The Zen Ten Cyber Security Protection for Oregon Cities

Greg Hardin, Cybersecurity Specialist/Systems Architect
Scott Moss, Program Administrator
Objectives

- Highlight examples from claims experience
- Explain the Zen Ten Cyber Security Protections
- Coverage tiers, premium, and limits
- Claims process
Cyber Threats Close to Home

Three claims prior to 2018

47 claims since 2018

Cyber attacks are up 600% worldwide since the start of pandemic
Ransomware

Coastal county with nearly 500K incurred costs

Two small cities over 100K
Fraudulent Instruction

- City paid bad actor posing as contractor
- Bad actor stole email credentials of contractor
Release of PII

- County paid nearly 80K for notifications
- Bad actor gained access to email for 10 hours
Introduction

Greg Hardin
Cybersecurity Specialist/Systems Architect
503-763-3889
ghardin@cisoregon.org
How do I protect my entity against cyber risk?
1) Adopt a cybersecurity policy
2) MFA (Multi-Factor Authentication)
3) **EDR/XDR**

- SentinelOne
- Cortex XDR
- Windows Defender ATP
- Carbon Black
- CrowdStrike
- Darktrace
- Albert Sensors (MS-ISAC)
4)Immutable Geo-diverse backups

Backups should be:
- Gated
- Offline
- In a different Geo region
- Tested on a random, monthly, quarterly, and annual basis
5) Training

CIS’ learning center offers online cyber security awareness training
6) Phishing exercises or social engineering tests

88% of data breaches come from human error
Tips for acing the test

- Use a different communication channel to verify the request
- Be suspicious of urgent requests asking for immediate action
- Inspect the from email address and the reply to address
- Hover over links to confirm they match the expected primary domain.
- Know your company policy on password change requests
Vulnerability Scanning

Cyber Hygiene Scan
Web Application Scan

Email: Therese Masse
theresa.masse@cisa.dhs.gov
Verify your password’s uniqueness

Use haveibeenpwned.com to check if your email or phone number has been compromised.

Use haveibeenpwned.com/passwords to check if your password is unique across all known data breaches.

123456 has been pwned over 24 million times.
7) Require complex passwords

- Longer passwords, not frequent expiration
- Use a password manager
- All password managers will generate one for you
Email Filters

Add custom message identifying outside emails
8) Patches

Stay updated on patches
9) **User Auditing**

Do you limit the number of administrative users?

Do you audit systems for users that may have access that no longer need it?

Add an expiration date for IT when asking for contractor access.
10) Purchase cyber insurance coverage (from CIS)
## Coverage Tier Limits

<table>
<thead>
<tr>
<th>Description</th>
<th>TIER 1</th>
<th>TIER 2</th>
<th>TIER 3</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS AGGREGATE:</td>
<td>$5,000,000</td>
<td>$5,000,000</td>
<td>$5,000,000</td>
<td>$5,000,000</td>
</tr>
<tr>
<td>TIER 1</td>
<td>$50,000</td>
<td>$50,000</td>
<td>$50,000</td>
<td>$50,000</td>
</tr>
<tr>
<td>TIER 2</td>
<td>$200,000</td>
<td>$200,000</td>
<td>$200,000</td>
<td>$200,000</td>
</tr>
<tr>
<td>TIER 3</td>
<td>$250,000</td>
<td>$500,000</td>
<td>$750,000</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>TOTAL</td>
<td>$500,000</td>
<td>$750,000</td>
<td>$1,000,000</td>
<td>$1,250,000</td>
</tr>
<tr>
<td>Cyber Extortion Loss (Ransomware)</td>
<td>$500,000</td>
<td>$750,000</td>
<td>$1,000,000</td>
<td>$1,250,000</td>
</tr>
<tr>
<td>Data Recovery Costs</td>
<td>$500,000</td>
<td>$750,000</td>
<td>$1,000,000</td>
<td>$1,250,000</td>
</tr>
<tr>
<td>Reputational Loss</td>
<td>$500,000</td>
<td>$750,000</td>
<td>$1,000,000</td>
<td>$1,250,000</td>
</tr>
<tr>
<td>Data &amp; Network Liability</td>
<td>$500,000</td>
<td>$750,000</td>
<td>$1,000,000</td>
<td>$1,250,000</td>
</tr>
<tr>
<td>Regulatory Defense &amp; Penalties</td>
<td>$500,000</td>
<td>$750,000</td>
<td>$1,000,000</td>
<td>$1,250,000</td>
</tr>
<tr>
<td>Fraudulent Instruction</td>
<td>$500,000</td>
<td>$500,000</td>
<td>$500,000</td>
<td>$500,000</td>
</tr>
<tr>
<td>Funds Transfer Fraud</td>
<td>$500,000</td>
<td>$500,000</td>
<td>$500,000</td>
<td>$500,000</td>
</tr>
<tr>
<td>Telephone Fraud</td>
<td>$500,000</td>
<td>$500,000</td>
<td>$500,000</td>
<td>$500,000</td>
</tr>
<tr>
<td>Breach Response</td>
<td>$500,000</td>
<td>$750,000</td>
<td>$1,000,000</td>
<td>$1,250,000</td>
</tr>
<tr>
<td><strong>Deductible</strong></td>
<td>$5,000</td>
<td>$5,000</td>
<td>$5,000</td>
<td>$5,000</td>
</tr>
</tbody>
</table>
## Tier 1 and 2 Premium

<table>
<thead>
<tr>
<th>Materials &amp; Services Budget</th>
<th>$50k Limit (Tier One)</th>
<th>$200k Limit (Tier Two)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0 - $500K</td>
<td>$650</td>
<td>$500</td>
</tr>
<tr>
<td>$500K - $1M</td>
<td>$800</td>
<td>$650</td>
</tr>
<tr>
<td>$1M - $2M</td>
<td>$1,200</td>
<td>$850</td>
</tr>
<tr>
<td>$2M - $5M</td>
<td>$2,300</td>
<td>$1,100</td>
</tr>
<tr>
<td>$5M - $15M</td>
<td>$3,600</td>
<td>$1,500</td>
</tr>
<tr>
<td>$15M - $30M</td>
<td>$5,500</td>
<td>$2,100</td>
</tr>
<tr>
<td>$30M+</td>
<td>$7,500</td>
<td>$3,000</td>
</tr>
</tbody>
</table>
## Tier 3 Premium

<table>
<thead>
<tr>
<th>POPULATION</th>
<th>$250,000</th>
<th>$500,000</th>
<th>$750,000</th>
<th>$1,000,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 9,999</td>
<td>$1,500</td>
<td>$2,800</td>
<td>$4,200</td>
<td>$5,500</td>
</tr>
<tr>
<td>10,000-24,999</td>
<td>$2,200</td>
<td>$5,500</td>
<td>$6,900</td>
<td>$9,500</td>
</tr>
<tr>
<td>25,000-49,999</td>
<td>$3,500</td>
<td>$8,200</td>
<td>$10,200</td>
<td>$13,600</td>
</tr>
<tr>
<td>50,000-99,999</td>
<td>$5,500</td>
<td>$11,000</td>
<td>$13,700</td>
<td>$20,500</td>
</tr>
<tr>
<td>100,000 plus</td>
<td>$9,500</td>
<td>$16,300</td>
<td>$17,000</td>
<td>$34,000</td>
</tr>
</tbody>
</table>
What Happens When A Claim is Filed

Call Carol!
1. Carol contacts "breach coach"
2. Meeting with you, IT, Carol, breach coach
3. Breach coach will tell you to call law enforcement
4. Forensics firm recommended – you get to decide and contract
4. Negotiation firm recommended (if needed) You get to decide and contract
CIS Cyber Adjuster

Carol Drouet
Senior Property Claims Consultant
503-763-3872
cdrouet@cisoregon.org
Detection and Remediation

How should the infected machines be handled?
Contact Information

Greg Hardin
Cybersecurity Specialist/Systems Architect
503-763-3889
ghardin@cisoregon.org
Contact Info

Greg Hardin
Cybersecurity Specialist/
Systems Architect
503-763-3889
ghardin@cisoregon.org
Resources

- https://cisooregon.org/Member/RiskManagement/ResourceLibrary
- https://learn.cisooregon.org/
- https://www.cisa.gov/
- https://www.cisecurity.org/ms-isa-c
Insight – CIS Risk Management Software

Insight Templates

- Cyber Detection
- Cyber Identification
- Cyber Protection
- Cyber Response and Recovery
- Cyber – Implementing MFA

Contact Scott Moss for more information
smoss@cisoregon.org