Understanding the FAIR Risk Assessment

Nebraska CERT Conference 2009
Bill Dixon
Continuum Worldwide
What is NOT Fair?
What is FAIR?

- Factor Analysis of Information Risk
- Founded in 2005 by Risk Management Insight LLC – Jack Jones
- The basis of the creation of FAIR is “result of information security being practiced as an art rather than a science.”
Other Assessment Methodologies

• Other risk assessment methodologies
  ▫ Department of Homeland Security
  ▫ NIST
  ▫ Octave
  ▫ CMS

• All have their place and use, but...
• Each have a different language
Speaking The Same Language
How FAIR Presents a Risk Assessment: Phase One

- Identify the components of the scenario
  - ID the asset
  - ID the community of threats
How FAIR Presents a Risk Assessment: Phase Two

- Evaluate Loss Event Frequency
  - Estimate the Threat Event Frequency
    - Very High > 100 x year
    - High > 10 - 100 x year
    - Moderate > 1 - 10 x year
    - Low > .1 – 1 x year
    - Very Low < .1 x year
  - Estimate the Threat Capability – how a threat can affect an asset
    - Very High – Top 2%
    - High – Top 16%
    - Moderate
    - Low – bottom 16%
    - Very Low – bottom 2%
- Estimate the strength of the controls – measure of the effectiveness of the controls
  - Very High
  - High
  - Low
  - Very Low
- Derive the vulnerability
- Derive the Loss Event Frequency
How FAIR Presents a Risk Assessment: Phase Two (cont.)

- Estimate the strength of the controls – measure of the effectiveness of the controls
  - Very High – Protects all but top 2%
  - High – Protects all but 16%
  - Low – Protects against bottom 16%
  - Very Low – Protects against bottom 2%
- Derive the vulnerability
- Derive the Loss Event Frequency
How FAIR Presents a Risk Assessment: Phase Three

- Evaluate Probable Loss Magnitude
  - Estimate worst-case loss
  - Estimate probable loss

<table>
<thead>
<tr>
<th>Magnitude</th>
<th>Range Low End</th>
<th>Range High End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe (SV)</td>
<td>$10,000,000</td>
<td>--</td>
</tr>
<tr>
<td>High (H)</td>
<td>$1,000,000</td>
<td>$9,999,999</td>
</tr>
<tr>
<td>Significant (Sg)</td>
<td>$100,000</td>
<td>$999,999</td>
</tr>
<tr>
<td>Moderate (M)</td>
<td>$10,000</td>
<td>$99,999</td>
</tr>
<tr>
<td>Low (L)</td>
<td>$1,000</td>
<td>$9,999</td>
</tr>
<tr>
<td>Very Low (VL)</td>
<td>$0</td>
<td>$999</td>
</tr>
</tbody>
</table>
How FAIR Presents a Risk Assessment: Phase Four

- Derive and articulate risk
FAIR... in a single slide

- Risk
  - Loss Event Frequency
    - Threat Event Frequency
      - Contact
      - Action
    - Control Strength
    - Threat
      - Capability
  - Vulnerability
  - Probable Loss Magnitude
    - Primary Loss Factors
      - Asset Loss Factors
      - Threat Loss Factors
    - Secondary Loss Factors
      - Organizational Loss Factors
      - External Loss Factors
Why FAIR can be successful

- Industry agnostic
- Build a case for controls (or identify excessive controls)
- Scenario application
- Metrics
FAIR- A case study

• Where FAIR works well
  ▫ Focusing on micro issues to establish a macro results
  ▫ Breaking down elements of risk calculations in multiple elements – precision based

• Where FAIR does not work well
  ▫ First time, holistic risk assessment
  ▫ Non-metric driven environment
References

- FAIR Whitepaper - http://fairwiki.riskmanagementinsight.com/
Questions

Bill Dixon, CISSP, CISM
Bill.dixon@continuumww.com