



Cyber and Data Security: Claims, Coverage and Marketplace Trends

Presented By:
Brown & Brown Executive Risk Team

*Hays Companies, Inc., an owned
subsidiary of Brown & Brown, 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



David Wasson

Brown & Brown, Panelist



Theresa Le

Cowbell, Panelist



Sean Hoar

Lewis Brisbois, Panelist



01

Claim Issues and Trends

Claim Issues and Trends

TYPES OF COVERAGE

First Party

- Data Breach
- Ransomware
- Social Engineering
- System Failure
- Data Restoration
- Business Interruption
- Contingent Coverage

Third Party

- Liability
- Payment Card Industry
- Media Liability

Claim Issues and Trends

- **Incidence and Types of Claims**

- » Overall increase in frequency of 743% since 2012.
- » Ransomware
 - Average demand \$1.8M
- » Social Engineering
- » Liability

- **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

- **Losses**

- » Breach Expenses
- » Ransom
- » Business Income



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
 - » Period of Indemnity

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
 - » Update data privacy policies to account for evolving state legislation
 - » Update information security policies and procedures to incorporate evolving defenses



Breach Counsel- Recommended Response to Ransomware

- **You should not do the following:**

- » Do not contact the attacker;
- » Do not turn off encrypted systems;
- » Do not unplug or power off network devices;
- » Do not wipe or restore devices without preserving evidence;
- » Do not make unnecessary public statements; and
- » Do not pay ransom without consulting legal counsel.

- **You should do the following:**

- Implement incident response plan;
- Disable (not power down) affected devices from network;
- Seal off ingress and egress from the Internet;
- Contact cyber insurance broker or carrier immediately;
- Engage legal counsel immediately;
- Assessment impact;
- Inform internal stakeholders;
- Draft internal and external holding statements/messaging;
- Commence additional containment measures and forensics investigation;
- Comply with legal obligations – statutory and contractual notification obligations; and
- Notify law enforcement at appropriate time.

03

Policy Placement Issues in the Marketplace

Placement Issues

Currently in a “hard” – but stabilizing – market phase. Increased frequency and severity of loss has resulted in:

- Increasing premiums
- Increasing retentions/deductibles and waiting periods
- Decreasing capacity
 - » Micro: almost all carriers limiting capacity for individual applicants
 - » Macro: many carriers writing on a net- or negative-capacity basis
- Coverage Restrictions
 - » Ransomware sub-limits and/or co-insurance
 - » Widespread event sub-limits and/or co-insurance
 - » CVE-related exclusions, sub-limits, and/or co-insurance
 - » Reduced coverage for dependent business interruption and system failure
 - » End-of-life software exclusions
 - » War and Government-mandated shutdown exclusions
- Increasing underwriting Standards



Placement Issues

- Underwriting Standards

- » Multifactor Authentication (MFA)

- All remote access (both employee and third party)
- All privileged user accounts, including when on premises

- » Endpoint detection and response (EDR) products

- » 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

- » Backups

- » Minimal service accounts in domain admin group

- » Privileged Account Management (PAM) tool

- » Security Operations Center (SOC)

- » Operation Technology (“OT”) Issues

- OT-specific or -inclusive security policy(ies)
- OT-specific or –inclusive business continuity plans(s) with testing at least E24M
- OT-specific tabletop exercises, specifically referencing ransomware
- Segmentation of OT environment from IT environment
- Segmentation of OT environment from internet

04

Questions and Answers





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.