JUNE 2023

State of the Market
Cyber Insurance

BRP
CYBER CENTER OF EXCELLENCE

A STABILIZING CYBER INSURANCE MARKETPLACE

Cyber risk and mitigation evolve rapidly—much like the technology sector itself. While the cyber security landscape remains dynamic and volatile, the cyber risk insurance market has shown signs of stabilization in the first half of 2023. The good news for insureds is that taking proactive steps to establish and maintain robust, up-to-date security controls will position your organization for a positive outcome when seeking new coverage or renewing coverage.

Key Drivers of Cyber Insurance Marketplace Trends

Insureds are generally seeing smaller renewal rate increases compared to recent years when some insureds saw increases of more than 120%. Several factors are contributing to this trend, including:

- **Growing Prevalence of Security Controls**—In recent years, companies and organizations have increasingly recognized the critical importance of cyber security and have made investments in security controls. These controls are making an impact, effectively preventing and mitigating claims activity.

- **2022 Leveling Off of Ransomware Attacks**—Ransomware remains a significant threat, but 2022 arguably saw attacks leveling off—or at least the frequency of attacks moderating. Measurements vary by geography and business size, with some analysts reporting declines in attacks for certain segments compared to 2021. This development may have helped encourage some insurers to expand their capacity for cyber coverage.

  That said, insurers will be closely watching attack trends, which are once more on the rise: March 2023 saw a record number of ransomware attacks, with North America the most targeted region. Small and midsize businesses (SMBs) are also increasingly targeted by ransomware attacks.[1]

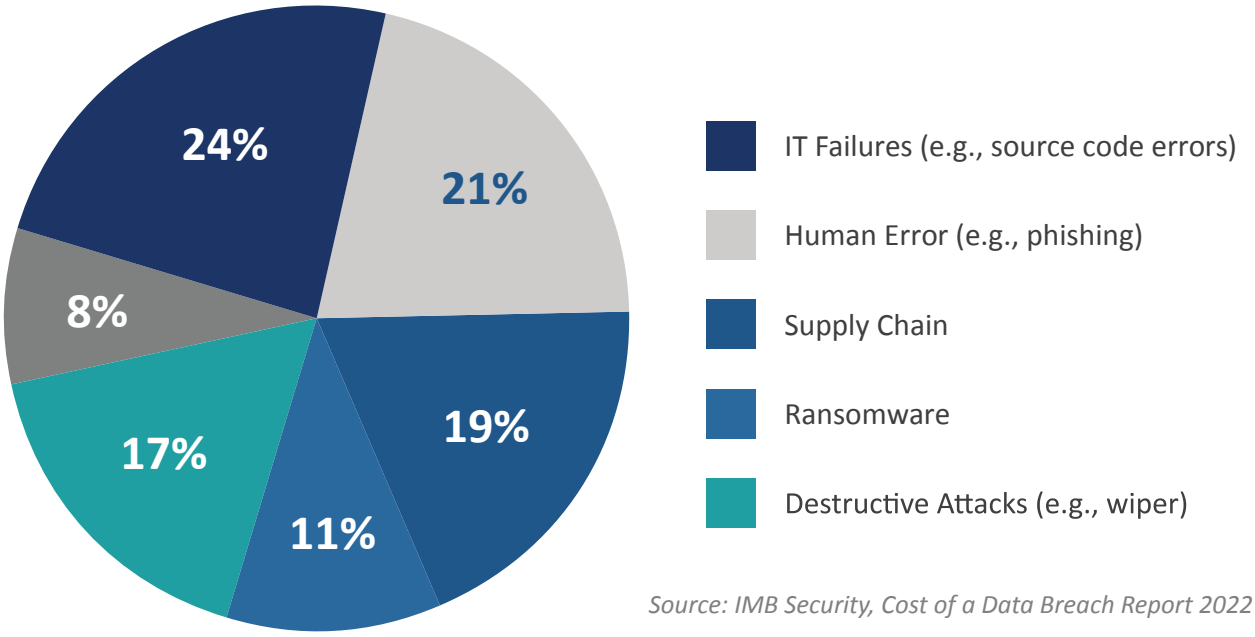
- **Healthier Loss Ratios**—The moderate improvement in the ransomware landscape combined with increased pricing has resulted in better loss ratios for carriers. Healthier balance sheets for cyber products allow insurers to expand capacity and moderate renewal rate increases.

Key Cyber Risks

- **Cyber Crime**—Cyber crime encompasses ransomware, social engineering fraud, payment fraud, data breaches, and other types of attacks. Estimates of the financial impact of cyber crime vary, but the cost is substantial by any measure. The FBI's Internet Crime Report puts the 2022 potential total loss from cyber crimes at more than $10.2 billion.[2] In one study analyzing 550 organizations from March 2021 through March 2022, the average cost to recover from a data breach in the U.S. was $9.4 million. The average cost of ransomware attacks during the same period was $4.54 million, not including the cost of the ransom itself.[3]

Healthier balance sheets for cyber products allow insurers to expand capacity and moderate renewal rate increases.

2022 Types of Breaches



Source: IMB Security, Cost of a Data Breach Report 2022

While cyber crime is the primary contributor to cyber losses, businesses face several other cyber risks or adjacent risks. Fortunately, strong operational controls can help to both mitigate these risks and earn favorable insurance pricing. Numerous services and technology solutions are available that can help address these additional risks, which include:

- **Regulatory Compliance—**There is a growing patchwork of state data privacy regulations in addition to sector-specific federal regulations such as HIPAA and FERPA and overseas regulations such as the EU's GDPR. Violation of data privacy rules may result in substantial fines. For example, BNSF Railway suffered a $228 million judgment last year for violating the Illinois Biometric Information Privacy Act (BIPA).[4]

- **PCI DSS Fines—**Any organization that accepts, processes, stores, or transmits credit card information must comply with the Payment Card Industry Data Security Standard (PCI DSS). Failure to comply with PCI DSS may result in monthly fines—imposed by card brands or acquirers—ranging from $5,000 to $100,000.[5] In addition to fines, non-compliance with PCI DSS may lead to liability for fraudulent charges, credit card replacement costs, and other consequences.

- **Business Interruption—**Downtime for a business from a cyber event can lead to substantial losses. While this type of loss is primarily associated with direct cyber attacks, it can also be a result of operational failures or a cyber incident affecting a contingent business, such as a supplier, vendor, or partner.

- **Reputational Risk—** Reputational risk also accompanies cyber risk. Companies with high-profile cyber events can incur costs to remediate reputational damage.

- **Emerging Risks, including AI—**Artificial intelligence and machine learning can contribute to strengthening cyber defenses, but these technologies are also being leveraged by bad actors for malicious purposes. In addition, businesses using AI for a range of purposes, such as generating content or surveilling customers, could face liability claims related to its use.

COVERAGE AND EXCLUSION ISSUES

While price increases in cyber insurance have stabilized, a number of issues have emerged that can potentially impact coverage and remediation from cyber attacks:

- **War Exclusions**—Cyber insurers have previously covered cyber incidents linked to nation states, despite war exclusions that are included in many types of insurance. The Russia-Ukraine War has raised the specter that insurers may invoke war exclusions to deny coverage from cyber attacks related to the conflict. Depending on policy wording, coverage could also be denied if nation-state cyber attacks cause systemic losses. Disputes about coverage may also arise because of the difficulty in attributing attacks directly to nation-state actors.

- **Panel Vendor Challenges**—As part of their coverage, many cyber insurers provide insureds with access to their panel of cyber security vendors. Under the terms of a policy, an insurer may mandate the use of their panel vendors, even if an insured has its own cyber security team and vendors who have deeper experience with the insured's IT systems and security controls. Policy terms and close communications between insureds, brokers, and insurers can help prevent these types of conflicts.

- **Application Misrepresentation**—Last year, Travelers filed suit against an insured, alleging that the company had misrepresented its security controls in its application. This type of dispute could lead to denied claims, and it makes it all the more critical that insureds work closely with their insurance advisors to provide comprehensive representations of their security controls.

While price increases in cyber insurance have stabilized, a number of issues have emerged that can potentially impact coverage and remediation from cyber attacks.

STEPS TO STRENGTHEN CYBER SECURITY AND BETTER POSITION YOUR RENEWAL

Simply put, there is a strong correlation between security controls and the frequency and severity of losses. Businesses and organizations can best position themselves for favorable outcomes in today's cyber insurance marketplace by taking a number of steps to harden their cyber defenses. Meeting insurers' security expectations can result in lower renewal costs and favorable policy terms. Your cyber risk advisor can serve as a valuable resource for evaluating and enhancing your security controls.

Proactive Cyber Controls

Carriers will be looking for robust security controls as they evaluate new applications and renewals. Key controls that will impact insurability, mitigation, and resilience include the following:

- **Multifactor Authentication (MFA)—**If not already implemented, your organization should strongly consider establishing MFA for access to technology systems, services, data, and email. MFA is especially important for remote access, access to mission critical technology, and access to confidential and proprietary data. MFA requirements should apply to employees, contractors, and third-party service providers.

- **Monitoring and Prevention Tools—**Cyber security can be strengthened by utilizing a number of monitoring and prevention tools, including:

    a. **Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR)—**EDR has long been one measure favored by insurers, but its scope may now be limited. XDR casts a wider net—to email, server, cloud applications, and other layers—to detect attacks. The use of XDR speeds response time, which in turn can significantly shorten the breach lifecycle.

    b. **Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)—**These network security tools monitor systems for malicious activity.

    c. **Protective Domain Name Service (DNS)—**Protective DNS analyzes queries to the internet's Domain Name Service and blocks malicious inquiries based upon their database of sites with known malicious content.

    d. **Security Information and Event Management Tool—**This type of software aggregates and analyzes IT infrastructure data to discover trends, detect threats, and enable organizations to investigate any alerts.

    e. **Email Filtering—**A number of tools are available to monitor email for red flags and route suspicious email for analysis, quarantine, and deletion.

    f. **Privileged Account Management—**This security strategy entails managing accounts with elevated permissions and controlling the use of those accounts.

    g. **Hardened Baseline Configuration—**This is an operational framework that sets security standards and baseline requirements for each system individually.

- **Encrypted Backups—**It's critical for recovery to maintain backups in secure, offsite locations, including via cloud services. Because backups themselves pose a cyber security risk, they should be encrypted.

TRAINING AND PLANNING

Insurers will also be looking for organizations to take operational steps to reduce cyber risk, including:

- **Cyber Security Training—**Human error is a significant vector for cyber attacks. Regular training and testing can help mitigate this risk. Organizations can further strength cyber security by providing or requiring cyber training for partners and vendors.

- **Incident Response Planning—**Developing, regularly testing, and updating a detailed incident response (IR) plan can significantly help lower the costs and impact of a cyber incident. The plan should lay out specific steps for responding to cyber crimes, data loss incidents, and service outages.

Challenges for Cyber Insurance Programs

As you prepare to establish or renew a cyber insurance program, be aware of the following challenges:

- **An Increasingly Arduous Application Process—**In years past, applying for cyber insurance was a relatively easy and brief process. This is no longer the case. Organizations must provide extensive, detailed, and accurate information on their IT systems and security controls. In some cases, in-house personnel may lack the expertise to complete applications. Your cyber risk advisor can serve as a key partner in developing a comprehensive renewal submission.

- **Higher Deductibles and Retentions—**Renewals may require substantial increases on deductibles or retentions. Carriers may also impose sub-limits for certain types of losses.

- **Restrictions on Systemic Risk—**Carriers are increasingly placing restrictions on coverage for systemic risks that could result in outsized and cascading losses. These restrictions apply to:
    a. **Aggregation Risk—**when all clients of an insured may be catastrophically affected.
    b. **Widespread Event Risk—**when a single point of technology failure, such as a zero-day vulnerability, results in widespread impacts.

- **Restricted Technology E&O Capacity—**While capacity challenges are less of an issue for general cyber policies, capacity is constrained for technology errors and omissions (E&O) coverage.

- **Renewal Time Requirements—**Given the complexity of the application process and the demand for cyber coverage, companies should begin to consider renewal options at least 120 days before their current policy expires. It's especially important to communicate early with broker partners on your renewal strategy and coverage options.

REACH OUT TO THE BRP CYBER TEAM

Collaboration is critical to mitigating cyber exposure. Evolving cyber risk requires companies to coordinate preventive measures companywide, utilize the best security controls, and work closely with trusted partners in the cyber security community.

The BRP Cyber Team has the experience, expertise, and industry reach to help organizations make the most of the stabilizing cyber insurance market. As a highly secure, trusted partner, we work closely with clients nationwide to identify risks, enhance security controls, and explore the fullest range of insurance options.

To learn more about the BRP Cyber Center of Excellence and how we can help you develop strategies to mitigate cyber risks, please reach out to a member of our team.

Emily Selck
312.508.2501
emily.selck@baldwinriskpartners.com

Emily Short
913.593.9006
emily.short@baldwinriskpartners.com

BRP
CYBER CENTER OF EXCELLENCE

1 NCC Group, Monthly Threat Pulse – March 2023.

2 Federal Bureau of Investigation, Internet Crime Report 2022.

3 IMB Security, Cost of a Data Breach Report 2022.

4 Hunton Privacy Blog, "First Ever BIPA Trial Results in $228 Million Judgment Against BNSF Railway," Oct. 19, 2022.

5 PCI Compliance Guide, PCI FAQs.