Brown & Brown

Cyber and Data Security: Claims, Coverage and Marketplace Trends

Presented By:
Brown & Brown Cyber Team

Brown & Brown Insurance Services, Inc.

Presentation Agenda

1. Claim Issues and Trends
2. The Role of Breach Counsel
3. Policy Placement Issues in the Marketplace
4. Q&A

Panelists

Aaron Stone
Brown & Brown, Moderator

Eric Olson
Brown & Brown, Panelist

Shari Keiser
Starr Companies, Panelist

Jennifer Coughlin
Mullen Coughlin, Panelist

01 Claim Issues and Trends

Claim Issues and Trends

Incidence and Types of Claims

- Ransomware
  - 2023 a “record breaking” year- estimated up to 7,600 impacted organizations
  - More active criminal groups: 47 up from 35 in 2022
  - Average cost rose to $5.13M in 2023, a 13% increase from 2022
- Social Engineering
- Business email compromises

Industries Impacted

- Size of Target
  - Companies with $100M+ in annual revenue prime targets
  - Companies with $25M-$100M in annual revenue saw significant increase in frequency
- Type
  - Healthcare, Energy, Professional Services, Manufacturing and Construction
  - Law Practices and Transportation, Logistics and Storage were prime ransomware targets in 2023

Losses

- Breach Expenses, Ransom payments, Business Interruption (Direct and Contingent)

Claim Issues and Trends

Third-Party Vendor Breaches

- What are they?
- How do carriers adjust them?
- Immediate impacts
  - » Notification obligations
  - » Contingent Business Interruption
- Contractual obligations/Subrogation Opportunities

Recent Claims

- SolarWinds
- MOVEit Transfer
- Change Healthcare

Emergence of AI

- What are possible impacts?

Claim Issues and Trends

Claim Process

- Reporting
- Role of Adjuster
- Communication with Insured

Common Coverage Issues

- Use of Panel v. Non-Panel Vendors
- Covered v. Non-Covered Loss (e.g. restoration v. betterment)
- Ransom: to pay or not to pay?
- Business Interruption Damages
  - » Does Policy afford Claims Preparation Costs
  - » Definition of Business Interruption Loss
  - » Waiting Period/Period of Indemnity
  - » Adjustment Process

02

The Role of Breach Counsel

Breach Counsel

Legal Purpose

- Attorney Client Privilege/Attorney Work Product Doctrine
- Regulatory compliance advice

Coordination of Vendors

- Project management
- Facilitation of vendor engagement for forensics, ransom negotiation/payment, network restoration, data mining, public relations, etc.
- Facilitation of prior approval of expenses from carrier

Notification advice and assistance

- Assessment of consumer and regulatory notification obligations
- Drafting of statutorily compliant notification letters
- Facilitation of vendor engagement for notification and remediation services such as credit monitoring and identify theft insurance

Communication with carrier and insured

- Establish cadence of communication
- Ensure all stakeholders are appropriately informed of status of matter and key decisions throughout the process

Breach Counsel

Pre-incident Mitigation Actions

- Incident response planning
- Tabletop exercises to test the incident response plan
- Conduct gap analysis of data privacy and information security programs
- Defend against evolving malicious technology and behavior
  - » Maintain conventional layered defense
  - » Maintain and test backup systems
  - » Prioritize security patching
  - » Implement multi-factor authentication to email platform, network and core applications
  - » Implement heuristic-based endpoint detection and response tools and monitor 24/7 for malicious behavior
  - » Strong password management
- Conduct third party contract review for liability related to data privacy and information security provisions; ensure inclusion of appropriate defense and indemnification language
- Update data privacy policies to account for evolving state legislation
- Update information security policies and procedures to incorporate evolving defenses

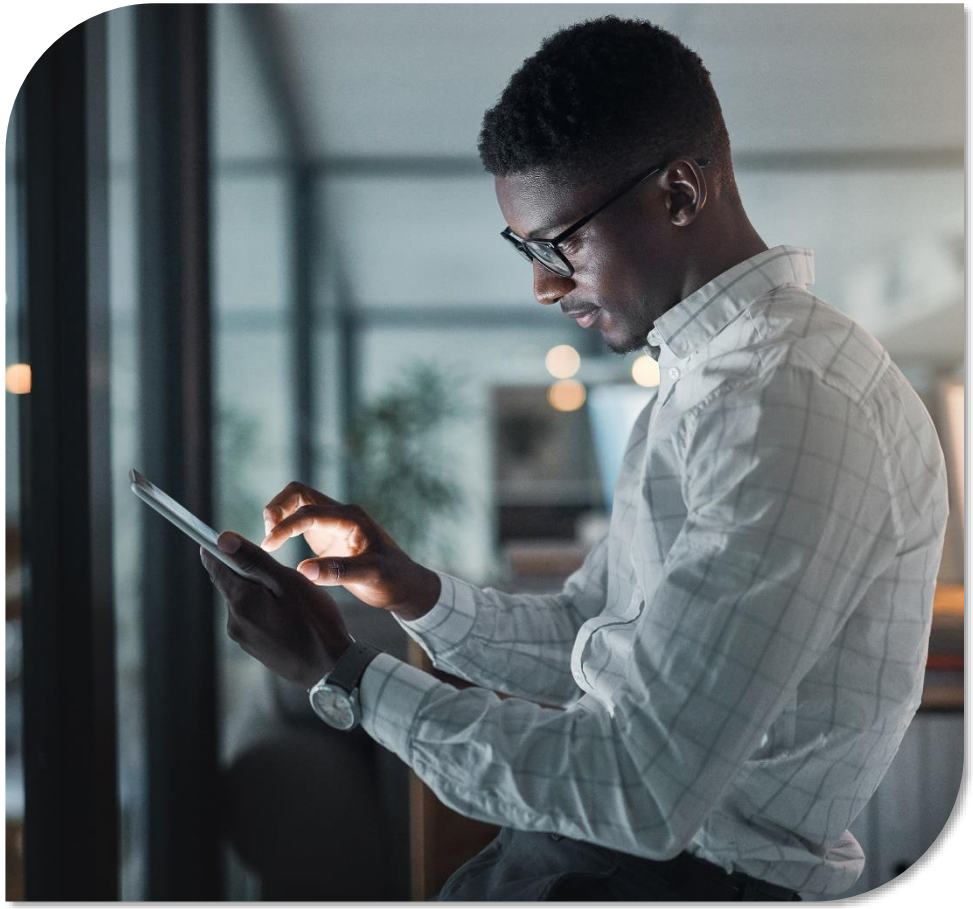
03

Policy Placement Issues in the Marketplace

Placement Issues

Rates in the cyber market are stabilizing on primary policies, currently averaging a reduction of 1% to 5% with even greater competition on layered programs.

- Increasing capacity, which is furthering the softening on pricing
- Frequency of cyber claims are still increasing, specifically for:
  - » Professional Services
  - » Education
  - » Manufacturing
- Carriers are closely monitoring privacy claims
  - » In many cases, they are adding language to clarify intent or narrow their coverage



Placement Issues

Underwriting standards remain high, with most carriers requiring the following controls to offer terms:

- Multi-factor authentication (MFA)
  - » All remote access (both employee and third party)
  - » All privileged user accounts, including when on premises
- Endpoint detection and response (EDR) on 100% of endpoints, including BYOD if able to access the network
- Strong backup procedures and policies

Additional Underwriting Standards

- Local administrative rights not granted outside of technology/security staff
- Patching cadence, specifically for critical and high/important severity patches
- End-of-life software and compensating controls
- Security Operations Center (SOC)
  - » Carriers prefer 24/7 coverage and do not have a preference for in-house vs third-party
- Operation Technology (“OT”) Issues
  - » Segmentation of OT environment from IT environment
  - » Segmentation of OT environment from internet

04

Questions & Answers

Brown & Brown

Find your solution at **BBrown.com**

Any solicitation or invitation to discuss insurance sales or servicing is being provided at the request of Hays Companies, Inc, an owned subsidiary of Brown & Brown, Inc. Hays Companies, Inc. only provides insurance related solicitations or services to insureds or insured risks in jurisdictions where it and its individual insurance professionals are properly licensed.