Competitive Cyber Market Expected to Continue

This year marks the 20th year in which Cyber Security Awareness Month has been observed. For many that means reminders about using strong passwords, implementing multi-factor authentication, and being aware of phishing and updating software.

But we wanted to take a deeper dive – focusing on what's going on in the market and how to help your clients make the most of it. We'll highlight two of the most talked about topics of the year: growing ransomware attacks, including the MOVEit data breach, and meta pixel tracking class action lawsuits as well as the Securities and Exchange Commission's (SEC) final cybersecurity disclosure rules that went into effect last month.

CONTACT

To learn more about how Amwins can help you place coverage for your clients, reach out to your local Amwins broker.

LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions.

Please refer to your policy for the actual language.

Courtesy of Amwins Group, Inc.

Ransomware Attacks Increase in Frequency and Severity

After a brief reprieve in attacks – attributed by most as a result of the Russian invasion of Ukraine – we have experienced a surge in ransomware claims. There has also been some change in the threat landscape as more of these attacks appear to be motivated by a social agenda rather than strictly an attempt to extort money.

We've seen an increased number of attacks based on either a group trying to further their own social agenda or a group trying to fight the agenda of a policy or group they don't agree with. And, because of the number of different motivating factors for these attacks, they can be harder to protect against.

For example, in August of this year, the group Anonymous **attacked Japanese nuclear websites** in response to the plan to release treated radioactive water from the failed Fukushima power plant. This attack was focused not only on nuclear power-linked groups in Japan, but other large organizations and political entities associated with nuclear power-related companies.

MOVEit Data Breach

In May 2023 a previously unknown vulnerability to MOVEit file transfer software was discovered and exploited by CLOP, a known ransomware group with ties to Russia. To date, **more than 2,200 organizations and up to 65 million individuals have fallen victim** to this unprecedented hack.

MOVEit was sold primarily to large companies working at scale and transferring large amounts of data. Not surprisingly, nearly 180 of those organizations attacked were colleges and universities. However, schools have taken this type of threat very seriously and put a lot of funds towards controls in the past few years, so it could have been much worse.

With an estimated $65 billion of losses at stake, we're reminded we must all be prepared when it comes to protecting data – especially when you consider that gross written premium (GWP) is estimated at $17 billion and expected to grow to more than $20 billion by 2025.

This discrepancy highlights just how much uninsured loss there is and just how exposed your clients may be. To help ensure adequate risk mitigation and protection for clients of all sizes, **we created a checklist of privacy and compliance requirements and training**, including resources businesses can implement to protect themselves before a cyber event happens.

Market Impacts

Despite the ongoing challenge of large and frequent ransomware attacks, the marketplace remains very competitive – a stark contrast from the hard market conditions of 2020 to late 2022. Renewal rates have decreased significantly, and some companies are eliminating sublimits and coinsurance on ransomware coverage which was common on cyber policies during the hard market cycle. This softer rate environment sees markets looking to make up that business with increased market share.

Insureds have seen a 30% to 50% decrease in premiums (especially in the larger space) as well as enhancements to coverage for social engineering. Where before most markets limited this coverage to $250,000, $500,000 to $1M sublimits are no longer as rare.

We are pushing for lower retentions and premium relief, as well as adding coverage enhancements such as Contingent Bodily Injury and Property Damage, Non IT dependent business interruption, post-breach remediation expenses and PCI recertification expenses.

Meta Pixel Tracking Lawsuits Result in Regulatory Scrutiny

In the past year, we've seen an exponential number of class action lawsuits alleging that healthcare companies' usage of online tracking technologies and subsequent sharing with the likes of Meta violate the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Meta is currently facing at least 50 class action lawsuits and U.S. Congress has begun an inquiry into a number of **telehealth companies accused of sharing patients' answers to medical intake questions and a recent study by The Markup** found that 33 of the top 100 hospitals in America were using Meta Pixel and sending Facebook information whenever a person clicked a button to schedule a doctor's appointment. The study also determined that seven of the health systems surveyed also had Meta Pixel installed inside password protected patient portals.

Litigation alleging that the use of tracking vehicles from Meta, Google, TikTok, and more, violates the federal Video Privacy Protection Act (VPPA) and may constitute wiretapping under federal and state wiretapping laws, is also on the rise.

While most suits have not been fully litigated, they have caught the attention of State Attorneys General and raise a number of legal questions, including what role – if any – terms of service and website disclosures play and how the use of tracking technology applies to both the Electronic Communications Privacy Act and Stored Communications Act. Further, the $18.4M settlement resolving a class action lawsuit against Mass General Brigham Hospital has caught the eye of insurance carriers.

It's still too early to tell if additional regulation will be enacted, but there are already parallels to compliance rules put in place within the payment card industry (PCI). These compliance rules were established in the early 2000s when the Federal Trade Commission (FTC) gained oversight of consumer protections.

With so many questions about Meta Pixel liability unanswered, insureds need to be prepared. As the industry learns more about this exposure, we expect rates will be adversely impacted. Underwriters will want to confirm that insureds are performing their due diligence properly and what protections are built into contracts with third parties.

You can **read our full report on meta pixel class action lawsuits here.**

SEC Inquiries

In September, the SEC's final cybersecurity disclosure rules went into effect. The annual cybersecurity disclosure associated with the new rules will follow starting mid-December. As these new rules go into effect, insureds should be prepared in the event they receive an SEC inquiry related to a security or privacy event.

We don't yet know what type of requests for records there will be. But we do know a cyber policy and breach coach could respond to the inquiry (as it's a regulatory investigation arising from a network security breach) and that D&O policies do not cover the costs of a breach coach.

It remains to be seen whether cyber or D&O coverage is best equipped to respond to an SEC inquiry.

What to Expect in the Coming Months

The next six to 12 months will be critical. We expect soft market conditions in the interim, but for classes such as Healthcare, Education, Payment Processing, Casinos/Gaming and Public Entities, market conditions may deteriorate swiftly. The prevalence of wrongful collection, biometric privacy and pixel tracking exclusions may become more widespread as we continue to try to negotiate those coverage restrictions out of placements.

At the same time, underwriters will be using previous loss data to set rates and determine coverage limits. But in this market, sometimes what happened in the past doesn't necessarily matter. Threat actors are always developing new ways to attack and capture data so security protocols must be adapted.

The Department of Homeland Security recently published a report stating that 2023 is poised to be ransomware attackers' second most profitable year. Why? Because threat actors have increased their use of multilevel extortion and targeting of large organizations, focusing on entities perceived as the most vulnerable or likely to pay the ransom. We've also seen the rise of intermittent encryption, where the attacker encrypts a system faster to reduce the chance of being detected.

Additionally, the recent MGM breach shows just how critical a role humans can play in these attacks – despite the most robust security controls. Allegedly, all it took was a 15-minute call, a quick LinkedIn search, and the attackers had access to the organization's help desk.

Insureds looking for ways to improve cyber defense measures should contact their carrier to determine what cyber security assessment services are available to review their security controls and help them implement changes so they are set up for their next renewal.

Almost every carrier offers complimentary services to help insureds improve their cyber security measures, including frequent external network scans, MFA tools, employee training and more.

Amwins offers our clients discounts on with industry-leading cyber security service providers, including CloudStrike, ePlace Solutions and SentinelOne. **You can learn more here.**

Takeaway

When you consider the fact that there are more than 200 carriers that offer some form of cyber coverage and a cyber form can have anywhere from 10 to 13 coverage agreements, it's daunting. We know you don't have a lot of time to become familiar with and work with all those forms – we do it for you.

The cyber specialists at Amwins are experts. Working with these forms day in and day out, we understand the different structures as well as the many coverage agreements. We are constantly working to develop enhancements and helping to ensure that your client doesn't have any coverage gaps from year to year. And, while pricing remains attractive in cyber, remember cheapest definitely isn't always the best.

Contact your Amwins broker to learn more.

About the Authors

- Gordon Gray, SVP with Amwins Brokerage in New York, NY
- Megan North, EVP with Amwins Brokerage in Seattle, WA
- Steve Vallone, EVP with Amwins Brokerage in San Francisco, CA