Cyber Risk Insurance & Resources for ICRMP Members

June 7, 2017

Steve Robinson
Area President
Today’s Presenter

Steven R. Robinson

AREA PRESIDENT, RISK PLACEMENT SERVICES, INC.
- Leads national Technology & Cyber practice of RPS, a division of Arthur J. Gallagher & Co.
- Leads team of insurance professionals, developing cyber risk insurance programs in the following sectors: public entity, edu, finance, hospitality, technology, retail and others
- National speaker, educator and author in matters of cyber risk insurance
- B.A., University of South Carolina
Today’s Topics

• What does a data breach look like?
• ICRMP Cyber Risk Insurance policy
• Claims we are seeing
• Incident reporting
• Resources
• Questions / Discussion
What Does a Data Breach Look Like?
10 Fact Patterns of Data Breaches

- Missing or stolen laptop or storage device
- Mis-mailing
- Erroneous Data Posting
- Willful release based on fraudulent instruction (social engineering)
- Compromised System (Hacking)
- Loss or Theft of Physical Documents
- Lost Back-up Data or Tape
- Breach Caused by a Third-Party Vendor
- Improper Document/Equipment Disposal
- Insider

Source: IDT911
Public Entity Exposures

The Vast Array of Services Provided By Public Entities = Information Risk

Endless networks – some connected, some not – all containing valuable information that thieves want to exploit
What is Cyber Risk Insurance?

Insurance coverage designed to protect a business or public entity from:

– Liability associated with:
  
  • Unauthorized release of confidential information
  
  • Violation of a person’s rights to privacy
  
  • Personal injury in an electronic/social media environment
  
  • Intellectual property infringement
  
  • Violations of state or federal privacy laws

– Self-incurred expenses incurred to make the above problems go away
ICRMP Cyber Insurance Policy
## Coverage Overview

*Note: This is not a guarantee of coverage and represents a high-level overview for discussion purposes only.*

<table>
<thead>
<tr>
<th>Key Coverages</th>
<th>Per Claim Limit</th>
<th>Per Claim Retention</th>
<th>Subject to Agg Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy &amp; Cyber Security Liability</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Covers allegations of privacy injury as a result of unauthorized release or misuse of personally identifiable information by you or a 3rd party and actual or alleged violation of a privacy law.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Includes privacy breach by cloud svc providers/vendors</td>
<td>$1,000,000</td>
<td>$25,000 or $50,000</td>
<td></td>
</tr>
<tr>
<td><strong>Media</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Covers liability associated with allegations of personal injury (ie: libel, slander, defamation) in media communications.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Social Media activities included</td>
<td>$1,000,000</td>
<td>$25,000 or $50,000</td>
<td></td>
</tr>
<tr>
<td><strong>Privacy Regulatory Defense, Awards &amp; Fines</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Costs for a district defending itself against regulatory actions and resulting fines and penalties following a breach of privacy regulations.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cost of defense</td>
<td>$1,000,000</td>
<td>$25,000 or $50,000</td>
<td></td>
</tr>
<tr>
<td>• Fines/Penalties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Breach Response &amp; Crisis Management Coverage</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Costs to notify customers/citizens of a data breach, costs to hire IT forensics experts, public relations consultants, implement credit monitoring and identity restoration services resulting from your obligation to comply with a privacy law.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Legal assistance</td>
<td>$1,000,000</td>
<td>$25,000 or $50,000</td>
<td></td>
</tr>
<tr>
<td>• IT forensics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Notification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Credit monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• PR expenses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Advertising expenses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cyber Extortion</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monies paid for purposes of ending an extortion threat to avoid corruption or damage to your computer system or website.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Extortion monies</td>
<td>$1,000,000</td>
<td>$25,000 or $50,000</td>
<td></td>
</tr>
<tr>
<td>• Additional expenditure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Recovery</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monies paid for purposes of ending an extortion threat to avoid corruption or damage to your computer system or website.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Fees to determine replicability</td>
<td>$1,000,000</td>
<td>$25,000 or $50,000</td>
<td></td>
</tr>
<tr>
<td>• Replace, restore, repair software/data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PCI Fines and Penalties</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Written demand from a Card Association or Acquiring Bank for monetary assessment due to non-compliance with PCI-DSS.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tied to Privacy or Cyber Security event</td>
<td>$100,000</td>
<td>$25,000 or $50,000</td>
<td></td>
</tr>
</tbody>
</table>

**$4,000,000 Policy Limit, Including claim expenses**
Current Claims in the Public Entity Sector

- Real Events
- Recent Events
- Lessons Learned
Claim # 1

• Type of Entity: Housing Authority
• Type of Event: Ransomware
• Coverage Triggered: Privacy & Security / Data Breach & Crisis Mgmt
• Payout: $250,000

• Overview
  – Contacted outsourced IT provider
  – Wiped critical data/evidence, hindering response
  – Forensics engaged
  – Notification of 6,893 individuals, credit monitoring, public relations.
Claim # 2

- Type of Entity: Board of Education
- Type of Event: Ransomware
- Coverage Triggered: Cyber Extortion
- Anticipated Payout: > $25,000

Overview
- Employee opened email containing malware
- Multiple computers and network drive affected
- Legal counsel engaged
- IT forensics
- No data exfiltration
Hello.
Your some files were encrypted with the strongest cipher RSA 1024 and AES.
No one will help you to restore files without our decoder. Any programs for
recovering files or disk repair are useless and can destroy your files
irreversibly. Irreversibly. So don't try to decrypt it yourself. We warned you.

There is only one way to restore your files - send e-mail to
with attached file "_how to decode[WIN764-bit].txt" (you read this file right now).
To test our honesty you can send an one encrypted file less than 4 MB (not zipped)
as *.doc *.xls *.jpg *.pdf, but not database file or backup file

We will decode your sample for free.

You will receive deciphered sample and our conditions how you will get the
decoder. Follow the instructions to send the payment. Be attentive! The decoder
for each server is paid separately.

**P.S. Remember, we are not scammers.** We don't need your files. If you want, you
can get the password for free after 6 month wait.
Just send a request immediately after infection and download the decoder.
All data will be restored absolutely.

Our guarantee of honesty - your deciphered sample.

E-mail: [redacted]
E-mail: [redacted]
Bitmessage: [redacted]
Claim # 3

- Type of Entity: County Government
- Type of Event: Virus Encryption
- Coverage Triggered: Data Breach & Crisis Mgmt
- Anticipated Payout: TBD

Overview
- County servers shut down, Thanksgiving holiday
- 911 center included
- 42 servers – Mamba variant – full-disk encryption
- Working with law enforcement, IT forensics
- Determining next steps, including data exfiltration
- Developing
Claim # 4

- Type of Entity: Design Svcs Company
- Type of Event: Ransomware
- Coverage Triggered: Cyber Extortion
- Anticipated Payout: $300,000

Overview
- Ransomware attack on insured’s servers and backup servers.
- Encryption made restoration from backup impossible
- Bitcoin ransom
- Extensive monitoring
- No data exfiltration
- Legal, forensics
Incident Reporting
Breach Response
Expert Resources are Ready to Assist

Suspected Data Breach Incident

Immediately Call Breach Hotline
855-566-4724
AND THEN
800-336-1985 ICRMP

Notify carrier via email:
proclaimnewnotices@xlcatlin.com
AND
intake@icrmp.org

Coordination of Breach Response Begins

Carrier Manages Claims Process Throughout

Goals:
• Ensure compliance
• Mitigate potential damage:
  • Financial
  • Operational
  • Reputational

Expert Legal Assistance
IT Forensics
Call Center
Public Relations
Notification
Regulatory Compliance
Credit/ID Monitoring
Do’s & Don’ts of Incident Reporting

• **DO** report any suspected privacy/information security incidents to your IT department/manager immediately – even if you are unsure

• **DO** prepare a brief description of the incident, timeline, key personnel

• **DO** call the insurance carrier Data Breach Hotline (if you have coverage)

• **DO NOT** attempt to handle the matter yourself

• **DO NOT** do anything to jeopardize the digital footprint of the incident

• **DO NOT** engage legal or IT experts without first calling the XL Catlin Data Breach Hotline
CyberRiskConnect.com
Available to ICRMP Members

Cyber Library
• Cyber risk articles, videos

Incident Roadmap
• Suggested steps to take following a network or data breach incident and free consultation with a Breach Coach®

Breach Response Partners
• Access to pre-qualified network of third-party resources with expertise in pre-breach and post-breach disciplines, including network vulnerability testing, IT risk assessments, incident response planning, security awareness training, data breach tabletops and more.

Risk Manager Tools
• Self-help for managing cyber risk, including a cyber risk assessment guide, breach notification guides, etc.

News Center
• Articles on major breach events, security and privacy blogs, IT security updates, risk management events and helpful industry links.
CyberRiskConnect.com
To Register & Access Content

- Go to www.CyberRiskConnect.com
- Complete the registration form and include your access code. Your access code is 10448.
- Once registered, you can access the portal immediately with the User ID and password you established during registration
Questions
Thank You!