CYBER INSURANCE FOR CITIES: WHAT YOU NEED TO KNOW
Do you have cyber insurance?

Do you need cyber insurance?
OMAG’s Old Coverage

- Third-party insurer and claims handling
- Law firm and Digital Forensics & Incident Response (DFIR) in another State
- Sublimits and exclusions
- Theft and eCrime through Property only
- Denied claims
OMAG’s New Coverage

- Up to $50k annually in coverage
- Deductible of $2,000
- Pool-wide annual limit of $2.5M
- Utilizes OMAG’s preferred partners for legal and Digital Forensics/Incident Response (DFIR).
- First-Party Coverage & Liability (Third-Party Coverage)
- Claims-Made, not occurrence.
First-Party Coverage

- Cyber extortion (ransomware)
- E-Crime, including:
  - Phishing
  - Hacking
  - Fraudulent Instruction
  - Identity Theft
Third-Party Coverage

- Breach Notice
- Breach Response
- Credit Monitoring Costs
- Defense
Have you read your policy?
Moral Hazard

- The tendency for an insured to be less cautious because “the insurer will take care of it”.
Moral Hazard means you trade insurance premiums for true security investment.

And on the Internet, this means everyone is less safe.
The Risk Managers RoadMap

**Risk Avoidance**
- No Public Services
- Deactivate Old Systems
- Decommission Windows XP

**Risk Mitigation**
- Firewalls
- MFA
- Encryption

**Risk Exploitation**
- Disaster Recovery Services
- Building Trust with Citizens
  - “Two birds, one stone”

**Risk Transfer**
- *Cyber Insurance*

**Risk Acceptance**
- “The Cost of Doing Business”

- No Public Services
- Deactivate Old Systems
- Decommission Windows XP
- Firewalls
- MFA
- Encryption
- Disaster Recovery Services
- Building Trust with Citizens
  - “Two birds, one stone”
The Risk Managers RoadMap

- **Risk Avoidance**
  - No Public Services
  - Deactivate Old Systems
  - Decommission Windows XP

- **Risk Mitigation**
  - Firewalls
  - MFA
  - Encryption

- **Risk Exploitation**
  - Disaster Recovery Services
  - Building Trust with Citizens
  - “Two birds, one stone”

- **Risk Transfer**
  - **Cyber Insurance**

- **Risk Acceptance**
  - “The Cost of Doing Business”

---

- Don’t Let Them Take the Corvette
- Send them to Driver Training
- Take the keys if they fail classes
- Buy Insurance
- Pray
## Risk Transfer: Calculating Residual Risk

<table>
<thead>
<tr>
<th>Risk Avoidance</th>
<th>Risk Mitigation</th>
<th>Risk Exploitation</th>
<th>Risk Transfer</th>
<th>Risk Acceptance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Calculation</td>
<td>Risk Calculation</td>
<td>Risk Calculation</td>
<td>Risk Calculation</td>
<td>Risk Calculation</td>
</tr>
<tr>
<td>$2,820,000</td>
<td>$2,820,000</td>
<td>$1.45M</td>
<td>$1.55M</td>
<td>$0.6M</td>
</tr>
<tr>
<td>Risk Calculation = 100,000 * $141 * .2</td>
<td>Risk Calculation = 100,000 * $141 * .2</td>
<td>Risk Calculation = 100,000 * $141 * .2</td>
<td>Risk Calculation = 100,000 * $141 * .2</td>
<td>Risk Calculation = 100,000 * $141 * .2</td>
</tr>
<tr>
<td>Number of Citizens = 100,000</td>
<td>Number of Citizens = 100,000</td>
<td>Number of Citizens = 100,000</td>
<td>Number of Citizens = 100,000</td>
<td>Number of Citizens = 100,000</td>
</tr>
<tr>
<td>Likelihood = 1 every 5 years</td>
<td>Likelihood = 1 every 5 years</td>
<td>Likelihood = 1 every 5 years</td>
<td>Likelihood = 1 every 5 years</td>
<td>Likelihood = 1 every 5 years</td>
</tr>
<tr>
<td>Revenue Increase: $100,000</td>
<td>“We Protect Your Data!”</td>
<td>$1M Policy with $100,000 Deductible (Cost of Policy: $50,000)</td>
<td>$600,000 self-insured retention and deductible</td>
<td></td>
</tr>
</tbody>
</table>

### Risk Avoidance
- **Delete Old Data:**
  - Revenue: -$820,000

### Risk Mitigation
- **At-Rest Encryption, DLP**
  - Revenue: -$500,000 (Increase in costs $50,000)

### Risk Exploitation
- **“We Protect Your Data!”**
  - Revenue: $100,000

### Risk Transfer
- **$1M Policy with $100,000 Deductible**

### Risk Acceptance
- **$600,000 self-insured retention and deductible**
Investigate

Detect Something Interesting on Server

Breach?

Fix it!

6 months go by

- Oh yeah, should we file a claim?
- If it’s bad enough somebody will call the cops or whatever
- I guess tell my boss, or like the CISO or something
Incident Response Plan (v2 – Now with Cyber Insurance)

Detect Something Interesting on Server

Investigate

Determine & Declare Incident

Activate Formal Incident Response Plan

Incident Response Plan

Log & Prioritize Incident

Notify… (if appropriate)

Management

Law Enforcement

Insurer

Public

Containment

Eradication

Recovery

After-Action Report, Analysis, and Continuous Improvement
An ounce of prevention...
Multi-factor authentication
Anti-virus (paid-for and monitored) on every workstation
Backups, backups, backups – of every file you can’t afford to lose
Firewalls in front of every Internet connection
Staff trained on “not clicking”
Don’t let staff have Administrator privileges – can’t install software – on their own PCs.
Do you have cyber insurance?

Do you need cyber insurance?
Wealth of resources available at:

www.omag.org/technology