2024 Q3 Cyber Market Update

Steve Robinson
National Cyber Practice Leader

Since the beginning of the year, we've made several predictions about the future of the cyber insurance market. Those that have come to fruition include market consolidation (some have exited, and insurtechs have partnered with traditional insurers), the continuation of large-scale data breaches, the expansion of artificial intelligence (AI) in political interference, and the ever-expanding threat of systemic events moving horizontally through specific industry sectors and the public at large.

What we haven't correctly predicted is the timing of market pricing adjustments in response to events like these.

Despite mega data breaches, highly publicized ransomware attacks, and systemic software failures that we see through the windshield, pricing continues to trend with an eye toward the rearview mirror, as if a slowdown in ransomware activity in the small- to midsize enterprise (SME) sector were the only indicator of risk. Today's threat environment is stretching the current environment for coverage, pricing, and capacity, yet all three of these areas continue to remain favorable for buyers.

It's been a summer of "what could go wrong?" and still, our predictions of market pricing corrections have yet to fully come to fruition. We're seeing it in pockets — from some markets, in some industry sectors — but we're still working in a market with few restrictions on pricing or capacity.

Let's take a look at some of the events that have re-defined the cyber landscape in just a few short months.

LARGE DATA BREACHES HAVEN'T GONE AWAY

Data breaches are unfortunately becoming commonplace these days, and the first half of 2024 saw quite a few.

In April 2024, a large health plan reported a data breach affecting upwards of 13.4 million people to the US Department of Health and Human Services.[1] Unlike data breaches involving malicious hacking groups gaining unauthorized access to data, this event involved the health plan sharing confidential patient information with third-party advertisers, including Google, Microsoft, and X (formerly Twitter).

Also in spring 2024, a large sporting, concert, and events ticket company reported a significant breach of customer data from a cloud database hosted by a third-party data services provider.[2] The breach, allegedly perpetrated by a group called ShinyHunters, potentially affected millions of customers and has led to class action lawsuits. This same event also impacted more than 100 other companies across several industry sectors, including six months' worth of call and text message records from one of the largest telecom companies in the world, affecting more than 73 million customers.[3]

RANSOMWARE REMAINS A PERVASIVE AND COSTLY THREAT

Ransomware isn't just a flash-in-the-pan trend; it's the pest that won't go away.

In February 2024, a significant ransomware attack on one of the nation's largest health networks disrupted insurance claims processing nationwide, affecting patients, pharmacies that were unable to fill preauthorized prescriptions and clinics that couldn't provide medical treatments. Smaller healthcare providers and rural pharmacies faced significant revenue losses. At the time of this writing, we still have insureds who have yet to fully understand whether their patient data was accessed without authorization, as the health network sent broad notices to their customers months ago lacking important details that were still unknown.

In June, a ransomware attack on one of the leading software as a service (SaaS) providers to the automotive industry affected more than 10,000 car dealerships, affecting sales, service, parts financing, and customer relations. Many dealerships had to revert to alternative manual processes, while some were unable to sell cars at all during the outage. The event contributed significantly to a 2.6% to 7.2% decrease in new-vehicle sales for June 2024.[4] RPS has received more than 100 notices on this matter. These reported claims will take longer than a traditional data breach to materialize, as insureds work to quantify and prove their lost revenue and extra expenses incurred during the outage.

AS IF DATA BREACHES AND RANSOMWARE ATTACKS WEREN'T ENOUGH

Data breaches and ransomware aren't the only things cyber thieves are up to in 2024.

In July, one of the leading cybersecurity providers to Fortune 500 companies released a faulty update to its security software. This release caused system crashes affecting approximately 8.5 million Microsoft Windows systems worldwide, causing significant disruptions across various sectors, including airlines, banks, hospitals, and government services. The outage may have cost Fortune 500 companies as much as $5.4 billion in revenues and gross profit, not counting secondary losses that may be attributed to lost productivity or reputational damage.[5] The outage has been dubbed the most important cyber accumulation loss event since NotPetya.[6] In addition, the Cybersecurity and Infrastructure Security Agency (CISA) issued a report warning of malicious activities conducted by cyberthreat actors who are leveraging the outage to conduct phishing attempts.[7] We have seen phishing become a trend associated with other cybersecurity events as well.

A key differentiator in today's loss environment versus the past is the longer tail on loss development, due to massive third-party events whose final outcomes have yet to be determined. Again, we have insureds who know there was a data breach in the healthcare billings ransomware attack, but don't yet know if or how much their customer data was affected. Business interruption (BI) losses due to recent wide-scale ransomware attacks and software failures will be significant but will take time to develop.

Unlike similar events our insureds experienced themselves, third parties our insureds rely on are increasingly experiencing these events. This removes the control from our insureds' hands, as timelines lengthen when hundreds of thousands or even millions of businesses are in the same boat.

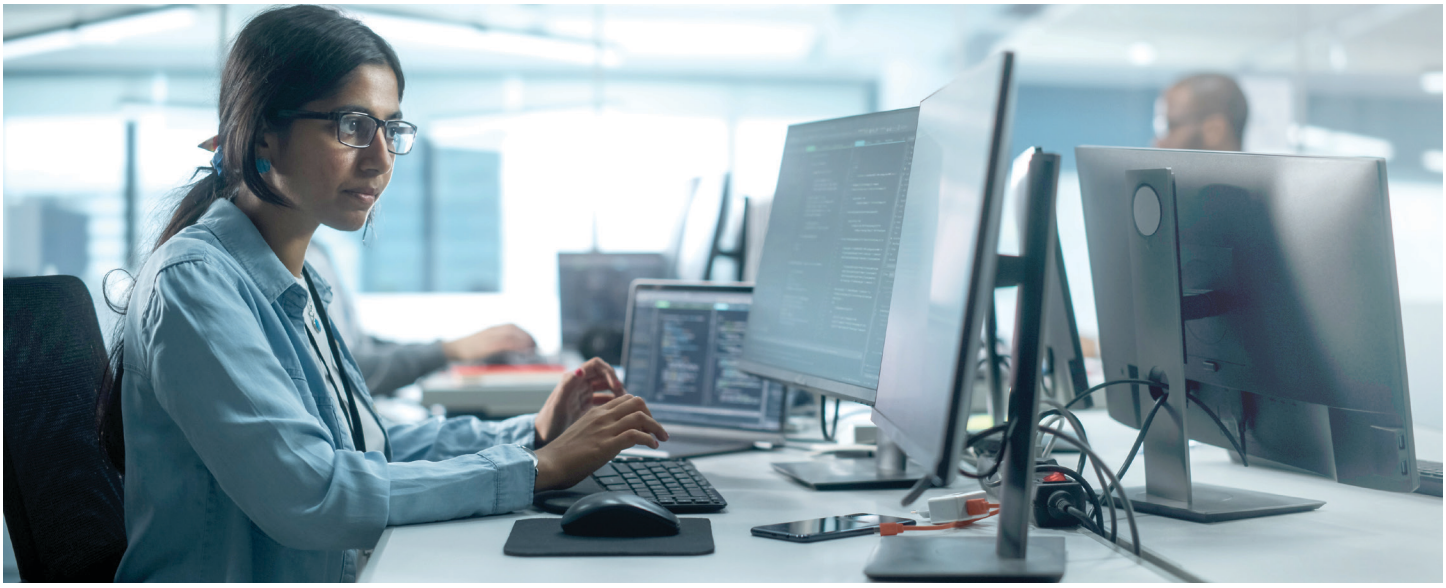
CLAIMS UPDATE

Funds transfer fraud/social engineering losses represent the highest frequency category SME insureds. That said, year-to-date frequency is trending a bit lower among our SME clients compared to the same time period in 2023. While not a major shift, this news is nonetheless encouraging, and is likely attributable to increased awareness among businesses, as well as employees training on transferring money and procedures for validating changes in payment instructions from clients and vendors.

Ransomware continues to be a threat to SMEs, but frequency of these reported events is down ever so slightly over the same time last year, although it isn't statistically relevant enough to call it a trend. Even so, a flat frequency curve is encouraging news, as attackers have increasingly focused on big-game hunting, and cybersecurity defenses for SMEs continue to improve. Also, businesses are far less likely to pay a ransom these days — a trend that has steadily dropped each year since 2019.[8] We've seen an increase in third-party privacy claims and expect this trend to continue as the large events of summer 2024 continue to develop.

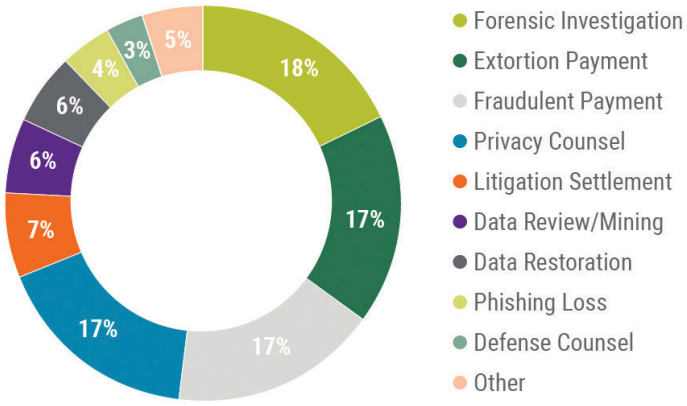
Industries leading the way in claims frequency among our SME clients so far in 2024 are charity/nonprofit, manufacturing, investment advisor/CPA/mortgage broker, construction, and healthcare. Education and public entity are deliberately excluded from these figures, as the SME market remains somewhat contracted for these sectors.

Industries with the most claims through Q2 2024



Taking a slightly different spin on claims analysis, we felt it would be useful to analyze the proportion of expenses allocated in paid cyber claims for SMEs among RPS insureds. The following information is representative of an 18-month study of claims from RPS proprietary claims data on small businesses across the US, in all industry sectors, under $100 million in annual revenue.

Paid cyber claim expense categories for SMEs:
Top categories are forensic investigation, extortion payment, fraudulent payment, and privacy counsel.



CYBER NOTES FROM THE FRONT LINES

A new element of our market updates will feature anecdotal information our Cyber practice encounters in their daily handling of cyber insurance submissions, quotes, renewals, and claims. These anecdotes can be great nuggets for retail agents to share with their insureds when asked about new developments (or important reminders) in the cyber insurance arena. Following are few things our team has noted in recent weeks.

- One insurer issued a brief moratorium on all new business submissions in the wake of the recent highly publicized security software vendor's software update failure. Additionally, several insurers required no-loss attestations relative to this event as a condition of binding new business and renewals.
- We're seeing various approaches to carrier fees on cyber policies. One market is offsetting the cost of their risk management offerings by adding new fees to their policy. The fees range from $250 to $2,500, depending on the size of the insured and their associated premium. Conversely, another market is doing away with fees. As cyber insurers continue to expand risk management offerings, it will be interesting to see how these offerings are financed.
- We can't emphasize enough the importance of training employees to recognize fund transfer scams. Just last week, an insured received an email requesting what they thought was a change in payment instructions from a fellow employee, appearing to come from their internal accounting department. Moments later, that same "employee" sent another internal email claiming they had called the requestor and validated the authenticity of the request, with instructions to process immediately. Seeing this as a reasonable check and balance, the employee sent the funds, learning later that both emails were from a fraudster, and the money was diverted to a criminal's bank account. Criminals are increasingly learning their victims' protocols to prevent fraud and are developing ways to circumvent them.
- A hacker gained unauthorized access to an insured's network and obtained passwords for the CEO's cryptocurrency wallet, stealing $70,000. Some policies address this exposure, but many do not.

- A legacy top-tier insurer for auto dealers recently amended their dependent BI waiting period to 24 hours on all accounts in the wake of a recent SaaS provider ransomware attack. Conversely, a newer specialty entrant is offering full policy limits for dependent BI with an eight-hour waiting period. This example illustrates the current dichotomy that often exists among players in the cyber insurance market.
- As claims related to the February 2024 medical billings software vendor's ransomware attack continue to develop, we're hearing differing interpretations among carriers about the description of services that the vendor provided to its healthcare provider customers. Dependent/contingent BI insuring agreements in cyber insurance policies address coverage via defined terms such as "service provider" or "outsourced provider," while some assign meaning within the definition of "computer system." These nuances become important as carriers interpret the work that this vendor provided, delineating between clearinghouse claims services and more literal IT services such as cloud hosting, processing digital assets, etc.

AI AND THE CONTINUED IMPACT ON COMMUNICATIONS AND CLAIMS

Switching gears from the very real to the very fake, in our 2024 Q2 Cyber Market Update, we warned of the anticipated use of generative AI in attempts to influence outcomes of the 2024 US elections. We're seeing this play out in various ways.

Within mere minutes of the attempted assassination of Donald Trump on July 13, deepfaked videos appeared depicting Secret Service agents smiling as they protected the former president, insinuating satisfaction with things "going as planned," along with memes circulating on X (formerly Twitter) showing President Biden holding an assault rifle as if he had been the one pulling the trigger.

As the English National Football team slugged their way toward the 2024 Euro finals, in what many believed to be an unimpressive fashion, deepfake videos of then-manager Gareth Southgate saying highly controversial things about his players were widely distributed on Instagram and other social media platforms.

We're indeed in the Age of Misinformation, fully amplified by rapid advances in AI.

From manipulated videos of the president and vice president making statements they never made to AI-generated photos falsely depicting former President Trump in compromising situations to the use of synthetic speech in attempts to incite financial instability in the US economy, these new technologies are being widely used for nefarious purposes both inside and outside of politics. More recently, X (formerly Twitter) CEO Elon Musk has caught heat for his reposting of a deepfaked campaign ad depicting Vice President Kamala Harris saying things as the new democratic nominee for president that she didn't say.

Whether politics or business, it's clear to see the impact of these technologies on both reputations and finances. While fraudulent payment claims on cyber insurance policies represent the highest frequency, we can expect the use of AI to exacerbate this trend. As threat actors employ new methods to make their schemes more believable, the importance of old-fashioned human intervention, due diligence, and employee training becomes even more important.

ON THE HORIZON

Whether the recent events described in this report are enough to move the needle on cyber insurance pricing remains to be seen. One thing is for sure — carriers have been concerned about systemic risk for some time, and we're increasingly getting reminders of how a single point-of-failure event can cause widespread disruption through lost productivity, lost revenue, and reputational damage.

Past events like the WannaCry and NotPetya ransomware attacks of 2017; the SolarWinds software hack of 2020; the Log4J software vulnerability of 2021; the Microsoft Exchange server hack of 2021; the Kaseya VSA ransomware attack of 2021; the MOVEit file transfer software vulnerability in 2023; and the more recent ransomware, hacking, and software failure events of 2024 will continue to inform decisions that cyber carriers make in their coverage offerings.

The levers of sublimits, waiting periods, exclusions, retentions, premiums, and restricted appetite will be pulled in various degrees. As carriers endeavor to strike the right balance of comprehensive coverage and appropriate pricing, the use of technological tools to help assess risk will continue to advance. We'll see increased scrutiny on the vendors with which our insureds work and the policy wording that protects insureds when these vendors experience disruptions that impact our insureds.

The bottleneck of impending losses associated with these events undoubtedly will lead to changes once these claims further develop. Working with a knowledgeable broker in this rapidly developing area of cyber risk has never been more important. At RPS, we'll continue to monitor these developments and help our clients secure the right coverage, at the right price, for our mutual insureds. With more than 140 members of our Cyber practice working in this space on a daily basis, we're well positioned to help you come through for your clients.

Sources

[1]Whittaker, Zach. "Health Insurance Giant Kaiser Will Notify Millions of a Data Breach After Sharing Patients' Data With Advertisers." *TechCrunch*, 25 Apr. 2024.

[2]Zetter, Kim. "Hackers Detail How They Allegedly Stole Tickmaster Data from Snowflake." *Wired*, 17 Jun. 2024.

[3]Hauari, Gabe. "How to Know If You Were Affected by the AT&T data breach and What to Do Next." *USA Today*, 12 Jul. 2024.

[4]"J.D. Power-GlobalData U.S. Automotive Forecast for June 2024 — Dealer Software System Outages Disrupt June Sales; Rapid Recovery Expected in July." *Business Wire*, 26 Jun. 2024.

[5]Fung, Brian. "We Finally Know What Caused the Global Tech Outage — and How Much It Cost." *CNN*, 24 Jul. 2024.

[6]Ayers, Erin. "'Most Important Cyber Accumulation Loss Event Since NotPetya' Highlights Single Points of Failure." *Zywave*, 25 Jul. 2024.

[7]"Widespread IT Outage Due to CrowdStrike Update." *CISA*, 06 Aug. 2024.

[8]"New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying." *Coveware*, 26 Jan. 2024.

RPSins.com

RPS® RISK PLACEMENT SERVICES