Whether they like it or not, Montanans are not immune to what law enforcement is describing as the “crime of the future.”
Cyber Claim
Case Study #1

Elementary ADA: 950
Middle School: 500
High School: 650
Total student population: 1,240

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
Threats to release staff and student information to the dark web
On Sunday the local sheriff released the ransom note to the local paper
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

Cyber Claim Case Study #3

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
Overall market position

The US cyber insurance market continues to expand. In 2017, overall market premium was almost $2 billion and it’s expected to be even higher for 2018.

Unit cost to conduct a cyber attack has reduced significantly, enabling hackers to target medium to small size organizations.

Mid- to small-size organizations don’t have enough technical expertise nor financial strength to defend against sophisticated cyber attacks.

Top 3 claims trends by volume

1. Phishing
2. Ransomware
3. Hacking
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