Cyber Liability – Proactive Risk Management In An Evolving Market

Alliant Insurance Services

Seth Cole, Senior Vice President Public Entity

Sedgwick

Jon Paulsen, Vice President Self-Insurance Pooling

AGENDA

1. The Cyber Liability Insurance Market
2. Underwriting Requirements
3. Resources and Support Services
4. When An Incident Occurs
5. Take-Aways
6. Q&A

THE CYBER LIABILITY INSURANCE MARKET

What is Cyber Exposure?

Cyber exposures are directly connected to the responsibility an organization has for certain electronic information and the risks associated with this information being compromised or misused.

These risks include, but are not limited to privacy notifications, cyber extortion payments, intellectual property infringement and financial injury, as well as obligations associated with Consumer Protection and Data Privacy Regulations.

First Party Risks

Third Party Risks

Understanding Cyber Insurance

It's Data, Data Privacy and Computer Equipment Insurance
(First Party, Third Party and "Other")

First Party

- Protection for Loss of My Data
- Business Interruption From Unauthorized Access Which Affected My Computer or Data
- Protection for Damage to My Computer

Third Party

- Liability For Losing Someone Else's Data
- Liability From Information Posted on My Website
- Government Fines for Not Complying to Specific Regulations
- Payment Card Fines For Non-Compliance

"Other"

- Costs to Let People Know We Lost Their Data
- Costs to Have Help Understanding the Most Recent Data Privacy Laws in Every State and Internationally
- Costs to Have Help Navigating the Messaging to Put Forward
- Recovering Money Lost in a Fraudulent Email that Caused a Transfer of Money

Cyber Coverages

Breach Response

- Legal Services
- Forensics
- Notification
- Credit Monitoring
- Public Relations/Crisis Management

First-Party

- Business Interruption
- Cyber Extortion
- Data Restoration
- eCrime
- Bricking
- Cyrptojacking
- Reputation Loss
- Criminal Reward

Third-Party

- Data and Network Liability
- Regulatory
- Payment Card
- Media Liability

State of the Market

- Financial Impact of Cyber Crime
  - Cyber crime estimated at $8.4 trillion in 2022
  - Projected to hit $10.5 trillion annually by 2025
  - Was approximately $2 trillion in 2019
  - Global cybersecurity spend over the next 5 years expected to exceed $1.75 Trillion
  - Costs of notifications in data breach
    - $5 - $25 per individual

Sources: https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5
Cost of notifications: Baker Hostetler discussion with Alliant

State of the Market - Statistics

- A consumer or business suffered a ransomware attack every 11 seconds in 2021…expected to drop to every 2 seconds by 2031!
- Ransomware is now the fastest growing in frequency and severity of claims for insurance companies
  - Largest cyber extortion demand +$40M
  - Largest cyber extortion payment +$40M
- World population on the internet is about 75%..expected to grow to 90% by 2030
- The cyber security insurance market is expected to reach $15BN in 2025

* SOURCE: 2022 Cybersecurity Almanac

Cyber Conditions

Capacity

Carriers have been extremely conservative with their deployment of capacity. As an example, many cyber insurers have cut their available capacity from $10 million down to $5 million.

Pricing

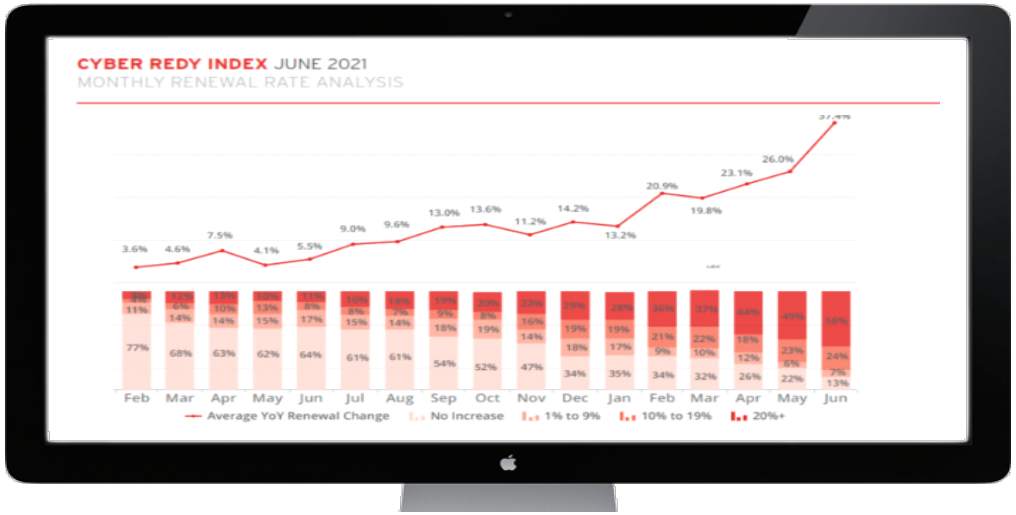
Abrupt pricing correction due to the uptick in severity of claims. Market leaders have consistently secured primary increases of
15% – 200% on their renewals during 2022.

Coverage

Coverage generally remains intact for public entities with mature information security programs and strong operational resilience. However, leading Primary carriers are pushing for up to 50% co-insurance provisions or other coverage restrictions for ransomware losses where companies are less secure.

Retentions

Excess markets are following Primary increases and in many cases are pushing
for higher percentage increases on certain attachment points. Continued pressure on primary retentions and waiting periods for business interruption losses.



Targeting Public Entities

Percentage of US and UK companies feeling 'very prepared' to anticipate and respond to cyber risk in 2021.
Median line indicates the mid-point of the data set across all industries surveyed.

Cyber Liability Insurance Market Challenges & Impact

- We are in a challenging cyber insurance market
- The industry loss ratio is improving - 75% at the height
- Combined ratios in excess of 100% (loss + expense)
- Driving premium increases and changes in coverage
  - Lower capacity deployment
  - Increased self-insured retentions
- Requiring evidence of security posture
  - MFA
  - Data Backups
  - Employee Education & Training Programs

UNDERWRITING REQUIREMENTS

Scrutiny ratchets up of companies' cyber insurance, practices

Underwriters now take a fine-toothed comb to commercial cybersecurity practices, and regulators are starting to do the same.

By **Walter Andrews, Andrea DeField and Sima Kazmir** | January 18, 2022 at 12:05 AM | The original version of this story was published on **Daily Business Review**

Ransomware Attacks Continue to Cause More Underwriter Scrutiny

Robin Fischer

Senior Vice President, Risk Management & Cyber Liability

DECEMBER 6, 2021

CYBER LIABILITY

Cyber Liability Underwriting – New Standards

- Multi-factor authentication - 100% implemented for remote access, laptops, and privileged access
- End-point protection, detection, and response product implemented across enterprise with 24/7/365 response
- If Remote Desktop Protocol connections enabled: VPN access only, MFA for access, Network level authentication
- Backups: 1 working copy, 1 offsite (disconnected not working), 1 onsite disconnected, tested at least twice/yr, ability to bring up within 24-72 hrs, protected with antivirus or continuously monitored

Cyber Liability Underwriting – New Standards

- Planning & Policies: Incident Response Plan, Disaster Recovery Plan, Business Continuity Plan
- Training: Social Engineering Training, Phishing Training, training of accounting team staff on fraudulent transactions, and general cyber security training for all personnel
- Email security protocols in place
- Plan or have adequate measures in place to protect end of life software

Cyber Underwriting – Challenging Responses

- **Multi-Factor Authentication:** If not a hard requirement already, this is becoming a required best security practice
- **Network Segregation / Segmentation (Compartmentalization):** Increases security through access limitations, traffic isolation, restriction of movement throughout the network
- **Employee Training and Education:** User error and susceptibility continue to be the leading cause of security breaches
- **Penetration (Pen) and Vulnerability Testing:** Insurers often running testing on external sites on their own

RESOURCES AND SUPPORT SERVICES

Available Resources and Support - Insurers

- **Breach Response Services**
  - Have this (800) and email contacts pre-loaded and available
  - Key breach vendors: Legal Services (PR, notifications, regulators), Forensics
    - Consider pre-designated contacts and relationships
- **Online Resources**
  - Training and online learning, training material
    - Incident response planning and samples
  - Threat and resource updates
  - Discounted Partner Rates (e.g. KnowBe4, RSA, etc.)

Governmental Resources

- **Cybersecurity & Infrastructure Resources**
  - www.cisa.gov/free-cybersecurity-services-and-tools (31 pages of resources)
  - System and website vulnerability scanning, penetration testing
  - Phishing awareness training, self-evaluation tools
  - Cloudfare, Microsoft Defender and BitLocker, Android Quad9, etc. tools
- **Department of Homeland Security**
  - Now providing support primarily through CISA above
  - Grant Program available

Cyber Security Vendors – Identify Your Need

- **What Type of Specific Support Do You Need?**
  - Underwriting compliance?
  - Technology updates/enhancements, general technology consulting?
  - Communications, crisis response, compliance
- **Vendor Market is Evolving Very Quickly**
  - Vendor due diligence
  - Network with peer risk managers

Cyber Security Vendors – Sample Listing

- K12 SIX (www.k12six.org)
- KYND Ready (www.kynd.io)
- Lodestone www.lodestone.com
- Progent (www.progent.com)
- ResoluteGuard (www.resoluteguard.com)
- VC3 (www.vc3.com)

Do you need to consider developing internal resources?

WHEN AN INCIDENT OCCURS

When An Incident Occurs – The First 24 Hours

- ***Notify your insurance company*** of any suspected data breach, security breach, cyber extortion threat or system failure
- Secure your IT systems
- Mitigate
  - Try to preserve all evidence pertaining to the incident
    - Memories fade
    - Emails get lost or deleted
- Communicate, Coordinate, & Execute with your insurance company

SELF-INSURING THE RISK

Zurich Insurance CEO: Cyberattacks Will Be 'Uninsurable'

BY **PYMNTS** | DECEMBER 26, 2022

As cyberattacks grow, they will become “uninsurable,” the CEO of Europe’s Zurich insurance said.

Why Are We Self-Insuring Cyber?

- Some entities are simply not purchasing the coverage
- Higher and higher deductibles/retentions
- Lower limits and sub-limits
- Tightening of coverage. Implementation of exclusions.
- Non-renewals

Why Are We Self-Insuring Cyber?

- Are we being pro-active or reactive?
- Do we have a self-insurance fund in place to pay for losses like other lines?
- Do we have comprehensive training to avoid losses?
- Do we have regular and secure backups?
- Are Incident Response, Disaster Recovery, and Business Continuity plans in place?

Remember to plan for Communications and IT Resources to be down

TAKE-AWAYS

What Can We Be Doing Now?

- Risk assessment: self-assessment, third party, insurer
- Hardened security
- What would you need to take more risk if necessary?
- Pre-contract key vendors? (from approved insurer lists)
- Crisis management planning (including RM representation)
- This will be a continuous, ongoing process

THANK YOU

QUESTIONS FOR DISCUSSION?

Alliant Insurance Services

Seth Cole, Senior Vice President Public Entity
scole@alliant.com
(415) 403-1419

Sedgwick

Jon Paulsen, Vice President Self-Insurance Pooling
jon.paulsen@sedgwick.com
(916) 244-1154

Complete Session Surveys on the App

Find the App, Click on Events, Click on Browse by Day, Click on the Specific Session, Click on Rate Event.