

A woman with dark hair is sitting at a desk, looking at a laptop. The scene is dimly lit, with a desk lamp providing light. The background is a soft, out-of-focus office environment. The entire image has a green overlay.

2023 U.S. Cyber Market Outlook

Helping you come
through for your clients



Despite being around for more than a quarter of a century, cyber insurance remains a relatively young market in insurance terms.

As such, it continues in a seemingly perpetual state of evolution with rapidly changing underwriting processes, coverage developments and increased regulatory influence.

The last two years, however, have been particularly tumultuous, with double- and triple-digit premium rises in the wake of an increased threat from cybercriminals and the inevitable influx of claims that followed.

“Capacity continues to be a challenge, driven by the combination of increased demand, two-plus years of significant premium increases, more judicious limits deployment and the exit of some players from the market,” stated Steve Robinson, Risk Placement Services (RPS) area president and national cyber practice leader.

In addition, the COVID-19 pandemic has created cyber challenges for insurers and insureds alike.

“The pandemic has shifted the geography of the workplace significantly in ways that will continue for the foreseeable future,” said Robinson. “As a high percentage of the workforce is still either in a remote environment—or at least a hybrid between home and office—remote access continues to be an exposed vulnerability. These remote work influences have had a significant impact on the cyber insurance market.”



The pandemic has shifted the geography of the workplace significantly, and remote access continues to be an exposed vulnerability.

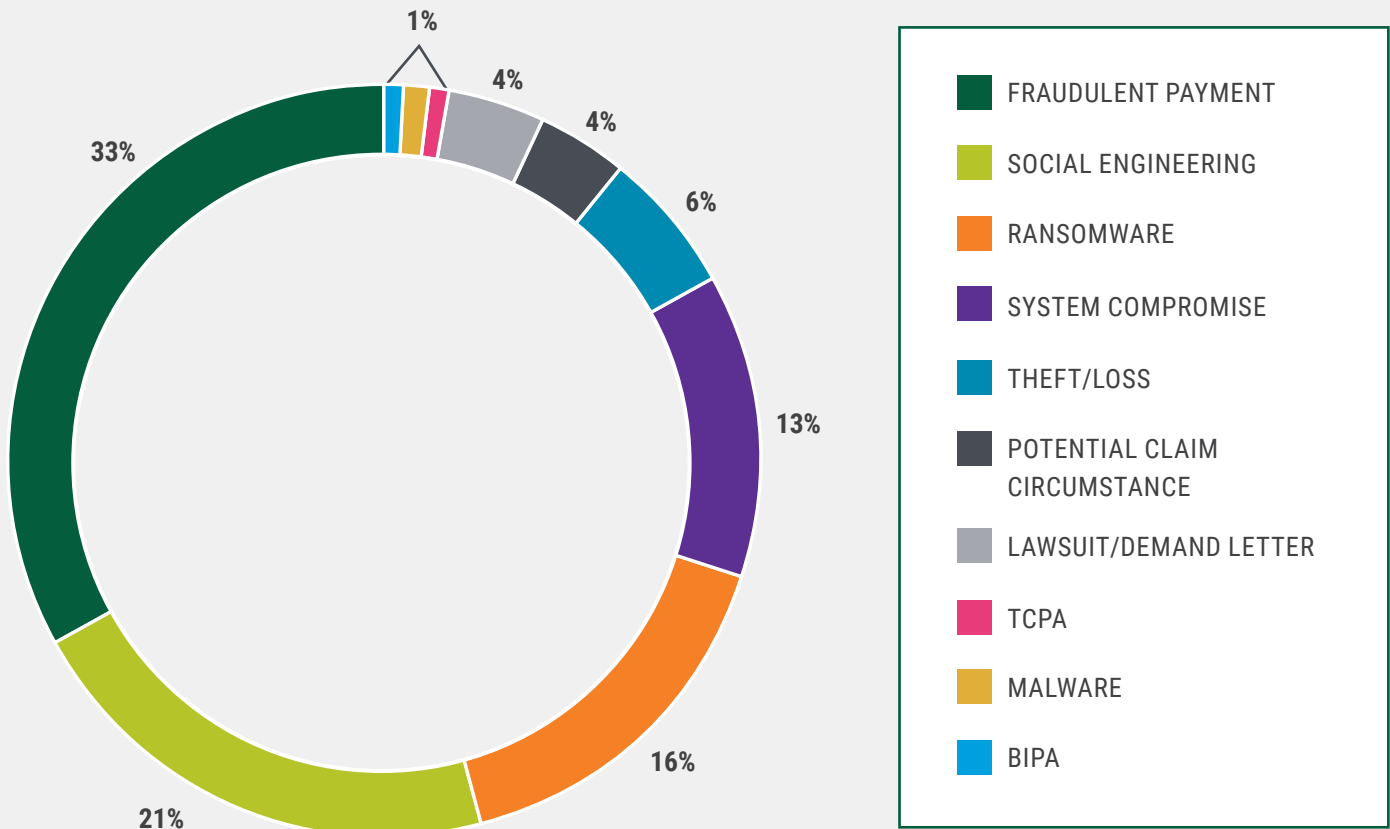
“Social engineering claims continue to climb in frequency as a result, with many organizations still not employing the proper controls to verify the authenticity of fraudulent changes in payment instructions.”

Indeed, over the first eight months of 2022, fraudulent payments and social engineering frauds have accounted for more than half of cyber claims on RPS small to mid-sized insureds (SME), with incidents of ransomware now

accounting for 16% of incidents—although this remains the third most common type of attack across the SME sector.

This time last year, ransomware accounted for a significantly higher proportion of reported incidents among this same demographic. While the downturn in ransomware is significant, there are concerns the trend may be somewhat anomalous.

YTD CYBER CLAIMS % BY MATTER TYPE



Source: Information derived from proprietary RPS claims data among insureds in the SME sector (< \$100 million annual revenue)



We have reached a tipping point where cyber risk has shifted from being purely a business risk to also being a risk to society overall.

RISING REGULATION

In response to this changing threat landscape, regulatory oversight is beginning to increase, with RPS Area Senior Vice President Comber McHugh saying that increased regulation had become inevitable given the impact and frequency of claims hitting the sector.

“We have reached a tipping point where cyber risk has shifted from being purely a business risk to also being a risk to society overall,” she said. “And that is when regulators step in to help accelerate change or correction and provide protection through oversight because the market forces are not adequately addressing the needs of society.

“We are now seeing billions of dollars a year being spent on cyber losses, as well as consequences becoming much more dire as a result of increased attacks on infrastructure – and that is when society begins to say we need to enact laws to modify behavior.”

Dozens of cyber-related laws are in various states of drafting and debate among lawmakers throughout the U.S., with a particular focus on data privacy in response to the GDPR regulations introduced in Europe.

“There has been a lot of talk around introducing a federal standard for data privacy, and an actual federal data privacy protection act is currently being debated in Congress,” McHugh said. “But it remains to be seen whether any federal standard would be the ceiling for regulation, or if it would act as a floor that more aggressive states such as California and New York would be able to build on.”

So far, direct intervention in the cyber insurance market has been limited, but states such as North Carolina and Florida have acted to ban public entities from paying ransoms in response to cyber extortion incidents, with other states considering similar measures.

This will be a cause of concern for public entities. Several insurers have

pulled back from covering public entities—including those in the K-12 public education sector—as a result of the high frequency of claims facing these sectors.

“As well as traditionally facing the highest frequency of claims, the public entity and education sectors are also often the least prepared for an attack,” noted Robinson.

Some states such as New York are considering banning private companies in addition to public entities from paying ransoms.

There is great debate among the political, legal and insurance communities around the anticipated efficacy of banning ransom payments, but Robinson said there is one thing everyone can agree on.

As well as traditionally facing the highest frequency of claims, the public entity and education sectors are also often the least prepared for an attack.

“As long as ransomware attacks remain both lucrative and anonymous, they will not suddenly disappear because a state law says certain sectors cannot pay,” he said. “For some, there is unfortunately no alternative, increasing the chances of these transactions occurring outside of public view.”

There is also speculation that states enacting bans may increasingly become targets of destructive attacks, as perpetrators apply pressure for reversal of these decisions.

“Payment of a ransom is not first on anyone’s list of preferences to gain access to an insured’s data,” Robinson added. “In fact, insurers and their vendors will do everything possible to avoid this. Taking the option off the table completely, however, may not be in the best interest of anyone.”



RANSOMWARE-AS-A-SERVICE

Prior to 2019, most ransomware attacks were mass-target attacks seeking nominal amounts in ransoms, meaning that they were likely to be paid in order for the victim to regain access to their data.

Things changed in 2020, and cybercriminals began more targeted attacks aimed at the “low-hanging fruit” for which they could extract higher ransom payments.

“Healthcare, retail, public entities, public schools, community colleges and government organizations were all targeted as low-hanging fruit by cybercriminals across 2020 and 2021,” said RPS Area Senior Vice President Bryan Dobes. “But those attacks were typically conducted in-house by an organization in a vertically-oriented attack with a specific entry point.”

Today’s ransomware attacks are more sophisticated, with ransomware-as-a-service expected to be one of the biggest threats to face the cyber market over the coming months and years.

“Ransomware firms are now effectively licensing out proprietary ransomware software that is leading to much wider-scale attacks with more potential facets to it,” Dobes said. “This makes it much less likely that an organization—or even a cybersecurity firm – will be able to pinpoint exactly how an attack is developing.”

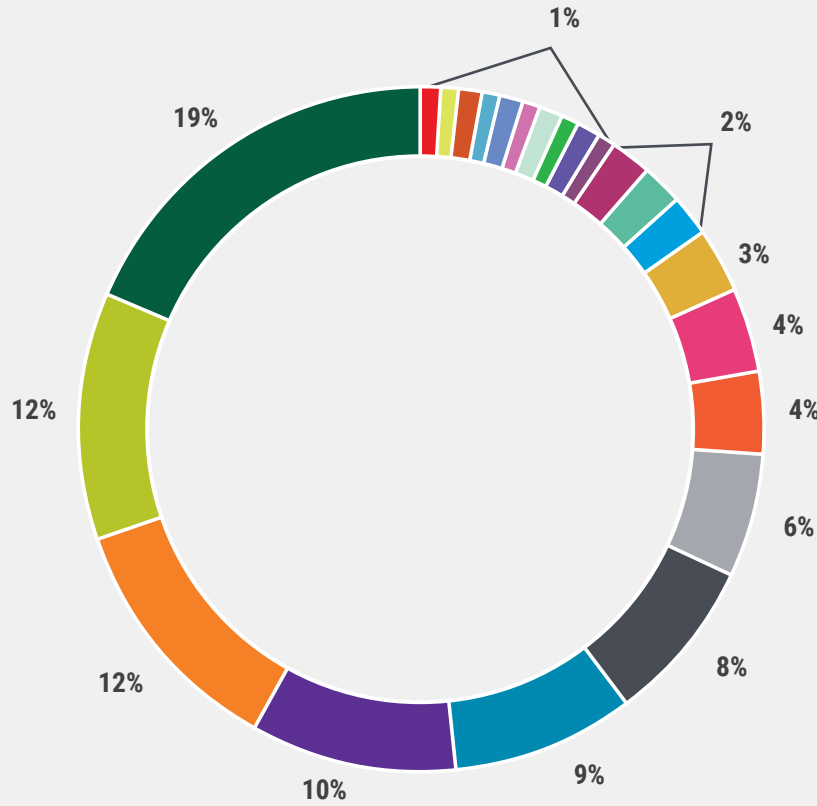
The more sophisticated nature of these attacks has also led to a change in the way cybercriminals are approaching the negotiation of a ransomware attack.

Today’s ransomware attacks are more sophisticated, with ransomware-as-a-service expected to be one of the biggest threats to face the cyber market over the coming months and years.

“These new threat actors have effectively ended the negotiation phase of an attack,” Dobes warned. “They are now often adopting a take-it-or-leave-it approach: If you don’t pay the initial ransom—or you involve a third-party forensics firm—they simply delete your data or sell it on the dark web.”

Looking to the future, ransomware attacks are no longer solely targeting data in order to charge a ransom to prevent publication of the data on the dark web. Instead, cybercriminals are focusing on attacks that take down systems and prevent businesses from operating—meaning traditionally unaffected sectors, such as manufacturing and wholesale distribution, are now firmly in the crosshairs.

YTD CYBER CLAIMS % BY INDUSTRY TYPE



MANUFACTURING	HEALTHCARE/MEDICAL	RETAIL
CONSTRUCTION	INSURANCE BROKER/COMPANY (COMMERCIAL)	FIN. INST.- COMMUNITY/STATE/CREDIT UNION
CHARITIES/NONPROFIT	TRADE ASSOCIATIONS	INSURANCE BROKER/COMPANY (PERSONAL LINES)
WHOLESALE DISTRIBUTOR	UTILITY	TITLE/ESCROW/SETTLEMENT/CLOSING AGENT OR AGENCY
PROFESSIONAL SVC EXEL LEGAL SVCS	LEGAL SERVICES	RESTAURANTS
GOVERNMENT	REALTOR	DOMESTIC SERVICES
EDUCATION (SCHOOLS)	HOTELS/HOSPITALITY	LEGAL SVCS(CONSUMER)
INVESTMENT ADVISOR/CPA/MORTGAGE BROKER	EDUCATION (COLLEGES/UNIVERSITIES)	

Source: Information derived from proprietary RPS claims data among insureds in the SME sector (< \$100 million annual revenue)



Over the first eight months of 2022, the manufacturing industry has been the target of almost a fifth (19%) of all cyber insurance claims reported by SME insureds, according to RPS proprietary data, with construction—another industry impacted greatly by business interruption claims—the second-most-likely industry to be targeted after facing 12% of all attacks.

“Manufacturing is starting to face a much bigger threat from cybercriminals because, while the sector doesn’t usually hold a lot of data, comparatively it has a very large business interruption risk,” noted RPS Area Assistant Vice President Zach Kramer. “I’ve seen cases where there have been \$800,000 to \$1 million ransom demands following an attack, and then an additional \$2 million to \$3 million in business interruption losses.”

Manufacturing is starting to face a much bigger threat from cybercriminals because, while the sector doesn’t usually hold a lot of data, comparatively it has a very large business interruption risk.

“This means that where historically manufacturing has been quite inexpensive for cyber coverage, we are now seeing a situation emerging where some insurance carriers simply will not cover that sector altogether. For carriers that are willing to insure this sector, it isn’t uncommon to see attachment points in excess of \$30 million, where previously they would have considered first-dollar coverage.”

POLICY WORDINGS TIGHTENING

Insurers' response to this changing threat metric has been widespread and rapid, with exclusions quickly becoming commonplace in the market.

One example is war exclusions, meaning that an insurance policy won't cover state-backed attacks influenced, at least in part, by the actions seen coming out of Russia following its invasion of Ukraine.

"We are starting to see insurers exclude cyber terrorism events and state-backed attacks from coverage," said Kramer. "It is not in every policy yet, but it is certainly coming.

"We are also starting to see exclusions relating to infrastructure attacks and carriers broadening their stance on what is considered infrastructure. We are also seeing the lowering of limits on the contingent business interruption elements of a policy."

Kramer added that many of these exclusions can appear inconsequential at first, but warned agents and brokers to look deeper into the wordings of the policies—particularly important due to the differences in insurers' approaches.

"A lot of the general mandatory endorsements can appear innocuous at first," he warned. "But look closer and they can include significant implications for a policy."

Insurers are also increasingly concerned by the systemic risk from widespread use of third-party cloud providers, going so far as to name the major players in policy wording.

"We are beginning to see insurers introduce sublimits or exclusions for claims that result from a specific large-scale attack or event in the supply chain that makes up the wider security infrastructure," Dobes said.

As a result, insurers are becoming more selective with their underwriting appetite.

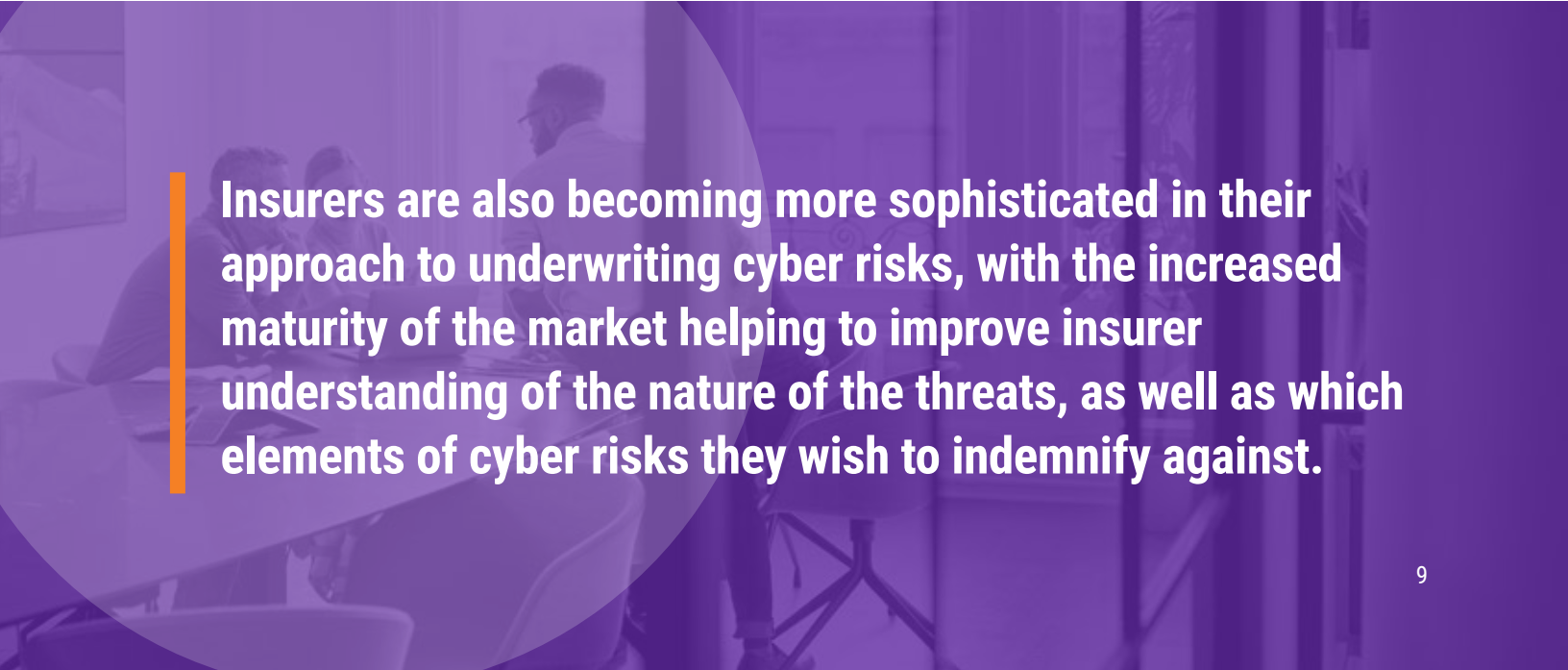
"Brokers now need to find the insurers where their clients fit like a puzzle piece into their underwriting appetite, and that is becoming increasingly difficult," noted RPS Area Senior Vice President Adam Connor. "We could even see insurers starting to exclude or limit coverage for a particular cloud provider if they feel their exposure to that provider is getting too high."

UNDERWRITING INCREASING IN SOPHISTICATION

Insurers are also becoming more sophisticated in their approach to underwriting cyber risks, with the increased maturity of the market helping to improve insurer understanding of the nature of the threats, as well as which elements of cyber risks they wish to indemnify against.

Connor said that this means question sets are changing in response, and insurers are increasingly using third-party scanning technologies to help detect security weaknesses.

"Question sets have grown a bit, but that is beginning to level off now," he said. "We might see things getting a bit more granular around systemic risks, but I wouldn't expect any material changes."



Insurers are also becoming more sophisticated in their approach to underwriting cyber risks, with the increased maturity of the market helping to improve insurer understanding of the nature of the threats, as well as which elements of cyber risks they wish to indemnify against.



Increased underwriting sophistication also means that insurers are becoming more stringent around the security measures insureds must have in order to achieve cover – particularly for larger companies.

“Insurtechs initially led the way when it came to technologically advanced and innovative underwriting approaches, and most insurers are now adopting these techniques into their underwriting practices.”

This increased underwriting sophistication also means that insurers are becoming more stringent around the security measures insureds must have in order to achieve cover—particularly for larger companies.

“If you’re under \$100 million of revenue, depending upon what class you’re in, you generally have options for lower limits that don’t require the same controls to be in place,” said Dobes. “But if you have revenues in excess of \$100 million, regardless of which industry you are in, there is now a much higher security requirement across the board.”

Endorsements around the security measures put in place are also being used by insurers to help them reduce their overall exposure where these measures may not be robust.

For example, Kramer said insurers are introducing endorsements around critical, known vulnerabilities on the National Vulnerability Database. “If it is not patched by insureds within 30 or 45 days, then it will start to affect their coverage,” warned Kramer. “And these coverage restrictions then increase for every month after that, introducing lower and lower limits, which places a lot of responsibility on the insured. This is particularly hard for smaller organizations to manage.”

Kramer added: “Sometimes these endorsements can also include an element of coinsurance.”

The good news is that these actions are leading to increased levels of security, making businesses more resilient in the event of an attack.

“Organizations are increasingly investing more in the basics of multifactor authentication (MFA) for remote access, improved backup solutions, managed endpoint detection and response, and employee

training,” noted Robinson, “driven in no small part by the increase in underwriting requirements from cyber insurers.”

“These are encouraging trends for insureds and insurers alike,” he added.

This is also helping insurers to better manage their losses and, in turn, will lead to a slowdown in the premium increases experienced in recent years as the market begins to adjust—even if increases of between 15% and 25% are still a common sight at renewal.

“More prudent limits deployment over the past two years, along with a more disciplined underwriting approach, are contributing to improved loss ratios among many cyber insurers,” noted Robinson. “It is, however, now much rarer to see \$10 million limits offered from a single insurer, whereas this used to be commonplace as recently as 2019.”

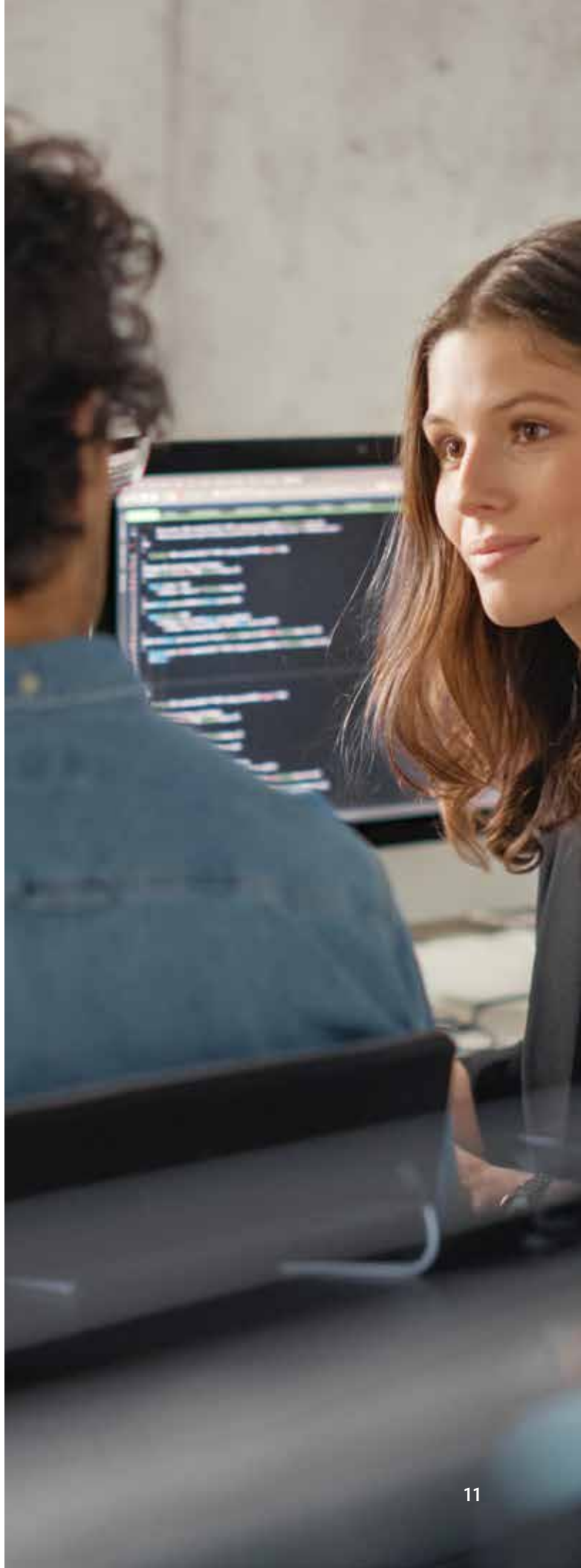
The pace of change is varied among carriers in the market.

“Perhaps the most interesting thing about the changes we are seeing now is how different one carrier’s tactics can be from another’s,” noted Robinson. “Last year, every market was taking large rate increases and increasing information security requirements in order to qualify for coverage. This year, we are seeing everything from a continuation of this trend among some markets to a swing in the opposite direction from others.”

Indeed, while one admitted carrier recently filed an across-the-board 38% rate increase and implemented a significant pullback in exposures to ransomware-related losses, others have reduced barriers to entry for small businesses and projected virtually flat premium expectations over the coming months.

The insurance industry as a whole has often been accused of having a short memory when it comes to actions taken to improve loss ratios. These conflicting approaches to the market provide support for this reputation.

Despite loss ratio improvements, the frequency and severity of claims remain a problem for insurers, and lower sublimits are increasingly making their way into policy wordings.



“We are seeing first-party sublimits as low as \$100,000 for some policies, maybe as much as \$500,000 to \$1 million,” noted Dobes. “So you might have a headline \$3 million aggregate limit containing a \$100,000 sublimit for any event triggered by a ransomware event.”

“Many insurers are quite dramatically reducing their exposure.”

For institutions that contractually or legally require a certain level of third-party liability cover, Dobes added, sometimes the only solution is to adopt a high level of retention or to take first-party coverage off the table.

CONSIDERATIONS FOR AGENTS IN THIS EVER-CHANGING MARKET

Agents and brokers still have a pivotal role to play in helping their customers to understand the threats they are facing and how to prevent them, as well as in choosing the best type of policy to protect their organization.

“Communication with your clients is key for any agent or broker,” urged Robinson. “You need to be speaking to your clients way ahead of their renewal so that any remedies that need to be put in place can be actioned ahead of the renewal application, making it easier to find the appropriate level of cover.”

“But that doesn’t mean you have to be an expert on cyber to make it work—partnering with firms such as RPS and leveraging that market knowledge can certainly help.”

And agents and brokers also have a lot to consider when it comes to managing their own books of business.

“As has always been the case, the more highly regulated industry sectors will often be ahead of the curve when it comes to cybersecurity, thus creating a more desirable pool of applicants for insurers,” argued Robinson. “The financial, healthcare and retail sectors are examples of areas where higher regulation, plus the adoption of more sophisticated cyber defenses, creates opportunities.”

THE NEW WORLD OF CYBER SUBJECTIVITIES

As insurers increasingly utilize advanced technologies to assess cyber risk, agents and brokers need to be aware of the new technical subjectivities that often accompany quotes and proposals.

Here are a few suggestions to help with your next cyber new business or renewal placement:

- Familiarize yourself with the scanning technologies insurers are employing. Be prepared to answer your insured’s questions about the “how” of the process (e.g., No, the insurance company is not going behind their firewall without permission!).
- Start early. For renewals, don’t be surprised if new subjectivities are in place that weren’t there previously. Read the fine print and be sure to call out the subjectivities in writing, separate from the proposal. They are sometimes buried deep within the document—highlighting them is critical.
- In an effort to increase response time, carriers are often releasing pricing indications that are not bindable. While this helps agents to quickly assess the viability of terms, there’s still hard work to be done. The best coverage and price still doesn’t guarantee a bind order until the insurer deems the risk acceptable.
- Don’t attest to subjectivity compliance with broad statements such as “Subjectivities have been satisfied.” Underwriters are increasingly demanding line-by-line technical answers to each individual subjectivity before releasing bindable terms. This requires the involvement of the insured’s IT personnel or third-party technology vendor.
- Keep in mind, insurers might not be lining up to insure your client, particularly if their controls are perceived as subpar—this isn’t 2017, and they need to take the application and the process seriously. Presenting their organization in the best yet most accurate light will help ensure the best results.

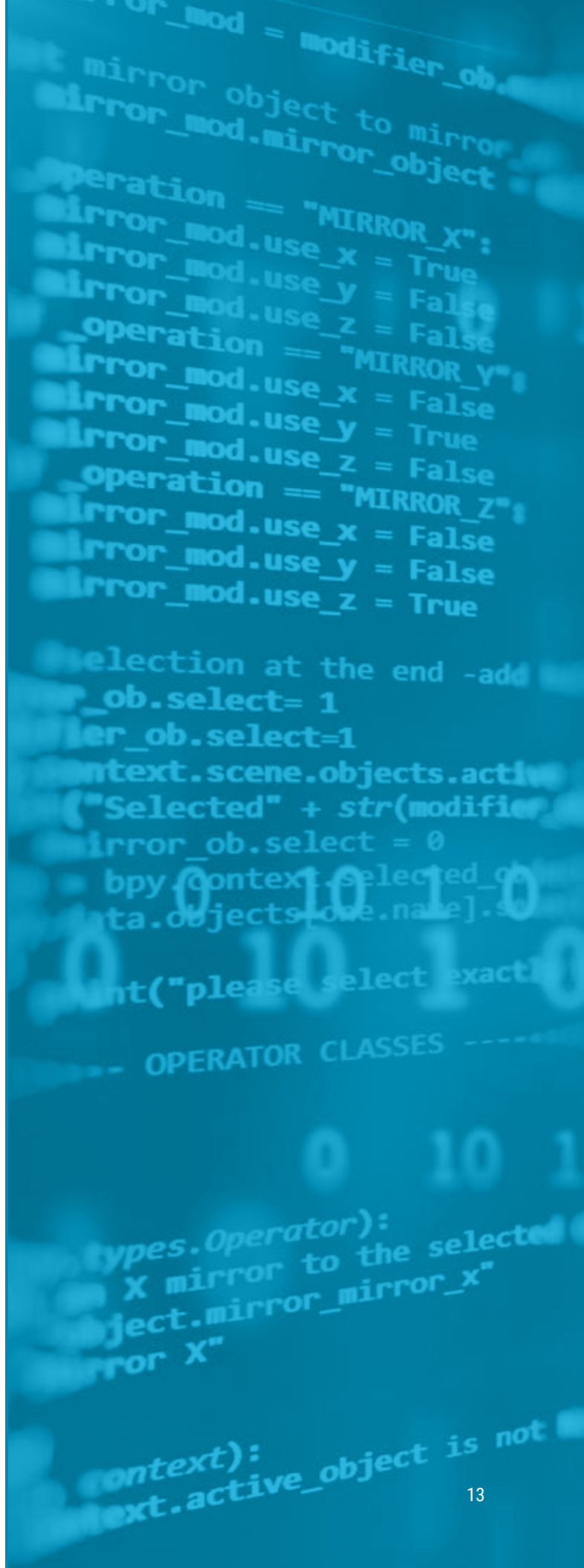
“In contrast to this, sectors previously thought to be low risk for data breaches—such as manufacturing and construction—have increasingly experienced the larger business interruption losses associated with ransomware attacks and, as a result, have become less desirable classes of business for most insurers.”

The perpetual state of change in the cyber insurance market is reflective of a risk that, by its very nature, is constantly changing. So it stands to reason that the levers of rate, underwriting requirements, limits deployment, retentions and exclusionary wording are pulled in different ways by different participants.

As the cyber insurance industry has taken on, in our view, an unfair share of criticism relative to “enabling” the ransomware epidemic to flourish, the irony is that the insurance industry is leading the way to promoting improved defenses and operational resiliency to these ever-evolving threats.

“To remain motionless in the face of a moving target will not yield sustainable results for a dynamic market that continues to show great promise,” Robinson stated. “And as the cyber insurance industry has taken on, in our view, an unfair share of criticism relative to ‘enabling’ the ransomware epidemic to flourish, the irony is that the insurance industry is leading the way to promoting improved defenses and operational resiliency to these ever-evolving threats.”

At RPS, we continue to monitor these developments in the cyber insurance marketplace, and provide insight and guidance as we help our agents and brokers come through for their clients.



LOOKING TO THE FUTURE

Several themes emerge as topics on the radar for Q4 and into the New Year, including:

- **Inside-out underwriting.** Advanced integration of 'behind the firewall' technologies will enable underwriters to craft cyber insurance programs and pricing that are more commensurate with the risk. Moving beyond paper applications with applicants' permission to view inside their network can potentially yield better results for all parties. Take-up rates for these offerings will be interesting to watch as insureds must decide if additional eyes on their data warrants cost savings and additional risk management value.
- **Temporary lull?** While ransomware losses have decreased in frequency, they have increased in severity and are more often accompanied by threats of data exfiltration. As the situation in Russia and Ukraine continues to develop, will the frequency of attacks state-side correlate with the geopolitical ebbs and flows? The most recent loss data suggests we could potentially return to a rise in frequency.
- **Underwriting Dichotomy** – Particularly in the SME sector, inconsistency has become the consistent trend among insurers. Some markets are lowering rates and easing underwriting requirements, while others continue a more disciplined approach. While these tactics are vastly different, one thing is certain: The cyber insurance market is extremely dynamic and offers great promise to those taking a measured approach. New entrants, pricing for fast market share, low barriers to entry and diving in with confidence that the ransomware epidemic is behind us, could find themselves in a fast retreat.
- **Social engineering/financial fraud continues to rise.** And why not? Put yourself in the mindset of the bad guys—as long as a simple email request can convince someone to wire you \$100,000 without questions, isn't that easier than stealing data and trying to monetize it? Insurers are tiring of the death-by-a-thousand-cuts losses they're paying for social engineering and wire fraud claims. Conditions precedents will increasingly find their way into policy language. The message: "If you're not making all best attempts to validate the authenticity of payment instructions, we're not paying your claim."
- **The next big thing?** Data breach, ransomware, social engineering, DDoS attacks, deep fake technologies: All are popular tactics amongst cybercriminals. As we report this, the next tactics are already being tested and deployed. The attack vectors that are currently unknown are perhaps the most worrisome. This is something unique to this line of coverage—the goalposts are always moving. We anticipate innovative threats to critical infrastructure, financial platforms, operational technologies and cloud-hosted environments. The question remains: will the significant advances in information security made by many insureds in the past two years protect them from these yet-to-be-discovered threats?

CONTRIBUTORS

Steve Robinson, Area President and National Cyber Practice Leader

Adam Connor, Area Senior Vice President

Comber McHugh, Area Senior Vice President

Bryan Dobes, Area Senior Vice President

Zach Kramer, Area Assistant Vice President

ABOUT RISK PLACEMENT SERVICES

Risk Placement Services (RPS) is one of the nation's largest specialty insurance products distributors, offering solutions to independent agents and brokers in wholesale brokerage, binding authority, programs, standard lines and nonstandard auto. The RPS team, fueled by a culture of teamwork, creativity and responsiveness, works with top-rated admitted and nonadmitted carriers to design robust coverage for clients through its more than 80 branch offices nationwide.

For more information, visit RPSins.com.

The information contained herein is offered as insurance industry guidance and provided as an overview of current market risks and available coverages and is intended for discussion purposes only. This publication is not intended to offer legal advice or client-specific risk management advice. Any description of insurance coverages is not meant to interpret specific coverages that your company may already have in place or that may be generally available. General insurance descriptions contained herein do not include complete Insurance policy definitions, terms, and/or conditions, and should not be relied on for coverage interpretation. Actual insurance policies must always be consulted for full coverage details and analysis.

Copyright 2022 Risk Placement Services, Inc. No copyright claimed in works of the U.S. Government.

RPS43388 1122