kentucky legislature passed a comprehensive data privacy bill, H.B. 15, that was delivered to the governor for signature. While not effective until 2026, if enacted, the bill will outline requirements and protections relative to consumer privacy and the technical and security practice requirements of businesses in the state.

Maryland

The Maryland Legislature passed the Maryland Online Data Privacy Act of 2024 (MODPA) on April 6, 2024.[2] The new legislation will make Maryland the first state "to pass a Washington Privacy Act variant that contains unique provisions regarding data minimization, sensitive data, minors' data privacy, and unlawful discrimination, among other provisions."

Utah

The Utah Consumer Privacy Act (UCPA) took effect on December 31, 2023.[3] The new law establishes parameters for businesses in protecting personal data and provides consumers with information about how they can exercise their rights.

Virginia

The Virginia Consumer Data Protection Act (VCDPA) grants consumers certain rights over their personal data and imposes obligations on businesses. The law went into effect in 2023.

Federal

After discussions and failed attempts at enacting federal privacy laws, a new bipartisan bill designed to preempt state privacy laws and "sets clear, national data privacy rights and protections for Americans, eliminates the existing patchwork of state comprehensive data privacy laws, and establishes robust enforcement mechanisms to hold violators accountable, including a private right of action for individuals," has been introduced.[4]

DEVELOPING THREATS IN THE CYBER WORLD

Cyber insurance is unique from any other property and casualty product in that constant evolution is required because the perils insured against are themselves constantly evolving. Wind is wind. Water is water. Fire is fire. But today's cyber isn't tomorrow's cyber. Here's an overview of several developing threats that will continue to impact insureds and, in turn, Cyber insurance coverage.

Advanced Persistent Threats

While not a new attack vector in and of itself, advanced persistent threats (APTs) are developing and adapting for increased effectiveness, largely aided by advances in AI, which we discuss later in this report. APTs are "a type of cyber threat characterized by their sophisticated, sustained, and covert nature. They are typically orchestrated by highly skilled adversaries, often state-sponsored or part of well-funded criminal organizations."[5]

Kapersky researchers predict APT actors will introduce new exploits on "mobile, wearables, and smart devices and use them to form botnets, as well as refine supply chain attack methods and utilize AI for more effective spear phishing."[6] These advancements are anticipated to intensify politically motivated attacks and cybercrime.

MFA Bypass Attacks

Since 2018, when multi-factor authentication (MFA) became one of the more well-known initialisms among Cyber insurance brokers and underwriters, cybercriminals have been developing ways to circumvent this security feature that was designed to ensure the right people can remotely access data that they're allowed to view. Here are a few examples:

- **MFA fatigue** — When threat actors manipulate users into giving access to their accounts unwittingly through repeated access requests. The user eventually tires of the constant requests and accepts, enabling the criminal's remote access.
- **Machine-in-the-middle attacks** — When attackers intercept communication between the user and the system that's authenticating access, capturing an MFA code or token in the process.
- **Token theft** — When cybercriminals steal MFA tokens generated by devices that have previously been authenticated/trusted. Phishing attacks and malware injection are methods by which this theft can be achieved.

Exploitation of IoT Vulnerabilities

As household devices, appliances, and entertainment systems are increasingly connected to the internet, the windows that cybercriminals look to climb through to access personal or corporate data or networks become more numerous and vulnerable. If manufacturers haven't taken the proper care to include cybersecurity in the development of these connected Internet of Things (IoT) devices, consumer and commercial information is increasingly at risk.

This threat goes beyond mere household devices and extends to modes of transportation (smart vehicles), leading to not only increased threats of data loss but also extending to physical threats such as bodily injury, property damage, and even loss of life.

There are concerns in the healthcare and utilities sectors where the exploitation of connected medical devices or supervisory control and data acquisition (SCADA) systems could lead to catastrophic loss.

Ransomware

Again, not a new threat here, but one that is constantly evolving. As ransomware variants continue to develop, threats of double and triple extortion involving threats to exfiltrate data, execute distributed denial of service (DDoS) attacks and contact customers directly present new dilemmas.

The early days of ransomware, where strong backup protections often insulated businesses from having to pay ransoms in exchange for decryption keys, have given way to more complex decision-making analyses when getting access to data is no longer the only problem.

AI's Influence on Cybercrime

Move over MFA; AI has surpassed you as the most used initialism in today's Cyber insurance lexicon. While still in its relative infancy, the meteoric rise of the impact of AI on problem solving — for good and for evil — cannot be overstated.

- The use of AI to analyze and adapt attack methods will enhance the efficacy of these attacks, providing a significant advantage to cybercriminals.
- AI will be an important tool in the criminal's arsenal to develop and more rapidly deploy malware, providing capabilities infinitely more effective than human programmers could develop.
- The use of AI to overcome language barriers and better inform cultural queues will facilitate more effective social engineering scams.

AI's involvement in various stages of cybercrime will show itself in many ways. Here are a few:

Data poisoning. This cybercrime involves introducing malicious behavior by manipulating training data for AI models. Attackers can inject poisoned data during model training, allowing them to compromise the model's performance or cause it to make incorrect or biased decisions that could benefit their cause.

SEO poisoning. Attackers target search engine results by manipulating content to appear legitimate while actually leading users to malicious websites. AI-driven techniques can enhance the effectiveness of search engine optimization (SEO) poisoning, making it harder to detect.

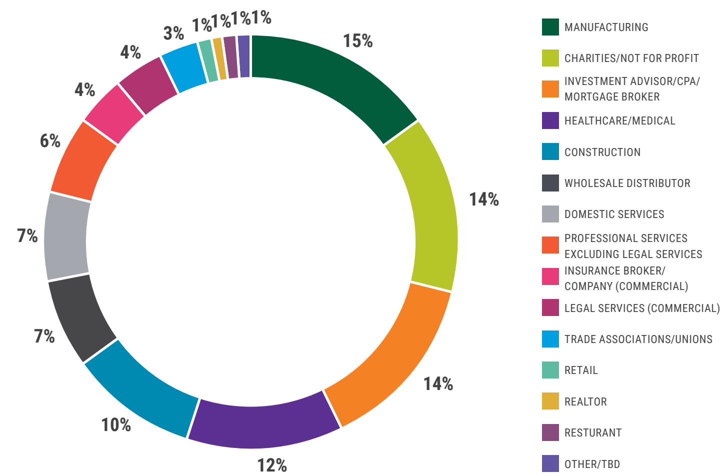
Election interference. As we embark on another election year, we can expect that those who wish to profit from political interference will employ advanced AI tactics to exert influence in new and creative ways. Among them:

- **Deepfake** — Altered or newly generated videos falsely depicting political figures in compromising positions or saying controversial things, all designed to influence voters in ways to benefit the threat actor's cause (or those who are paying them).
- **Text-to-speech** — We've all received voicemails from candidates that we didn't ask for. Think: voice-message generation targets a voting population with manipulated messages.
- **Text-to-image (AI-altered images)** — Similar to Deepfake, but in a static image context, typically leveraging social media to promote an alternative agenda. While easier to identify using AI-enabled tools, these campaigns could achieve their desired outcome for receptive audiences or those looking through a less skeptical lens.
- **DDoS** — Use of AI to automate DDoS against campaign-related websites, which could affect fundraising capabilities and efforts to get out the vote.

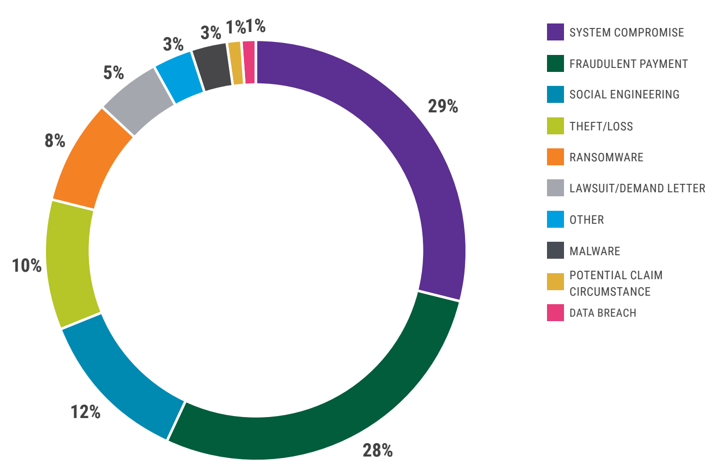
CYBER CLAIMS UPDATE

As a leader in Cyber insurance for the SME sector, the RPS Cyber practice has vast amounts of claims data that provide a real-time glimpse into incident types and industries affected. We curate this data to specifically exclude public entity losses, as they are not considered "SME," and many carriers still exclude cities, counties, public schools, and other public agencies from coverage. That said, below are some trends we witnessed in Q1 2024 in RPS's proprietary claims data for small- to medium-sized enterprises (SMEs).

YTD CYBER REPORTED INCIDENTS BY INDUSTRY SECTOR



YTD CYBER REPORTED INCIDENTS BY MATTER TYPE



CYBER-INSURER DYNAMICS

Against the backdrop of increasing claims frequency, new attack vectors, high-profile systemic vendor breaches, regulatory positioning, and a hyper-charged domestic and geopolitical environment, we continue to anticipate changes ahead in the Cyber insurance marketplace, which we discussed in detail in our RPS 2024 US Cyber Market Outlook.

However, as the clicks on the tracks slow down, we've yet to see consistent changes from many of our insurer partners that are reflective of what we're seeing at the top of the hill. From a pricing perspective, there continue to be vast inconsistencies among the carriers and managing general agents (MGAs) that offer standalone Cyber insurance policies.

In a marketing exercise, it isn't unusual to see outliers with a 60% disparity in rate on the same risk. While the dramatic dips in renewal premiums have eased a bit from 2023 pricing, we haven't yet witnessed the correction we expect in 2024. But there are signs. For instance, one prominent cyber insurer recently announced across-the-board 10–15% rate increases and increases of 35% across the healthcare sector specifically, in reaction to the Change Healthcare incident.

With respect to appetite, classes once completely out of favor, such as public entity and public k-12 education, have again attracted interest from a handful of players, both domestically and in the London markets. The firmer market pricing during 2019–2022 was accompanied by the requirement of drastically higher retentions for middle-market and risk-management-sized accounts. Generally, we've seen those remain consistent even in a down pricing cycle, making some of these more loss-exposed classes a bit more tolerable for insurers looking to grow their top line.

As the markets navigate the balance of top-line growth and bottom-line profitability, we've seen a void in coverage creativity that was a hallmark of the Cyber insurance market's pre-2021 days. Today, the most comprehensive coverage doesn't always win out if there are significant pricing disparities, especially if the lowest price provides full limits for cyber extortion.

Perhaps nowhere is this trend more acutely observed than in aggregator platforms that line up as many as 15 different markets, churning out quotes from a single application. While enormously efficient and highly effective for those with expertise in this coverage area, in the wrong hands, these tools can become digital beauty pageants, rewarding the contestant not with the best coverage or robust risk management offerings but the one with the lowest price. This disregard for coverage, we fear, could have significant repercussions for agents not well versed in Cyber insurance, or at least working closely with professionals like RPS's Cyber practice advising them.

ON THE OTHER SIDE OF THE HILL

In the months ahead, what do we predict from our carrier partners? Here are a few quick takes.

Enhanced Risk Management Offerings From Carriers

While MFA quickly became a required practice for remote access, access to email, cloud applications, backups, and even on-premises access for privileged users, we see similar expectations on the horizon for endpoint detection and response (EDR), managed detection and response (MDR), and extended detection and response (XDR) solutions that can not only detect but respond to threats in a proactive 24/7 nature. Increasingly, these tools will incorporate AI elements. More carriers will make available their own (or outsourced) solutions to fit hand in glove with their insurance offerings. Some will be for a fee, while others will be wrapped in the total offerings at no additional cost.

We also expect to see developments in social engineering prevention techniques and tools as wire fraud claims continue to escalate. There is a void in the market for this type of risk management. We expect to see this change, as carriers don't want to die of a thousand cuts from these sub-limited, yet frequent, losses.

Coverage Retraction

- As more widespread systemic events occur, we anticipate deeper underwriting of certain dependent business interruption coverage grants, and possibly even a return to sub-limits.
- As states increasingly mirror the biometric information protections that more closely mirror Illinois' Biometric Information Privacy Act, we expect that exclusions will continue in the areas of unlawful collection and use.
- As class action lawsuits mount in relation to various website tracking software tools, Cyber insurance policies will continue to add exclusions that contemplate this risk or implement effective underwriting tools to assess the risk.
- In an election cycle, we expect to see election fraud-related exclusions in some Cyber policy language specific to the public sector.

Pricing Adjustments

We continue to say that increasing claims frequency in the face of decreasing rates isn't a formula for long-term sustainability. As discussed, we're seeing signs of change, but perhaps not as quickly as formerly predicted. Nevertheless, this change in carrier strategy is inevitable.

A Change in Underwriting Appetite

This change is relative to specific industry sectors affected by widespread software exploits.

As cybercriminals increasingly favor single-point-of-failure attack methods, often involving widely published software solutions, the unique industries that these software programs serve will likely see scrutiny from cyber insurers (i.e., MOVEit's impact on public entities,[7] Change Healthcare's impact on physician practices, or Blackbaud's impact on nonprofits and education[8]). As previously discussed, we're already seeing this trend in healthcare over the past month. These widespread exploits will continue, as will the appetite and underwriting process surrounding those affected.

Consolidation of Insurtechs by Conventional Insurers

This one isn't going out on a limb, as we witnessed a prominent deal late in 2023.[9] Acquisitions like this will make sense for certain insurers at the right prices, leveraging the creative capabilities that many of these progressive operations bring.

Beyond increased market share, from advanced underwriting technologies to risk management offerings, we anticipate more deals on the horizon, and it will be interesting to see the impact they have on the developing Cyber insurance landscape.

PLEASE KEEP ARMS AND LEGS INSIDE THE CAR AT ALL TIMES

Those who choose to focus on Cyber insurance as a career likely know they're not in line for the teacup ride. This is a rollercoaster with twists and turns and, well, excitement. The clicks are indeed getting slower, and change is on the other side of the hill. After all, thrill-seekers wouldn't want it any other way.

The RPS Cyber practice stands ready to guide agents, brokers, and their customers, ensuring the ride is free of long lines, safe, enjoyable, and always ready for another spin around the track.

Sources

[1]Chen, Heather and Kathleen Magramo. "Finance Worker Pays Out $25 Million After Video Call With Deepfake 'Chief Financial Officer,'" *CNN.com*, 4 Feb. 2024.

[2]Stauss, David. "Maryland Legislature Passes Consumer Data Privacy Bill," *ByteBackLaw.com*, 8 April 2024.

[3]"Utah Consumer Privacy Act: A New Law To Protect Online Data," *Utah Office of the Attorney General*, 15 Feb. 2024.

[4]"Committee Chairs Rodgers, Cantwell Unveil Historic Draft Comprehensive Data Privacy Legislation," *House Committee on Energy and Commerce*, 7 April 2024.

[5]Hewitt, Nik. "Advanced Persistent Threats (APTs): 2024 Identification and Response Tactics," *SecurityBoulevard.com*, 8 Jan. 2024.

[6]CNW Group. "Kapersky Releases Predictions for Advanced Threats Landscape in 2024," *Yahoo! Finance*, 14 Nov. 2023.

[7]Newman, Lily Hay and Matt Burgess. "The Biggest Hack of 2023 Keeps Getting Bigger," *Wired*, 2 Oct. 2023.

[8]"SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors," *U.S. Securities and Exchange Commission*, 9 Mar. 2023.

[9]"Travelers To Acquire Corvus Insurance," *BusinessWire*, 3 Nov. 2023.

Related content cards

https://www.rpsins.com/learn/2024/jan/2024-us-cyber-market-outlook/

https://www.rpsins.com/learn/2024/feb/what-generative-ai-means-for-cyber-insurance/

https://www.rpsins.com/learn/2024/feb/why-is-cyber-insurance-pricing-so-volatile/