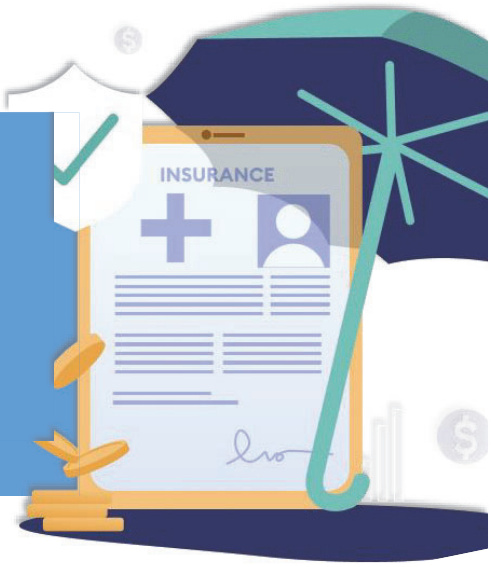
Sunshine and Cyber Insurance



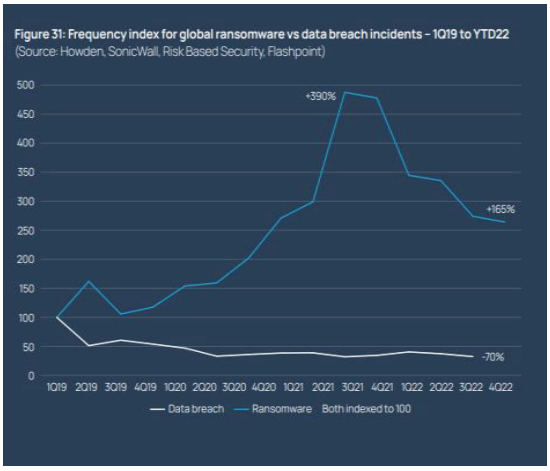
Kara Altenbaumer-Price
Senior Vice President
McGriff Executive Risk Advisors

Natalie DuBose
Insurance Recovery Partner,
Haynes and Boone, LLP

1

State of The Cyber Market: 2023

> **"The U.S. standalone cyber market currently insures an estimated $670 billion in exposure for $7.6 billion in premium."**
>
> **-CyberCube, cyber risk modeling firm**



Breach Environment

Distracted threat actors

1H22 saw tapering of US cyberattacks possibly due to Russia concentration against Ukrainian targets; trend did not hold into second half of year.

Ransomware resumes

Threat actors more than caught up with past volume as ransomware attacks increased in back half of 2022; extortion demands on the rise and threat actors using social media posts to shame victims into paying. Banks reported $886m in ransomware payments in 2022.

Focus on Attacking OT

Threat actors persist in attacking operation technology (OT) for reconnaissance and to test efficacy of novel exploits such as next generation malware of Stuxnet, BlackEnergy, Crash Override and Triton.

Cyberwarfare

Detrimental impact to victim countries from cyberwarfare and other collateral damages to companies remain a major concern for all policyholders as insurers seek to impose exclusions for cyberattacks originated by nation states.

Systemic Risk/Widespread Attacks

Attacks against tech vendors with large client base (MSPs, AWS, etc.) present significant single point of failure risk to underwriters.

McGriff

2

2023 Cyber Insurance Market Dynamics

Worsening Threat Trends	Expanding Regulatory Issues	Cyber Market Forecast
Data Harvesting News Corp attacked by Chinese APT group; data theft likely for espionage or to launch subsequent attack(s).	Illinois BIPA Litigation intensifies following the $248m in statutory damages the jury awarded against BSNF; underwriters requiring biometric applications and limiting coverage with regularity.	Retentions Overall, self-insured retention levels for most clients have stabilized. Additionally, cyber insurers are offering more meaningful premium savings in return for clients taking on higher retentions.
System Outages Hackers successfully take online booking system offline at IHG, parent company of Holiday Inn, Crown Plaza and Regency Hotels.	Momentum at State level States are following CA, VA, CO, CT and UT in proposing new privacy regulations adding to the complex patchwork of privacy laws and regulations to which companies must adhere.	Premium Although cyber premium levels increased through 1H22 (ranging from from 30-80% increases), in 2H22 premiums stabilized due to improved underwriting results and competition from excess markets. Many 4Q22 renewals saw single digit to modest increases, a few enjoyed flat renewals.
Pixel Litigation Meta Platform and large hospital and healthcare providers face privacy litigation for not notifying and getting consent in the scraping and transmittal of PHI/PII from patients using websites, and patient portals.	Wrongful Collection Increased scrutiny around company and vendor practices in notifying and obtaining consents from employees and consumers regarding the collection of various forms of non-public information, search patterns, and preferences.	Future Rate Influences Expect underwriting questions linked to what carriers are learning from recent losses; insureds overutilization of service accounts with domain admin privilege(s) continues to be a problem for many insurers; heavy emphasis on data inventory management and purging legacy data.
Phishing of Intel for Invoice Manipulation Denso Corp (Toyota Motor Corp) suffered system breach that allowed hackers to get invoicing details, along with internal email correspondence and purchase orders, presumably to be used in future social engineering schemes.	Federal Reg Scrutiny SEC, FTC, DOJ and other regulatory authorities are becoming more aggressive in investigating company breach response efforts and maintaining proper security controls and information security best practices.	Coverage Prognosis Broad coverage still available although carriers cautious about overexposure to contingent business interruption and system failure losses. BIPA and Pixel exclusions commonplace. Markets managing limits for systemic risk.
Trade Secret Theft Hacking group, Lapsu$ threatened to leak stolen data from Nvidia (largest semiconductor chip manufacturer); exposed employee login credentials and other sensitive data on the dark web.	Doctrine of Standing Decisions in Spokeo and TransUnion cases set a high bar for class certification for data breach cases where there is no significant harm to the victims; several cases in 2023 will challenge precedent potentially opening the flood gates.	Reinsurance Pressure Reinsurers demanding carriers clean up "silent cyber" exposure on other lines of coverage; reinsurance treaties in London will follow LMA rules regarding war exclusions.

Past & Present Cyber Insurance Market Snapshot

Overall Cyber Insurance Market

- After 18 months of a hard cyber insurance market where premiums increased 100-300% through 2021, another 30-80% in the first half of 2022, we finally saw relief in Q4 2022 where premiums largely stabilized. Most renewed with either a small increase or no increase over expiring.
- Retentions have also largely stabilized, and finally, cyber insurers will offer meaningful premium savings in return for increased self-insured retentions, something we largely did not see in the past 18 months.
- Excess Capacity & Increased Limit Factor (ILF): excess competition is abundant with new capacity entering the market. Where insurers were oftentimes limiting their capacity deployment to $5m lines in 2021, those same carriers are looking to increase lines to $10m. Overall market capacity is robust.
- Underwriter's expectations regarding strong InfoSec controls remain of utmost importance. For example, Beazley will update their underwriting requirements every 60 days. (See appendix for up-to-date and detailed underwriting meeting expected questions). Unchanged position that underwriters will outright decline a risk if controls are deemed poor.

Coverage Challenges

- Ransomware Exposure: if insured(s) completes the RW Supplemental and maintains strong InfoSec controls, insurers are no longer imposing sub-limits nor co-insurance for RW coverage.
- Russia, Ukraine, Belarus: as the conflict continues, insurers want to understand insured's exposure along with insured's technology partners. Where insured or tech partners have servers and operations in these countries, insurers may impose an exclusion if exposure deemed to be significant.
- War Exclusion (see following slide)
- Coverage for Operational Technology: several carriers will now require OT Supplemental(s) to be completed, and expectations that strong controls around IoT and ICS are in place.
- Coverage for Wrongful Collection: not a given and being offered by fewer and fewer markets.

Underwriting Information Requirements:

- Cyber Renewal Application
- Ransomware Supplemental Application
- Operational Technology Supplemental (if applicable)
- Biometric Data Collection Application (if applicable)
- Wrongful Collection Supplemental (AIG Only)
- Underwriting Meeting / Call (expect follow up questions)

2023 Cyber Trends

Trend to Watch	Explanation	Potential Impact
Federal Regulators sharpen oversight and enforcement efforts over corporate security breaches	FTC investigation and eventual criminal case against former UBER CISO, Joe Sullivan, indicates increased pressure on company executives to be fully transparent with authorities regarding data breaches and corporate response efforts.	Questions remain on what is "material" for disclosure purposes and potential criminal and/or personal liability for under-reporting could lead to over reporting and other unintentional negative consequences (worsening loss ratios and increased premiums).
Lloyd's of London leads push to exclude state-sponsored attacks from cyber coverage	The Lloyd's Market Association (LMA) is requiring its syndicates (primary, excess and reinsurers) to clarify coverage limitations for cyberattacks that are part of war operations, have major detrimental impact on essential services and security defenses of the country where the victim(s) are located, and can be attributed by government authorities or reasonable presumption.	Poorly worded and overly broad exclusions can swallow coverage that policyholders felt was key to their cyber insurance purchasing decision. Expect more litigation with respect to the invocation of new war and other narrowing exclusions. Regardless of coverage restrictions, Howden Group still expects premiums in the global cyber insurance market to more than double to $25B by 2026.
Extortion Groups resort to any measure to get the victim's attention and extortion payment	In addition to freezing systems/data with illicit encryption methods and launching Denial of Service attacks, threat actors further increase pressure on victim companies by publishing stolen data on social platforms like YouTube and Twitter.	Ransomware will continue into 2023 and extortion payments will likely increase as victim companies fall prey to shaming schemes. Experts caution that these criminal rings cannot be trusted, and companies should refuse payment. Immutable and tested back-ups can help reduce period of disruption, but steely grit (and wise counsel) is required to deal with consequences of not paying criminals.
Breach Reporting Rules Expand	The FTC, SEC, Cybersecurity and Infrastructure Security Agency (CISA), and NY Dept of Financial Services are each working on ways to add to the existing patchwork of state and federal rules for breach reporting.	Clients and their breach counsel already struggle to piece together varying reporting obligations; imposing tight deadlines (48 hours) to report security incidents may result in errors or misstatements when forensic facts remain under investigation and discovery; proponents for new regulations are hopeful they will include safe-harbors and incentives to bolster cyber security measures.

2023 Privacy Trends

Case Type	Litigants	Privacy Allegations	Implications
Website Tracking	Javier v Assurance IQ LLC Popa v Harriet Carter Gifts Inc	Session replay software and chat bots alleged to be "eavesdropping" in violation of California and Pennsylvania state wiretap laws.	Companies must obtain prior express consent from all parties to communication before recording (California and Pennsylvania) and that websites cannot track users' scrolling, typing and other interactions with the site without first obtaining their explicit approval (Pennsylvania). Plaintiff's Counsel noted that having wiretap law at its disposal (in addition to other state privacy laws) provides a "greater level of certainty and solid foundation for the adequacy of these claims." In short, expect much more of these claims.
Meta Pixel	Anonymous Maryland hospital v Meta (in re Meta Pixel Healthcare litigation)	Complaint alleges that the defendant knowingly or should have known that the web tracker is being improperly used on websites resulting in Facebook receiving such data when a person registers as a patient, signs into a portal or sets an appointment. Additional claims against H&R Block, TaxAct and TaxSlayer filed making similar allegations	Cyber insurers asking specific underwriting questions around policyholder usage of pixels and privacy practices utilized to protect patients/consumers; cyber insurer(s) mandating specific pixel exclusions. Dept of Health and Human Services has also issued a bulletin Dec 1 stating that regulated entities are not permitted to use tracking technologies if such would allow impermissible disclosure of protected health information to tracking technology vendors. Expect this issue to dominate headlines in 2023.
Meta Pixel	Doe et al v Meta Platforms Inc as well as various defendants using the code. (The Atlantic, ESPN, Warner Bros Discovery Inc, the NBA, and Paramount Global)	Alleged violation of Video Privacy Protection Act of 1988 by disclosing private information related to users' viewing habits to Meta via the pixel tool. The statute requires stand-alone consent for the disclosure of personal information that identifies an individual.	Defense counsel hoping these cases die on the vine as discovery may show that the website owners are not conducting the kind of business activity that the statute is meant to regulate nor does the underlying activity involve the disclosure of user's video content selections as prescribed under the VPPA.
Biometric Privacy	Rogers v BNSF Railway Co.	Complaint alleged that BNSF (vis a vis its vendor) had failed to secure legally required consent in the collection and usage of fingerprints for identity verification at job sites; Chicago federal jury awarded $248 million in statutory damages.	In addition to significant damage award, this case underscores importance for companies to know exactly what data it and its vendors are collecting, how they are storing and deleting such information, and how they secure and manage consent for such collection. Cyber insurers have application or supplemental questions for insureds with respect to their biometric data collection, usage and disposal practices. Many carriers will insist on full biometric exclusion, some will only cover defense costs for wrongful collection claims, few offer full coverage.

Title search: Sunshine and Cyber Insurance

First appeared as part of the conference materials for the
45th Annual Corporate Counsel Institute session
"Sunshine and Cyber Insurance"