Understanding Cyber Insurance & Cyber Risk Quantification

Ransomware and how automated cyber risk quantification can reduce financial risk for underwriters, carriers, and the insured
Agenda

Introductions
- Dan Verton, ThreatConnect (Moderator)
- Felicia Thorpe, AHT Insurance
- Jerry Caponera, ThreatConnect

Presentations
- Ransomware Trends
- Insurance Industry Implications
- Financially Quantifying Cyber Risk

Demonstration
- Automated Cyber Risk Quantification

Audience Q&A
Introductions

Dan Verton (Moderator)
Director of Content Marketing, ThreatConnect

Felicia Thorpe
Managing Advisor, AHT Insurance

Jerry Caponera
VP Cyber Risk Strategy, ThreatConnect
Ransomware

- Colonial Pipeline, JBS USA, Kaseya
  - Ransomware attacks are up 57% this year (underreported)
- Average ransom in 2021 - Approx. $310,000 (+171%)
- Average Recovery cost - $1.85 million
- 2021 estimate - $20 billion in global damages
- Average down time - 21 days; Approx. 287 days to fully recover
- Disturbing trends
  - Kaseya (REvil) leveraged a zero-day vulnerability - $70 million ransom
  - Ransomware is now an industry (RWaaS)
    - There are financial backers & revenue targets
    - Malware developers / access brokers
    - Hostage negotiators / intermediaries
    - You can even get a discount for paying before the deadline!
  - It’s not just about encrypting & locking your files
    - Step 1 is often exfiltration (70% of ransomware attacks)
    - Third party exposure - clients, business partners, service providers, employees
    - Additional levels of extortion (REvil now offers DDoS attacks and voice-scrambled VoIP calls to journalists and colleagues as a free service for its affiliates)
Who is being targeted? Most at risk?

- Those who can pay
- Those who are more likely to pay
  - Healthcare
  - Law firms
  - Critical infrastructures

The New York Times

*Cyber Attack Suspected in German Woman’s Death*

Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital’s computers. It could be the first fatality from a ransomware attack.
Insurance & Cyber Risk

- Premiums increasing by 30-50%
- More restrictive policy terms & coverage limits
- Carriers reducing or dropping ransomware coverage amounts (AXA)

Deeper Investigation Reveals

- Insurance underwriters rely on a highly manual, point-in-time approach to gathering data and assessing a company’s cyber risk exposure.
- Underwriters lack the ability to correlate loss data to vulnerabilities, deficient controls, misconfigured hardware or software, and the ability of an attacker to successfully compromise a critical application/system.
- Security assessments are conducted once before binding coverage and not revisited again until it’s time to renew the policy. In many cases, security assessments that are conducted on behalf of an underwriter are never shared with the company seeking insurance.
Cyber Insurance Implications

AHT INSURANCE
A BALDWIN RISK PARTNER

Felicia Thorpe
Managing Advisor, AHT Insurance
THIRD PARTY COVERAGE

Third party coverage – liability coverage designed to protect the insured from third-party suits alleging financial damages. The insurer pays the damages and defense expenses that the insured becomes legally obligated to pay; up to policy limits based on terms and conditions.

- Network Security and Data Privacy – coverage for financial damages alleging data breach or security failure that result in dissemination of protected data or third-party corporate confidential information. Includes PCI, PHI, PII.

- Media Liability – coverage for claims arising from copyright infringement, plagiarism, defamation, libel, slander or invasion of privacy.

- Professional Liability (E&O form) – coverage for a suit from a third party alleging financial damages due to technology products or services.
FIRST PARTY COVERAGES

First Party Coverages – non liability coverage grants that a company sets aside for their own usage in the event of a breach or claim.

- Crisis management
- Notification and Identity protection Expense
- Data Privacy Regulatory Expense
- PCI Expense
- Social Engineering
- Cyber Crime
- Cyber Extortion/Ransomware
- Business Interruption
- Dependent or Contingent Business Interruption
- Data Restoration Expense
- Cyber Investigation Expense
- Bricking
- Telecommunication Fraud
- Funds Transfer Fraud
- Reputational Harm
CLAIM REPORT STATUS

Percent of ransomware claims by industry (top 5)

- Consumer discretionary: 28%
- Professional services: 16%
- Healthcare: 12%
- Financial services: 9%
- Information technology: 8%

Average ransom demand

<table>
<thead>
<tr>
<th>Year</th>
<th>Q1</th>
<th>Q2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020</td>
<td>$230,110</td>
<td>$338,669</td>
</tr>
</tbody>
</table>

47% increase in average ransom

* Source: Coalition
MONUMENTAL RANSOMWARE ATTACKS

- Colonial Pipeline
- C N A
- Kaseya
- Sunburst
- Solarwinds
- Hafnium
- JBS
### UNDERWRITING CHANGES

<table>
<thead>
<tr>
<th><strong>REDUCTION IN COVERAGE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Limits being reduced</td>
</tr>
<tr>
<td>• Excess carrier options limited</td>
</tr>
<tr>
<td>• Non-renewals at all time high</td>
</tr>
<tr>
<td>• Increased retentions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>INCREASED UNDERWRITER SCRUTINY</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Tech E&amp;O forms are contracting ransomware coverage</td>
</tr>
<tr>
<td>• Supplemental apps being required for coverage</td>
</tr>
<tr>
<td>• MFA is key to securing coverage</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>INCREASE IN PREMIUM</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Hard Market</td>
</tr>
<tr>
<td>• COVID-19</td>
</tr>
<tr>
<td>• Market Conditions</td>
</tr>
<tr>
<td>• Huge Ransomware attacks</td>
</tr>
<tr>
<td>• Q1 Cyber coverage premiums increased on average 18%*</td>
</tr>
<tr>
<td>• Ransomware attacks increased 404% from 2018-2019*</td>
</tr>
</tbody>
</table>

* Source: CIAB
TOP UNDERWRITER CONSIDERATIONS

1. Strong Overall IT Security Posture, Procedures and Response Capabilities
2. Deployment of Patches Regularly
4. Security Efforts Used to Filter Attacks, Secure Open Ports & Endpoint Security at Workstations
5. Disaster Recovery & Continuity Plans
6. Phishing & Security Awareness Training
What should you do if there is an attack:

- Report the incident ASAP to the response team hotline
  - Authorities (FBI) and Insurance Carrier
- Do not pay the ransom until the response team authorizes payment
- Keep track of all pertinent information
- Work collaboratively with the response and legal teams
Cyber risk is business risk

An approach to financially quantifying cyber risk
Risk - in our definition - involves the financial impact of attacks to the business

Everyone knows the frequency of attacks are increasing - but more importantly the cost of attacks are increasing as well.

And ransom (extortion) costs are growing too:

- Colonial Pipeline pays $4m in ransom
- Brenntag paid $4m in ransom
- Petroleos Mexicanos - approx $5m ransom
- JBL paid $11m in ransom
- CNA Financial paid $40m in ransom

And this will only grow as utilities and energy companies have to keep systems online.
Which is counter intuitive when you look at how much is spent on cyber

Spending on cyber has consistently grown - yet the impact of attacks increase

Companies are increasingly asking security questions like

- Are we secure enough?
- How much spending do we really need?
- What’s the impact if we get hit?

And answers are in technical jargon, not business terms.
What’s the issue?

Companies don’t prioritize cyber risk in a way that

- The business understands
- Aligns business demands with security realities
- Is tied to finances and ROI

So we work items that aren’t in the sweet spot.
What’s the solution?

ROI based prioritization of cyber investments
The first thing we have to do is help companies understand their exposure

Cyber risk quantification should be used for decision making - to enable actions to be taken that help companies

- Understand their exposure
- Transfer what they can
- Mitigate risks in ways that provide the most ROI
Mitigations - where should I be investing?

- Long Term Mitigations provide guidance on spending decisions using ROI
- The painful reality of cyber risk is that it changes often. Quantification needs to keep up
Mitigations - what do I do about it today?

Short Term recommendations are things you can do today.

Risks change daily. Over 60% of major breaches are due to vulnerabilities being exploited. Yet people still struggle to patch.

CRQ can help here.
CRQ brings transformation to the whole security organization

CRQ provides executives a prioritized list of actions to take that link
- Financial risk
- threat(s)
- Actions to take

Not all risks and threats will be mitigated - some will be accepted.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Threat to the business</th>
<th>Asset at risk</th>
<th>Financial Risk</th>
<th>Action(s)</th>
</tr>
</thead>
</table>
| New vulnerability identified with high IOCs in our company | High - on all key systems | Revenue for critical systems  | $25,000,000   | Segment network  
Patch  
Remove Chrome from endpoints |
| Possible C&C server in our network | High - health care data at risk | Data (PHI)                    | $15,000,000   | Block  
Investigate |
| Increased level of spear phishing attacks | High - sophisticated attacks | Cash (business email compromise) | $10,000,000   | Buy new tool  
Update network security  
Outsource email hosting |
| Solarwinds vulnerability          | Low - only in test environment today | Revenue for critical systems  | $5,000,000    | Remediate Software  
Replace vendor  
Accept |
RQ Demonstration
Thank You. Questions?

Thank you to

ThreatConnect.com