POOLING TODAY

PRESENTED BY AGRiP/CAJPA/NLC-RISC

What You Need to Know Now about Cyber Security

Susan Leung, Alliant

WE ENERGIZE THE POWER OF POOLING
AGRiP
ASSOCIATION OF GOVERNMENTAL RISK POOLS

CAJPA
California Association of Joint Powers Authorities

NLC NATIONAL LEAGUE OF CITIES
NLC-RISC RISK INFORMATION SHARING CONSORTIUM

Agenda

- State of the Cyber Insurance Market for Public Entities
- Claims Trends
  - By Public Entity Sub Class
  - By Location (U.S. & Canada)
- Reaction of the Cyber Insurance Marketplace
- General Insurance Coverages
- General Claims Process

State of Cyber Insurance Market for Public Entities

State of the Market

- Cybercrime projected to hit $6 trillion annually by 2021, was $2 trillion in 2019
- The cyber security insurance market is expected to reach $20BN in 2025, registering a Compounded Annual Growth Rate of 20-25%, during the forecast period (2018 – 2025)
- Ransomware is now the fastest growing in frequency and severity of claims for insurance companies
  - Largest cyber extortion demand +$20M
  - Largest cyber extortion payment +$5M
- Recent Cyber Attacks
  - Canadian government (national revenue agency) – August 2020
  - New Bedford, MA – Ransom demand north of $5M – 2020
  - Schools - 348 districts reported attacks - 2019
- New Market Entrants
  - Managing General Agencies – Limited appetite for Public Entity Pool business

Insurance Companies' Perspective/Feedback

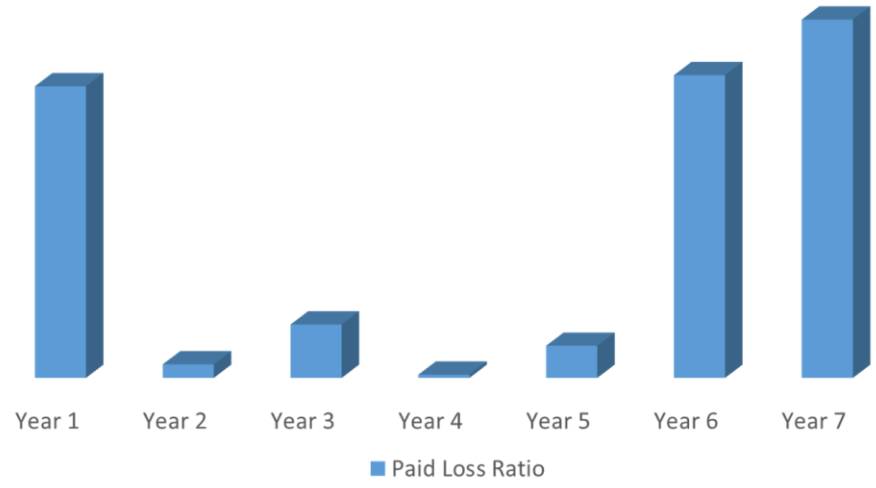
- Top 10 cyber insurance carriers (controls about 70 - 75% of the marketplace) all report an overwhelming increase in ransomware claims
  - No industry class was spared
  - Public Entity was the most successfully targeted sector in terms of penetration by the attackers and frequency
    - Amongst the least prepared due to older software/computer equipment, lack of training, low IT security budgets
- The Public Entity sector is now being viewed very closely by Insurance Company management, and continuing to tighten
  - Especially for JPAs and Pools, carriers are worried about the vast number of members with the same ransomware exposure under the same policy

Claims Trends

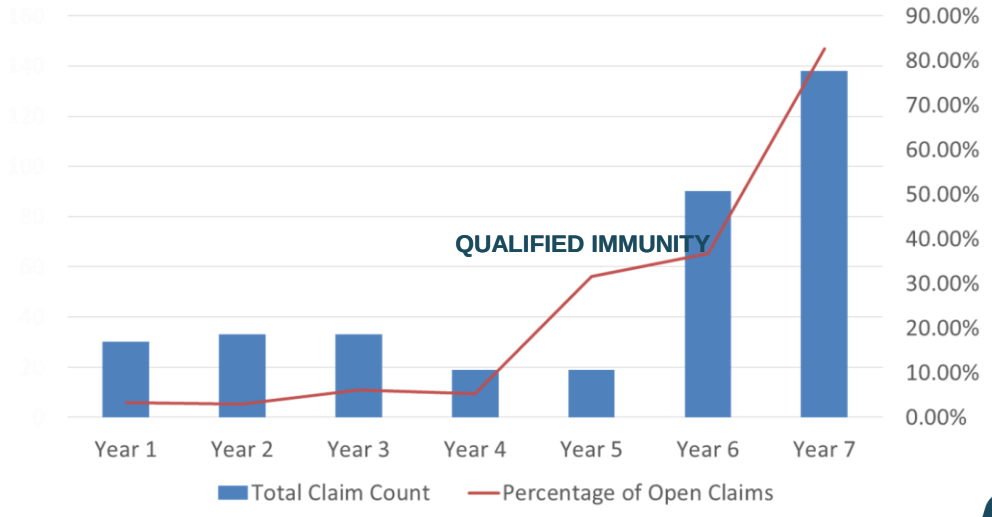
Claims Trends: By Sub Class, Location

- By Sub Class
  - Public Hospitals, Education (K-12 and Colleges/Universities, Cities and Counties are the highest frequency and severity
  - Followed by:
    - Transportation
    - Special Districts – Utilities, Water, etc.
- By Location
  - The U.S. is a target for attack more frequently than Canada
  - Within the U.S., there is no specific geography that has been spared from attacks
  - Attacks are more concentrated on sub class of public entities

Claims Trends: Paid Loss Ratio

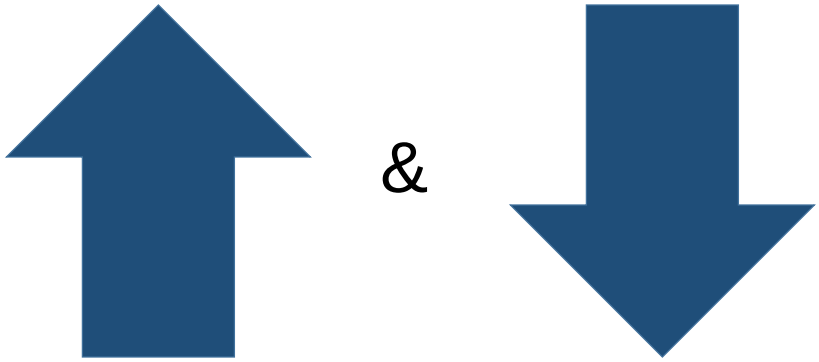


Claims Trends: Claims Count, Open Claims



Reaction of the Cyber Insurance Marketplace

Reaction of the Cyber Insurance Market



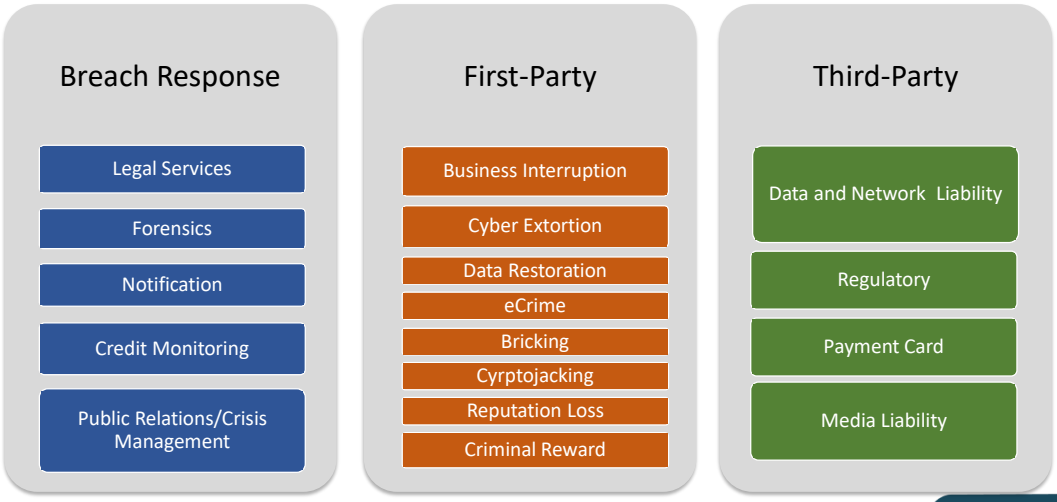
What Initial Marketplace Reaction Means

Higher	Lower
Increase in Critical Examination of Risks	Lower Capacity
Retentions	Limits/Aggregate Limits
Premiums	Sublimits
Increased Request for Information	Less Expansion of Coverage Terms
Increase in Declinations	Less Accommodations

- How long will this last?
  - Only time will tell, next 12 months are critical to watch
  - If ransomware eases up and no other new form of loss takes its place, the industry could recover quickly
- What should we keep an eye out for?
  - Naïve capacity
  - Changes in vendor services and the interactions with vendors during a claim

General Insurance Coverages

General Cyber Coverages



Exclusions (Including, But Not Limited To)

- Exclusions (Including But Not Limited To):
  - Bodily Injury
  - Property Damage (carve back for Bricking - computers or any associated devices or equipment)
  - Insured vs. Insured
  - Unlawful Collection of Personally Identifiable Data
  - Prior Known Acts
  - Betterment
  - Failure of Power, Utility, Mechanical or Telecommunications Infrastructure or Services That are Not Under the Insured's Control

General Claims Process

Notifying a Cyber Incident

When? ASAP!

- Any suspected Data Breach, Security Breach, Cyber Extortion Threat, or System Failure
- Build notice protocols into your Incident Response Plan
- Escalate systematic, reputational, and catastrophic incidents
- ***Helps preserve members' rights under applicable Policy***

Content of Notice

- Include:
  - Briefly describe incident
  - Date of incident event (if known)
  - Date of incident discovery
  - Contact information of your Breach Coordinator
- Exclude
  - Specific Personally Identifiable Information (PII) and/or Protected Health Information (PHI)

The First 24 Hours

Secure your IT systems

Mitigate

- Try to preserve all evidence pertaining to incident
  - Memories fade
  - Emails get lost and/or deleted

Coordinate

- You will be contacted by a Claims Manager
- Conference call to discuss the incident and investigation
  - Attendees:
    - Your Breach Coordinator (mandatory)
    - Key Incident Response Team members (recommended)
    - Insurance Claims Manager

General Claims Process

1 **You are here:**

Your public entity has suffered a security incident. The clock is now ticking. It's time to do right by your citizens, employees, shareholders and others. A quick, effective response may help you avoid lawsuits and regulatory inquiries.

2 Immediately gather your internal team and review your incident response plan.

Contact your insurance company

3 **Debrief Your Insurance Company.**
Some important things to cover:
- What type of event?
- Lost device?
- Malicious hacker?
- Disgruntled employee?
- What type of information?
- Where are affected individuals located?
- How many people involved?

4 **A Claims Specialist will help you formulate your response plan:**
- Engage pre-approved expert privacy attorneys to determine legal applicability of actions to respond to reporting requirements and maintain privilege.
- Engage computer forensics to determine existence, cause and scope of the breach.
- Do we need to hire a public relations or crisis communications firm?
- Do we need to notify? If yes, who? Customers? Employees?
- Do we need a call center?
- Do we need to provide credit or identity monitoring?

5 Execute your Response Plan with your insurance company as your partner along the way

Service Offerings in Addition to Insurance

Data Breach Response Partners

- Computer Forensics
- Data Breach Notification and Call Center Services
- Credit and ID monitoring
- Expert legal counsel
- Public Relations and crisis management

Claims Experts

- Dedicated and experienced attorneys/staff who provide hands-on service through the entire breach and claims process
- Ability to submit data breaches 24-hours a day, staffed by carrier claims team

Proactive risk mitigation resources through the carriers' network of industry partners:

- Advanced endpoint protection and security services
- Social engineering and phishing campaigns
- Privacy awareness training
- Incident response planning
- Cyber security compliance assistance

Clients also have access to online resources to learn more about cyber-security readiness and incident response services

Thank you!

Susan Leung
Vice President
Public Entity
Alliant
Susan.Leung@alliant.com