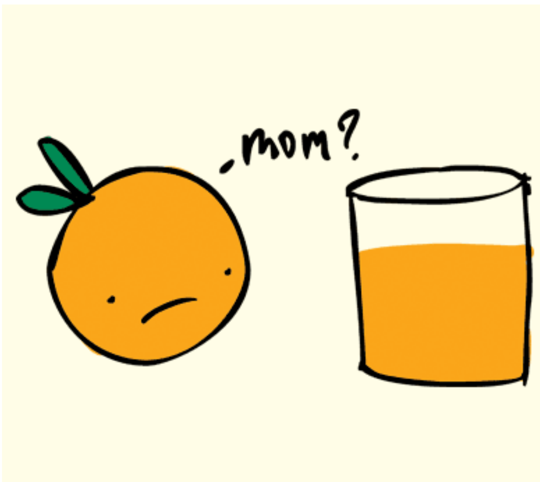
Understanding the FAIR Risk Assessment

Nebraska CERT Conference 2009
Bill Dixon
Continuum Worldwide

What is NOT Fair?



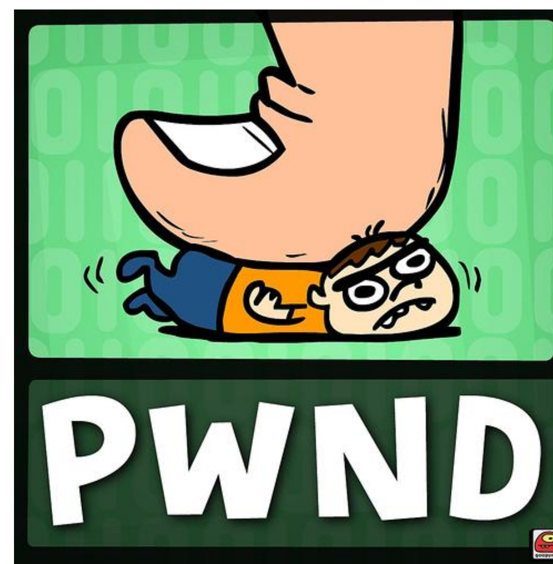
What is FAIR?

- 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

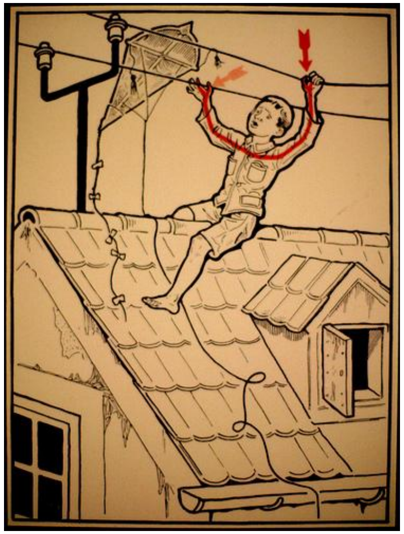
- Other risk assessment methodologies
  - Department of Homeland Security
  - NIST
  - Octave
  - CMS
- All have their place and use, but…
- Each have a different language

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

Magnitude	Range Low End	Range High End
Severe (SV)	$10,000,000	--
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1,000	$9,999
Very Low (VL)	$0	$999

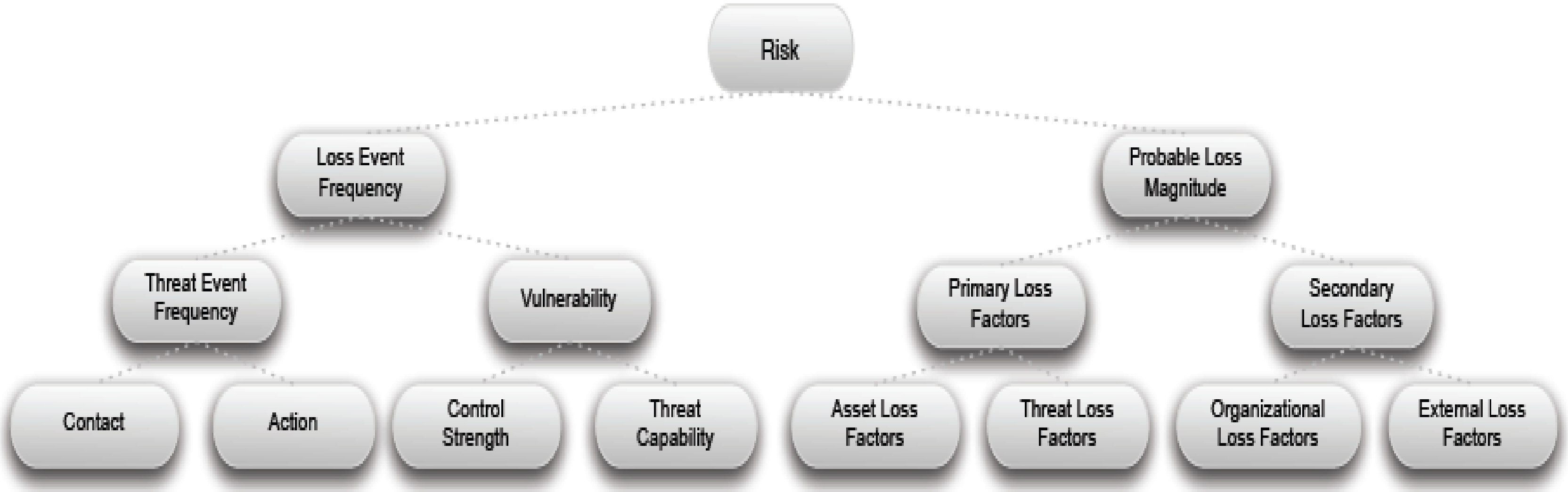
How FAIR Presents a Risk Assessment: Phase Four

- Derive and articulate risk

Risk

PLM					
Severe	H	H	C	C	C
High	M	H	H	C	C
Significant	M	M	H	H	C
Moderate	L	M	M	H	H
Low	L	L	M	M	M
Very Low	L	L	M	M	M
	VL	L	M	H	VH
			LEF		

FAIR… in a single slide



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