Can the cybersecurity insurance market incentivize better risk management?

Dialogue

- Insurers
- CISOs
- Risk Officers/Managers
- Critical Infrastructure Owners/Operators
- Academic Community
- Other Public/Private Sector Stakeholders

Working Session Readout Reports

Cyber Incident Data Repository

CIDAWG White Papers

Cyber risk analytics to inform and improve cyber risk management investments and practices and cyber insurance policies
 Repository Concept Development Timeline

- **2012-2014**: NPPD facilitated four Cybersecurity Insurance Working Sessions

- **February 2015**: NPPD published the Cyber Incident Data Repository Value Proposition White Paper

- **June 2015**: NPPD established the Cyber Incident Data and Analysis Working Group

- **September 2015**: NPPD published the White Paper on Overcoming Information Sharing Challenges

- **December 2015**: NPPD published the White Paper on Overcoming Information Sharing Challenges

- **April 2016**: Cyber Incident Data and Analysis Workshop

- **??**: Repository Proof of Concepts Development

- **Cyber Incident Data Repository**
Key obstacles:
• Lack of actuarial data;
• Absence of best practices, standards, and metrics;
• Limited knowledge of critical infrastructure dependencies & interdependencies; and
• Underdeveloped enterprise risk management programs.

Key Recommendations
• Focus on the concept of a cyber incident data repository (CIDAR)
• Engage Chief Information Security Officers (CISOs) and other cybersecurity professionals as essential discussion partners in the development of a CIDAR.

Available on DHS' Cybersecurity Insurance webpage at: www.dhs.gov/publication/cybersecurity-insurance
NPPD established the Cyber Incident Data and Analysis Working Group (CIDAWG) in February 2014 to explore the benefits and the feasibility of cyber incident data repository.

CIDAWG participants include private sector IT risk management professionals representing various critical infrastructure sectors and functions and insurance companies.

The CIDAWG conducted biweekly meetings to:
- Develop the Value Proposition
- Identify Repository Data Points
- Identify Information Sharing Challenges and solutions

CIDAWG white papers were published on DHS’s website: 
Cyber Incident Data and Analysis Repository

Data Points

- Type of Incident
- Timeline
- Contributing Causes
- Use of Cyber Security Framework

Benefits

- Top Risks and Effective Controls
- Peer-to-Peer Benchmarking
- ROI
- Sector Differentiation
- Forecasting, Trending and Modeling

DATA POINTS

- Federal and SLTT governments and private sector data
- Comprehensive (volume, variety, quality)
- Advances actuarial data
- Free – contributing data is the “cost of admission”
- Non-government hosted, voluntary, secure and anonymized
Value Proposition

Identifying Top Risks and Effective Controls

Informing Peer-to-Peer Benchmarking

Showing Return on Investment

Allowing for Sector Differentiation

Supporting Forecasting, Trending, and Modeling

Advancing Risk Management Culture
Information Challenges - Solutions

### Challenges

- **Legal/Policy**
  - Non-Disclosure Agreements
  - Terms of Service
  - Safe Harbor Legislation

- **Design**
  - Sequential or randomized alphanumeric identifier
  - Two-server System
  - Validations/Background checks
  - ISO 27001-like compliance Requirements
  - Architecture/database/OS Security reviews
  - Response Plans

- **Making The Business Case**
  - Engage ISACs, ISAOs, USG, existing info sharing platforms
  - Executive summaries, technical presentations, training workshops, and public statements with targeted messaging by early adopters
  - Internal outreach campaign
  - Process tools, frameworks, guiding principles
The 16 Data Points

- Type of Incident
- Severity of Incident
- Use of a cyber security framework
- Timeline
- Apparent Goal
- Contributing Causes
- Security Control Decay
- Assets Affected
- Type of Impact
- Incident Detection Techniques
- Incident Response TTPs
- Internal Skill Sufficiency
- Mitigation Prevention Measures
- Costs
- Vendor Incident Support
- Related Events
Objective: To identify cyber incident data categories that could be used to perform trend and other analyses by enterprise risk owners and insurers

What data points would achieve the collective benefits identified in the Value Proposition?

- Participants identified, developed, evaluated and consolidated more than 30 candidate data categories into 16, each tied to three or more of the six value proposition categories.
- Language and priorities differ between communities—many compromises were agreed to in order to arrive at a single list.
- Throughout, members balanced privacy needs, ease of data collection/reporting, and value of the data for analysis by both cybersecurity professionals and insurance underwriters.
Quantifying aggregate risk, primarily in terms of direct and indirect financial costs, and actions that might reduce those costs.

- “Impacts” of a cyber incident include losses and/or compromises of various types.
  “What was harmed?”

- “Severity” of a cyber incident addresses the relative scale or scope of an incident within the context of the incident contributor’s industry and circumstances. This category captures the scale/breadth of those impacts relative to an organization’s capacity.
  “How bad was the harm?”

- “Costs” of a cyber incident represent the quantifiable pay-outs by the incident victims, insurers, suppliers, etc., required to “fix” those impacts
  “What did it cost to identify, detect, respond, and recover from the incident, including costs incurred to protect against future recurrences?”
General CISO Concerns

- Focus on data categories that enable them to identify and prevent attacks
  - Avoid oversimplification of data categories

- Rejected a “Cybersecurity Maturity Indicator Index” data category
  - Lack of standardization across industry sectors
  - Self-assessments are time and labor intensive post – incident
  - Maturity does not correlate with ability to ward off attacks

- Data categories are framed as much as possible in information security terminology where feasible in order to help ensure standardization for better analysis.
<table>
<thead>
<tr>
<th>#</th>
<th>Title</th>
<th>Submitter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Incident Context</td>
<td>N/A</td>
<td>Generic (to protect privacy) company and incident information (industry sector, size, date of report, etc.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Who else might look like you?</strong></td>
</tr>
<tr>
<td>1</td>
<td>Type of Incident</td>
<td>Insurers/CISOs</td>
<td>Major category of attack in industry terms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>What Happened?</strong> DDOS, ransomware, destructive WORM, etc.</td>
</tr>
<tr>
<td>2</td>
<td>Severity of Incident</td>
<td>Insurers/CISOs</td>
<td>Difficulty in stopping/controlling incident (e.g., Low-Med-High, 1-5, Mild-Catastrophic, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>How bad was it? Really bad, or pretty minor?</strong></td>
</tr>
<tr>
<td>3</td>
<td>Use of Cyber-Security Framework</td>
<td>CISOs</td>
<td>Does the affected organization use a cybersecurity framework? If so, how, and to what effect?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Generally speaking, how were you postured before the incident?</strong></td>
</tr>
<tr>
<td>4</td>
<td>Timeline</td>
<td>Insurers</td>
<td>Date of detection, date of effective control. Retroactive timeline of attack steps (if it can be established).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>How did the incident/attack progress?</strong></td>
</tr>
<tr>
<td>5</td>
<td>Apparent Goal</td>
<td>Insurers</td>
<td>Financial, reputational, and operational value of assets to attackers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>What were the attackers after?</strong></td>
</tr>
<tr>
<td>6</td>
<td>Contributing Causes</td>
<td>Insurers/CISOs</td>
<td>People/Processes/Technology failures relevant to incident (e.g., misconfiguration, insider, poor training, etc.). Includes 3rd parties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>How did they get in? What weaknesses were exploited?</strong></td>
</tr>
<tr>
<td>#</td>
<td>Title</td>
<td>Submitter</td>
<td>Description</td>
</tr>
<tr>
<td>----</td>
<td>-------------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Security Control Decay</td>
<td>CISOs</td>
<td>If a relevant security control was present, why/how was it not effective? Assesses how security controls break down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Specifically what controls failed and how?</strong></td>
</tr>
<tr>
<td>8</td>
<td>Assets Affected</td>
<td>Insurers</td>
<td>Points in the network and/or the business that were compromised (e.g., SCADA/ICS, business sys servers, 3d party systems, websites).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>What did they hit?</strong></td>
</tr>
<tr>
<td>9</td>
<td>Type of Impact</td>
<td>Insurers/CISOs</td>
<td>Total impacts on all affected, including 3d parties (e.g., infrastructure/cloud/application service providers, the target organization, suppliers,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>customers, employees). Identifies Aggregate Risk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>What were the effects?</strong></td>
</tr>
<tr>
<td>10</td>
<td>Incident Detection Techniques</td>
<td>CISOs</td>
<td>How was the compromise identified? E.g., Internally by IPS, custom script, analytics, etc., or Externally, by FBI, the attacker (extortion),</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>outsourced security, IaaS/SaaS provider, etc.?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>How did you find out?</strong></td>
</tr>
<tr>
<td>11</td>
<td>Incident Response TTPs</td>
<td>CISOs</td>
<td>What techniques were used to stop the attack? Were they effective? How did you respond? Did that work?</td>
</tr>
<tr>
<td>#</td>
<td>Title</td>
<td>Submitter</td>
<td>Description</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 12 | Internal Skill Sufficiency            | CISOs              | Availability/sufficiency of in-house skills to quickly address incidents  
Did you have what you needed to respond? |
| 13 | Mitigation/Prevention Measures        | Insurers/CISOs     | Actions taken to stop incident and prevent future occurrences.  
What was the “final” fix? |
| 14 | Costs                                | Insurers           | Financial and other quantifiable costs incurred as a result of an incident, including mitigation, recovery, liability, and profit loss.  
How much did it cost to clean up, in total? |
| 15 | Vendor Incident Support              | CISOs              | Vendor behavior in assessing/resolving incidents, e.g.: unknowledgeable, indifferent, cooperative, helpful, hostile)  
Were other involved parties helpful? |
| 16 | Related Events                       | Insurers           | Related activities that provide incident context (e.g., upcoming merger discussions, corporate policy publicity, product launch).  
Was anything relevant going on at the time? |
One of the biggest challenges for repositories is the development of correct metrics and measurements that incentivize a broad array of stakeholders to make contributions. Break-out sessions will consider:

- What are the underlying data points in each data category?
- What cyber incident data points do organizations already track;
  - What additional data points should they be tracking for the purposes of the repository; and what would be the additional cost of tracking those new data points?
- Which data points are the easiest to automate and operationalize?
- Do the 16 data categories identified by the CIDAWG accurately reflect the needed data, which if anonymously shared into a repository, could be used to perform trend and other analyses by enterprise risk owners and insurers?
### General Incident Information
- **Type of Incident** - High-level descriptor/“tag”
- **Apparent Goals** – Attacker motivation as suggested by assets targeted
- **Assets Compromised/Affected** - The points in a network and/or business where an incident and/or attack took place.
- **Related Events** - Related activities/events that may provide context

### Organizational Practices and Maturity
- **Use of Cyber Security Standards & Best Practices**
  Cyber risk management practices, procedures, and standards in place at the time of the incident
- **Specific Control Failure(s)** – If a security control was present, identifies why/how it was not effective
- **Incident Response Playbook** – The Action, methods, procedures, and tools used to respond
- **Internal Skill Sufficiency** – Availability/sufficiency of in-house skills to quickly address incidents

### Incident Response and Recovery
- **Incident Detection Techniques** - Techniques used to identify an incident and/or attack
- **Mitigation/Prevention Measures** - Actions to stop incidents and prevent future occurrences
- **Timeline** - Detection to effective control.
- **Vendor Incident Support** - Vendor behavior during the assessment and resolution of the incident

### Consequences and Impacts
- **Severity of Incident** - The relative scale or scope of an incident within the context of the industry
- **Type of Impact(s)** - Total impacts on all affected, including 3d parties. Identifies Aggregate Risk
- **Costs** - Financial and other quantifiable costs incurred as a result of an incident and/or attack.
- **Contributing Causes** – People/process/technology failures contributing to an incident