Cyber Insurance 101

**KEY TAKEAWAYS**

Common Ground
Value Proposition
What's Included & What's Not
Calculating Claims Costs
Market Intel
Q: Cyber Insurance or InfoSec?

"It's scary and confusing...but at least it's boring..."

CFO Healthcare Services Provider 2019

A: Yes
CEO: "Last time I saw you, I gave you money for more security"

CISO: "We've been hacked!"
"Jeffrey, slow down. I didn't understand a word you said"

Robert "@RSnake" Hansen 2017
Cyber Insurance Value Proposition

**OUTSIDE PERSPECTIVE**
Free second look under the hood can validate existing security efforts

**IMMEDIATE SUPPORT**
Access to vetted legal, forensics, notification and other related experts who know how to resolve problems

**FINANCIAL RECOVERY**
Reputation management, lost income, fines & penalties, and credit monitoring

**GET BACK TO BUSINESS**
Continued legal and financial support as well as security tools tools to augment your existing efforts
Cyber Insurance: What is it?

**Insurance Contract**
Stand-alone policy or endorsed to other business insurance policies such as property, medical malpractice, and crime

**Distribution**
Primarily via property & casualty insurance agents and brokers

**Warranties & Channel**
Also used to back security vendor warranties and MSSP offerings
Cyber Insurance: Product Offering

**FIRST PARTY COVERAGE**
Your stuff

**THIRD PARTY COVERAGE**
Liability claims brought by a third-party

**SERVICES**
Vetted vendors & evolving security services
# Cyber Insurance: "First-Party" Remedies

## Your Direct Expenses

<table>
<thead>
<tr>
<th>BREACH RESPONSE</th>
<th>CYBER CRIME</th>
<th>BUSINESS INTERRUPTION</th>
<th>OTHER STUFF</th>
</tr>
</thead>
</table>
| • Incident Response  
  • Legal Expenses  
  • Notification  
  • Forensics  
  • Public Relations  
  • Credit Monitoring  
  • Post Breach Remediation | • Extortion  
  • Funds Transfer Fraud  
  • Phishing  
  • Telecom Fraud | • System Interruption  
  • Dependent System Interruption  
  • Reputational Damage  
  • Net Income & Expenses  
  • Data Recovery | • Hardware  
  • Court Attendance  
  • Reward Expenses  
  • Cryptojacking  
  • Claims Preparation |

---

CYBER INSURANCE 101: FOR SECURITY PROFESSIONALS
# Cyber Insurance: Third-Party Coverage

## Legal Defense and Indemnity

<table>
<thead>
<tr>
<th>SECURITY &amp; PRIVACY</th>
<th>REGULATORY DEFENSE</th>
<th>PCI-DSS LIABILITY</th>
<th>MULTIMEDIA LIABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Defense &amp; Damages</td>
<td>- Regulatory Defense</td>
<td>- Defense &amp; Damages</td>
<td>- Electronic &amp; Written</td>
</tr>
<tr>
<td>- Assumed Under Contract</td>
<td>- Compensatory Awards</td>
<td>- Assessments</td>
<td>- Libel, Slander &amp; Disparagement</td>
</tr>
<tr>
<td>- Malware Transmission</td>
<td>- Fines &amp; Penalties</td>
<td>- Fines</td>
<td>- Infringement: Copyright, Domain Name, Trademark</td>
</tr>
<tr>
<td>- Unauthorized Release of PHI/PII</td>
<td>- Federal, State, Local or Foreign</td>
<td>- Penalties</td>
<td>- Plaigarism</td>
</tr>
<tr>
<td></td>
<td>- Insurable by Law</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**CYBER INSURANCE 101: FOR SECURITY PROFESSIONALS**
Cyber Insurance: Insurer Services

Vetted Response & Recovery

- Legal
- Incident Response/Forensics
- Notification & Credit Monitoring
- Forensic Accounting
- Public Relations
# Claim & Services Timeline

1. **Breach Report & Evaluation**
   - Breach coach
   - IT Forensics
   - Claim legitimacy
   - Legal and regulatory
   - Engage other resources

2. **Managing Short-Term Crisis**
   - Notification
   - Credit monitoring
   - Public relations
   - Data recovery

3. **Managing Long-Term Consequences**
   - Loss of income,
   - Brand Management
   - Legal Defense
   - Class Actions
   - Regulatory fines & penalties

4. **Mitigation Tools & Consultation**
   - Training
   - Phishing simulations
   - Domain protection
   - Network monitoring
   - Patch management
   - Password management
   - Legal/PR & security consulting

---

**Cyber Insurance 101: For Security Professionals**
Coverage Limitations

Coverage limitations include policy *exclusions* but are also buried in *conditions and definitions*....
## Limitations: Typical Exclusions

<table>
<thead>
<tr>
<th>INSURED ELSEWHERE</th>
<th>UNINSURABLE</th>
<th>AGAINST PUBLIC POLICY</th>
<th>OTHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Trust</td>
<td>Nuclear</td>
<td>Intentional Acts of Senior Executives</td>
<td>Outside Policy Period</td>
</tr>
<tr>
<td>Bodily Injury &amp; Property Damage*</td>
<td>War*/Terrorism*</td>
<td>Sanctions</td>
<td>Contractual*</td>
</tr>
<tr>
<td>IP/Patent Infringement</td>
<td>Core Internet Infrastructure Failure</td>
<td>Criminal Acts</td>
<td>Betterment*</td>
</tr>
<tr>
<td>Management Liability</td>
<td>Utility Power Failure*</td>
<td>Fines &amp; Penalties Not Insurable By Law</td>
<td>Technology E&amp;O*</td>
</tr>
<tr>
<td></td>
<td>Domain Revocation</td>
<td></td>
<td>Government Orders</td>
</tr>
</tbody>
</table>

* Indicates additional exclusions or limitations.
Limitations: Conditions & Definitions

To name a few...

- Representations & Warranties
- Reporting Provisions
- In The Event of a Claim
- Retentions and Wait Periods
How Much Do We Need?

Scenario 1

A data breach could cost Cyber Risk Underwriters:

$5.4M

$3.59 per record

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach Coach</td>
<td>$130,000</td>
</tr>
<tr>
<td>Forensics</td>
<td>$250,000</td>
</tr>
<tr>
<td>Crisis Management</td>
<td>$150,000</td>
</tr>
<tr>
<td>Notification</td>
<td>$840,000</td>
</tr>
<tr>
<td>Call Center</td>
<td>$730,000</td>
</tr>
<tr>
<td>Credit Monitoring</td>
<td>$870,000</td>
</tr>
<tr>
<td>PCI Fines and Assessments</td>
<td>$0</td>
</tr>
<tr>
<td>Regulatory Fines &amp; Defense</td>
<td>$420,000</td>
</tr>
</tbody>
</table>

Does this estimate an average cost? Why do you not ask for Industry and Revenue? Why are PCI costs so high?

View Frequently Asked Questions and Disclaimer

Courtesy of At-Bay Insurance
How Much Do We Need?

Scenario 2

<table>
<thead>
<tr>
<th>Question</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Whose records?</td>
<td>Customer and Employee</td>
</tr>
<tr>
<td>2. How many individuals’ data?</td>
<td>1,500,000</td>
</tr>
<tr>
<td>3. Type of records?</td>
<td>Health and Credit Card (PHI &amp; PCI)</td>
</tr>
<tr>
<td>4. Type of breach?</td>
<td>Hack</td>
</tr>
<tr>
<td>5. Based out of California?</td>
<td>Yes</td>
</tr>
<tr>
<td>6. Store customer mailing addresses?</td>
<td>100%</td>
</tr>
<tr>
<td>7. Publicly disclosed breach in last 2 years?</td>
<td>No</td>
</tr>
<tr>
<td>8. Network complexity?</td>
<td>Medium</td>
</tr>
<tr>
<td>10. Security controls?</td>
<td>Average</td>
</tr>
</tbody>
</table>

Does this estimate an average cost? Why do you not ask for Industry and Revenue? Why are PCI costs so high?

View Frequently Asked Questions and Disclaimer

A data breach could cost Cyber Risk Underwriters:

**$36.4M**

**$24.28 per record**

Breach Coach $130,000
Forensics $500,000
Crisis Management $200,000
Notification $840,000
Call Center $730,000
Credit Monitoring $1,200,000
PCI Fines and Assessments $11,000,000
Regulatory Fines & Defense $820,000
Class Action Settlements & Defense $21,000,000

Courtesy of At-Bay Insurance
"The cyber insurance market continues to grow and underwriting performance in this sector remains strong. As well as things are going, there are challenges, with uncertainty around pricing being just one. Underwriting business interruption remains difficult. Also, the threat that insurers are most worried about remains a systemic event that could cause extensive losses and jeopardize a cyber insurers solvency."

- AM BEST
Cyber Insurance Market

Evolving and competitive

- 1% of business insurance premiums
- Some 200 insurers providing coverage but only about 20 serious players
- Two distinct markets: Enterprise & SME
- Take up rates difficult to measure but under 50%
Q&A