



---

# Sharing the Unverifiable: Prediction Exchange

## Predictive Risk Assessments

[infectionvectors.com](http://infectionvectors.com)



# Attack Measurements

---



- Common Taxonomy Key to Conceiving Metrics (Yurcik, 2000)
  - Existing Methods Aim at Impact
  - “Type” of Attack Measured
- Yurcik Model Provided Scope of Current Activity...
  - ...But Not of Future Attacks
  - ...And Uses Past Attack as Predictor of Chaotic Events in the Future



# Accuracy in Current Methods

---

- Besides Being the Prima Facie Focus for Many Casual Observers...
- Sarewitz & Pielke (2003) Posit that Accuracy Can Settle Arguments
- “Verify” What Happens

# Accuracy Measurements

---

- Lack of Long-term Experience Makes Meaningful Comments Difficult
- “Expert” Opinions of Cases that Involve Numerous Moving Parts Make These Claims Worse
  - “Non-stationary” Input Variables
  - Shaped by Bias, Personal Experience, Anecdotes, etc.

# Accuracy of What?

---

- Must Ensure Focus is Correct
  - Lessons of Climatology
  - Security Aims at Payload Issues
    - Liability of “Unofficial Patches”
    - Remote Control
    - Information Theft
- =Gridlock in All Disciplines

# Risk Assessments



- Risk = Attention
- Vulnerability = ?
  
- A Completely Risk-based Approach Hurts Security Efforts



# PRA Guidance



- Subjective Information + Guru = Overestimate Risk
  - Natural “Err on Side of Caution” Reaction
  - But, in Large Fault Trees, This is not Efficient
- Fault Trees in Aerospace Industry Built on Binary Answers



# 2005 Bulletin Breakdown

---

Of the 55 bulletins from Microsoft:

-29 were rated “Critical”

-18 were rated “Important”

-8 were rated “Moderate”

# Category Breakdown

---

The average scores for each (with the “Critical” criteria removed):

-Critical:	4.00
-Important:	3.61
-Moderate	3.25

# Additional Information

---

For the research leading up to this presentation and complementary topics:

<http://www.infectionvectors.com>