Cyber Liability Claims

Learned Panel of Experts

Shawn Bubb, Director of Insurance Services at Montana Schools Group Insurance Authority

Ed Cooney, Account Executive at Conner Strong & Buckelew, Underwriting Manager for Municipal Excess Liability JIF (NJ) and New Jersey Counties Excess JIF (NJ)

Greg Gilliam, Claims Manager at Schools of Ohio Risk Sharing Authority

Atul Poladia, Chief Information Officer at Texas Municipal League Intergovernmental Risk Pool

Brennan Quintus, Chief Executive Officer at North Dakota Insurance Fund
Whether they like it or not, Montanans are not immune to what law enforcement is describing as the “crime of the future.”
What Happened

- Afternoon of Sept. 13
- Superintendent and parents receive graphic and violent text message threats against students
- That evening, superintendent emails other local area superintendents
- Minutes later all area superintendents start receiving threatening emails

What Happened Next

On Friday, a 7 page ransom letter was received for $150,000 in bitcoin

On Sunday the local sheriff released the ransom note to the local paper

Threats to release staff and student information to the dark web
Who knew forensic computer work was so expensive?!?

- Weekly update meetings

Daily demands by staff, parents, and community members to know if their information was taken

All parts of the network were imaged, scanned

Trail of access begins to be seen.

Notifications

- 853 current and former staff members
- Slightly over 1,100 students
- PHI and PII in different combinations
- Some had relocated to other states
- Vendor used for mailing
- 1 year of credit monitoring provided to all impacted
Lessons We Learned

Big wake up call about needed network computer security measures statewide

MSGIA developed network computer assessments for members

Cyber incident response plans were developed for all members

Having cyber coverage is very important but prevention is even better

And the Claim Costs Were...

- Forensic Computer: $110,500
- Legal: $73,000
- PR Management: $1,000
- Notification Services: $12,500
- Credit Monitoring: $3,250

Total claim costs of approximately $200,000
Cyber Claim Case Study #2

Ransomware
Member Housing Authority in rural North Dakota

Lessons
- Educate pool and member employees
- Understand data retained and where it is stored
- Run regular back-ups
- Have a plan
- A cyber incident isn’t always a disaster, but mishandling it is

Cyber Claim Case Study #3

State: New Jersey
Municipalities: 9
Attack: Ransomware
When: December 2018
What Happened?

- **Affected**: Nine (9) separate cyber claims, nine (9) different members
- **Timeframe**: Three weeks in December 2018
- **Strains**: Ryuk Ransomware, GandCrab
- **Vectors**: Compromised credentials, email phishing
- **Ransom Demands**: $100k - $300k (25 BTC – 85 BTC)

Best Practices

- **Backups**: Daily backups with at least 14 days of versioning, off-network
- **Patching**: All software, asap
- **Defensive Software**: antivirus, firewalls, anti-spam, close all unused ports, VPN, Protected Mode
- **Training**: One hour of employee training, annually (malware identification, social engineering)
- **Incident Response Plan**: Clear, detailed plan, and practice it
- **Access Controls**: Limit privileges
- **Encryption**: Encrypt confidential, PII and PHI files
- **Passwords**: Strong and regularly changed, and no use of previous passwords
Cyber Claim Case Study #3

Computer Fraud—Damages
School District—duped ACH transfer

Coverage
• Difference: Cyber Liability vs Crime
• Check exclusions
• Understand: “Social Engineering”
• Limits?
• New wrinkles (and insurer reactions)

Claims Trends
No organization is immune to cyber threat.

It is not a question of “if”... it is a question of “when?”.

Thus, you need:
- Prevention Plan
- Response Plan

Top 3 claims trends by volume

1. Phishing
2. Ransomware
3. Hacking
Phishing Prevention Tips

• Phishing Awareness Training for all employees.
• Conduct regular phishing simulation by using online tools like KnowBe4, ProofPoint, PhishLabs, Mimecast, etc.
• Turn on Multi-Factored Authentication.
• Flag or visual indicator for any email received from outside your domain.
  • Prepend text “[External]:” to a subject line.
  • Enable ToolTip to warn user email is from outside domain.

Phishing Prevention Tips

• Enable Domain Keys Identified Mail (DKIM), DMARC and SPF to protect your domain and brand.
• Implement org policies to double check authorization before performing any finance related transactions, if possible eliminate financial authorization by email.
• Provide “Phish” alert buttons within mail application, and
• Implement smart spam filters.
Ransomware Tips

• Backup is your friend.
  • How frequently are you taking full and incremental back up for your critical systems and data.
  • How frequently is your IT team is conducting backup recovery drill?
• When was the last time your IT team conducted Blackbox and Whitebox penetration test on your network?
• How many critical and high vulnerability exist on your network and what is the plan to address them?

Managing Member Needs

<table>
<thead>
<tr>
<th>Member Challenges</th>
<th>Pool Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of funding for cyber risks</td>
<td>Analyze key claims areas, develop mitigation strategy</td>
</tr>
<tr>
<td>Organizational and financial risks</td>
<td>Coverage, expertise</td>
</tr>
<tr>
<td>Uniqueness of managing cyber claims</td>
<td>Claims map, best practices, education, key partners</td>
</tr>
<tr>
<td>Aging infrastructure and diverse systems</td>
<td>Cybersecurity experts, shared services</td>
</tr>
<tr>
<td>#1 weakness = employees</td>
<td>Employee training</td>
</tr>
</tbody>
</table>
Thank you!

• Closing Comments
• Questions