

# Cybersafety

# Objectives

- Review of Concepts. What is (are):
  - Information Systems?
  - Information Security?
  - Information Systems Security?
  - Information Assurance?
  - Cyber Security?
  - Defense in Depth?
- Significance / Importance of Concepts
- Advanced Topics in Security Risk Analysis
- Present & Future Challenges

# Review of Concepts

- *What are Information Systems?*
  - Systems that store, transmit, and process information.

+

- *What is Information Security?*
  - The protection of information.

- 
- *What is Information Systems Security?*
    - The protection of systems that store, transmit, and process information.

# Review of Concepts

- *What is Information Assurance?*
  - Emphasis on Information Sharing
  - Establishing and controlling trust
  - Authorization and Authentication (A&A)
- *What is Cyber Security?*
  - Protection of information and systems within networks that are connected to the Internet.

# Review of Concepts

- Progression of Terminology

Computer Security  
(COMPUSEC)



Information Security  
(INFOSEC)



Information Assurance  
(IA)



Cyber Security

Legacy Term (no longer used).

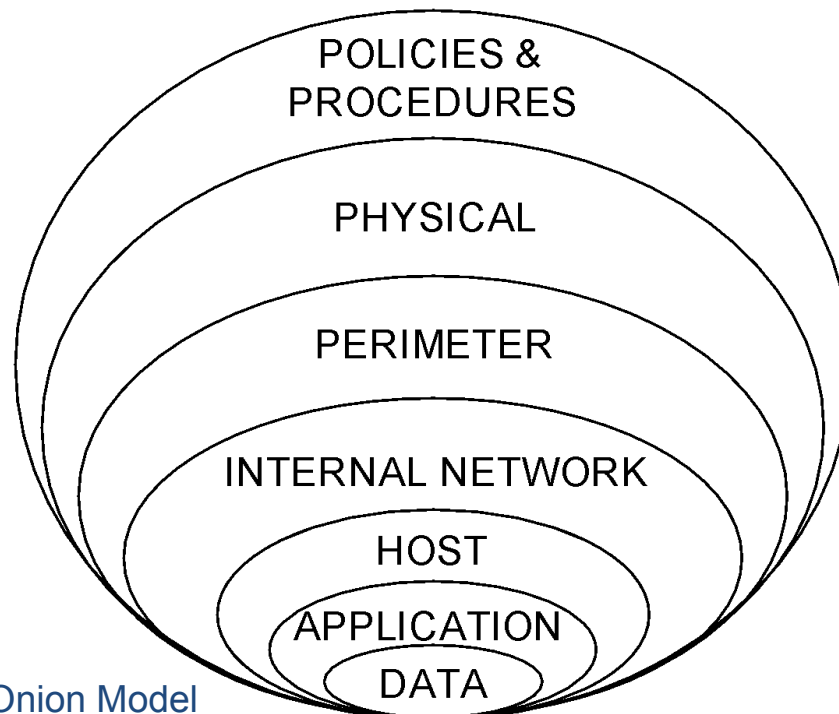
Legacy Term (still used).

Term widely accepted today with focus on Information Sharing.

Broad Term quickly being adopted.

# Review of Concepts

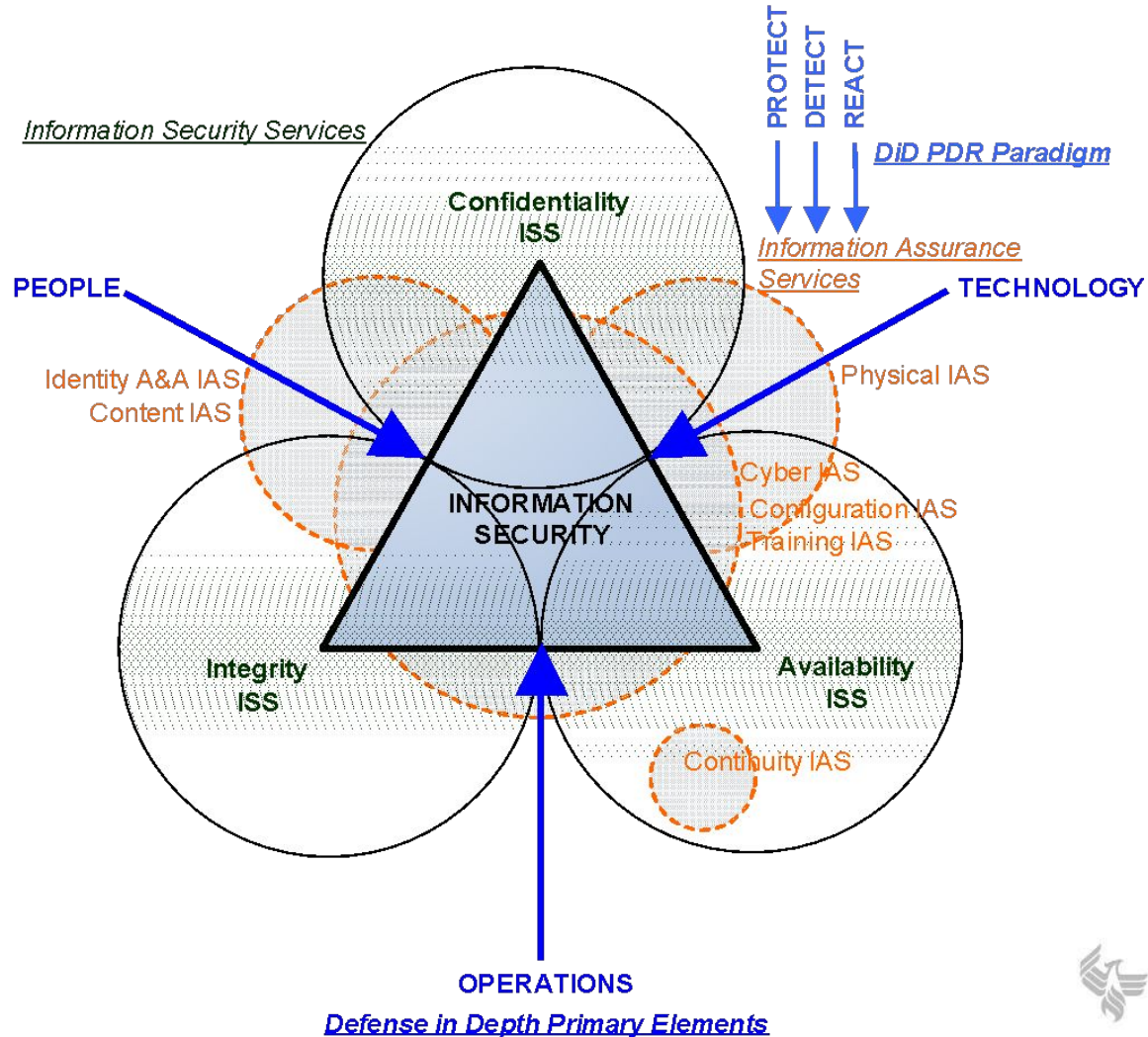
- What is the Defense in Depth Strategy?
  - Using layers of defense as protection.
- People, Technology, and Operations.



Onion Model

# Review of Concepts

## INFORMATION ASSURANCE



# ISS Management

- *What is a Backup Plan (BP) vs Disaster Recovery Plan (DRP) vs Emergency Response Plan (ERP) vs Business Recovery Plan (BRP) vs Business Impact Analysis (BIA) vs Incident Response Plan (IRP) vs Continuity of Operations Plan (COOP) vs Contingency Plan?*
- Policy & Planning
- Test, Audit, Update
- Configuration Control
- Protection, Detection, Reaction  
(Assessment, CND, Incident Response)



# Why is this important?

- Information is valuable.

*therefore,*

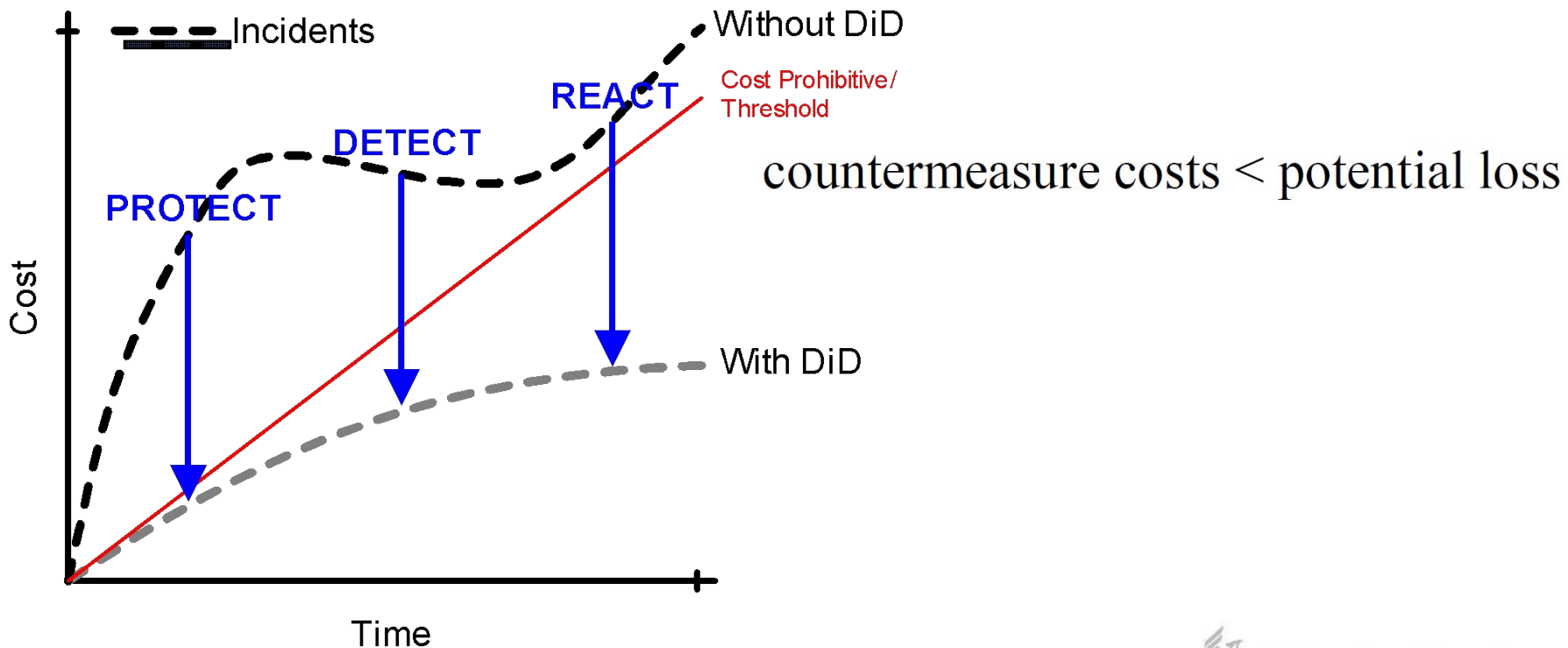
- Information Systems are valuable.

*etc...*

- Compromise of Information Security Services (C-I-A) have real consequences (loss)
  - Confidentiality: death, proprietary info, privacy, theft
  - Integrity: theft, disruption
  - Availability: productivity lost, C2, defense, emergency services

# Why is this important?

- Fixed Resources
- Sustainable strategies reduce costs



# Advanced Topics: Measuring Risk

- What is Risk?

Risk = -Opportunity

Risk =  $f_{\text{impact}}$  (uncertainty)

*thus*

Risk =  $-|f_{\text{impact}}(100\% - \text{confidence})| = \text{loss}$

- Qualitative v.s. Quantitative Methods
- Risk Assessments v.s. Risk Analysis
- Security Risk Analysis (SRA)
- Units for measurement?

# Advanced Topics: Measuring Risk

- Risk is conditional, NOT independent.

Risk  $\neq$  Threats  $\times$  Vulnerabilities  $\times$  Impact

$$\begin{aligned}\text{Risk}_{\text{EV}} &\neq \sum_n \omega_{i,n} \cdot P_i(\lambda_i) \cdot P_i(\theta_i) \\ &= \sum_n \omega_{i,n} \cdot P_i(\lambda_i | \theta_i)\end{aligned}$$

$$\begin{aligned}\text{Risk} &= f[\text{impact, probability(vulnerability | threat)}] \\ &= f[\omega_i(\text{CONF, INT, AVAIL, } \omega_{\text{CAT}}), P_i(\lambda_i | \theta_i)]\end{aligned}$$

# Advanced Topics: Measuring Risk

- Quantitative, time-dependent (continuous),  
Risk Distribution Function:

$$R_n(t) = \int_U \{1 - \{P[\lambda(t) | \theta(t)] \cdot [1 - \delta(t)]\} \cdot \{\omega \cdot [1 - \gamma(\delta, t)]\}\} dt$$

Source:

Robbins, P. (Dec, 2011). [Security Risk Analysis and Critical Information Systems](#) (Master's Thesis). Hawaii Pacific University, Honolulu, HI.

# Advanced Topics: Measuring Risk

- Expected Value of Risk = Product of Risks

$$\text{Risk}_{\text{EV}} = \prod_i^N R_i$$

- Risk is never zero

$$\lim_{N \rightarrow \infty} \text{Risk}_{\text{EV}} \approx 0$$

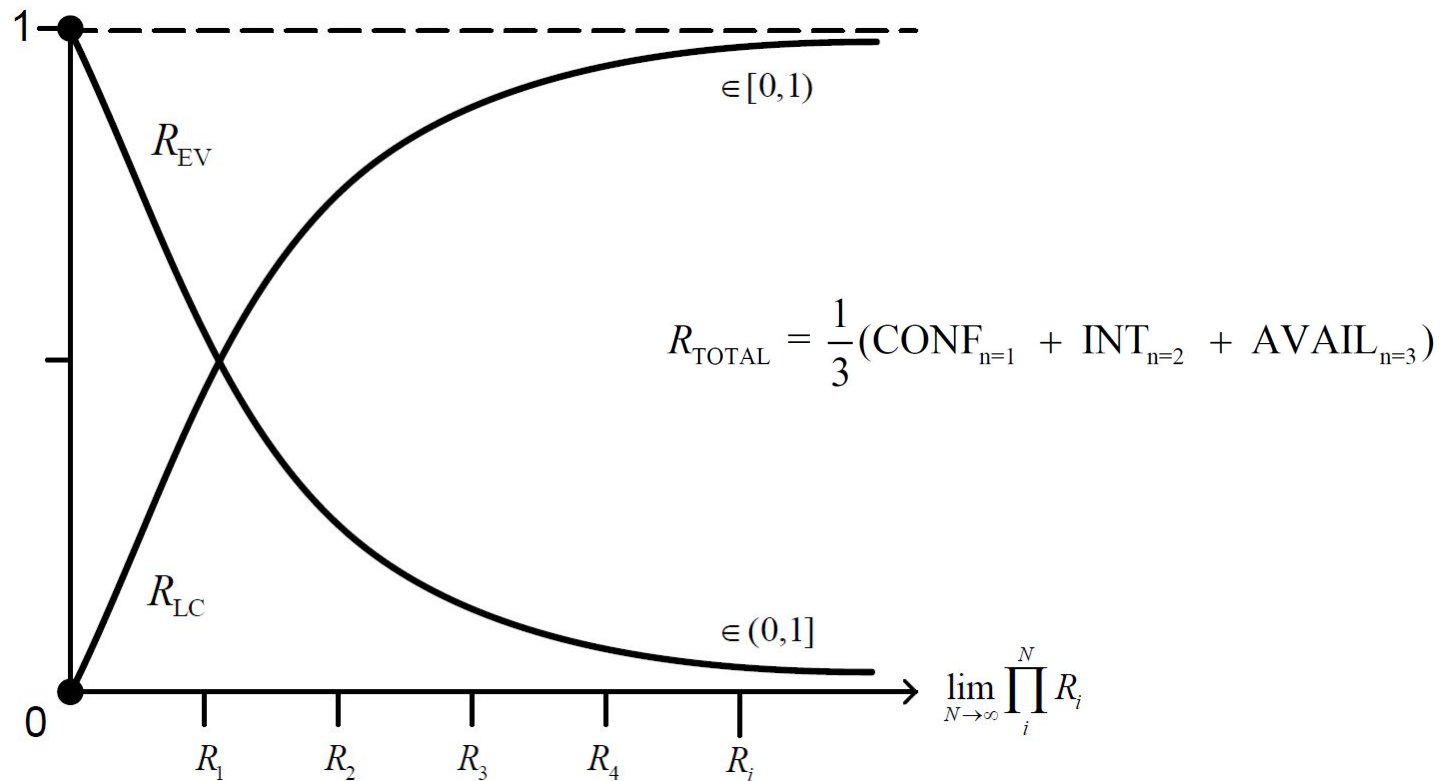
$$\text{Risk} \neq 0$$

- Risk Dimension (units): confidence in ISS, C-I-A

$$\text{Risk}_{\text{EV}} = 100\% - (\text{Risk Loss Confidence})$$

# Advanced Topics: Measuring Risk

- Expected Value and Risk Loss Confidence vs Cumulative Risk Product



$$R_{LC} = 1 - R_{EV}$$

# Advanced Topics: Measuring Risk

- Quantitative Risk Determination Expression

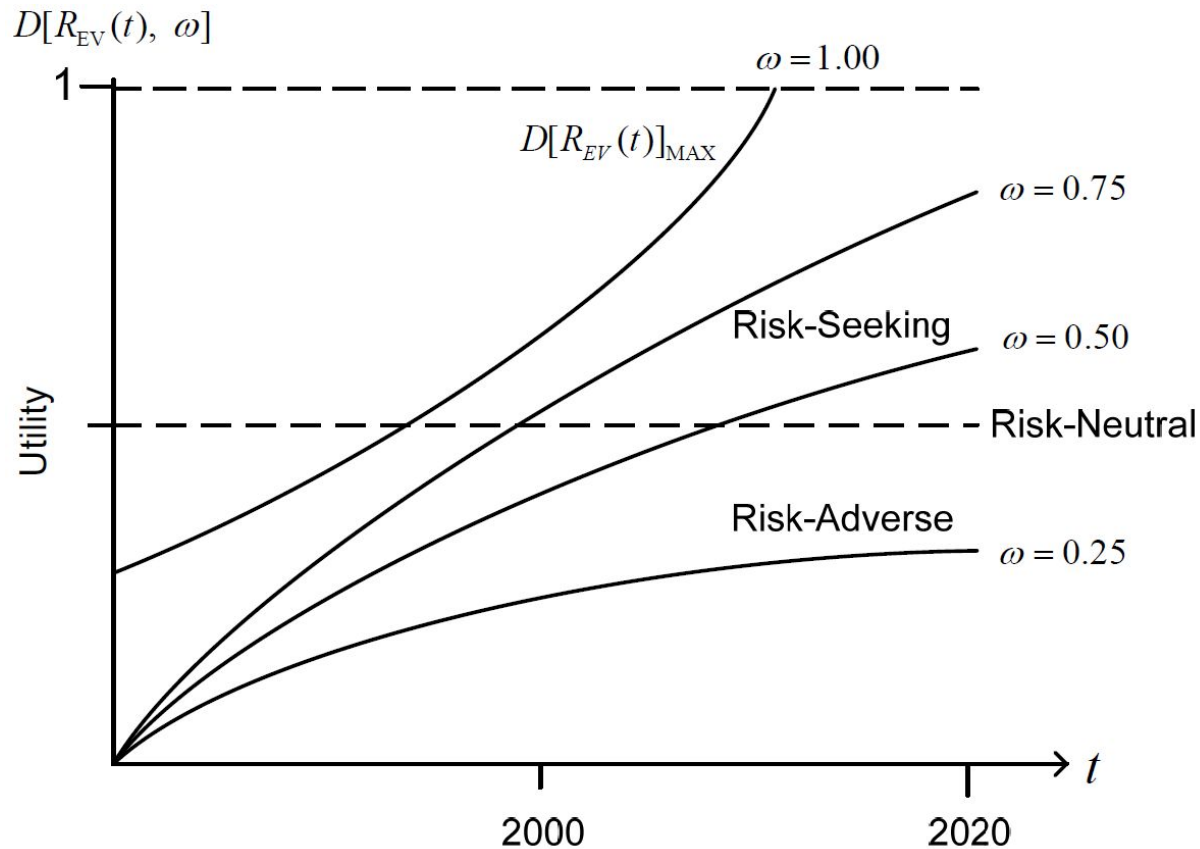
$$D(R) = R_{s,i}(t) \cdot \frac{dR_{s,i}(t)}{dt} \cdot \frac{d^2 R_{s,i}(t)}{dt^2}$$

- Risk Rate & Risk Variability
- Adjudication of Risk



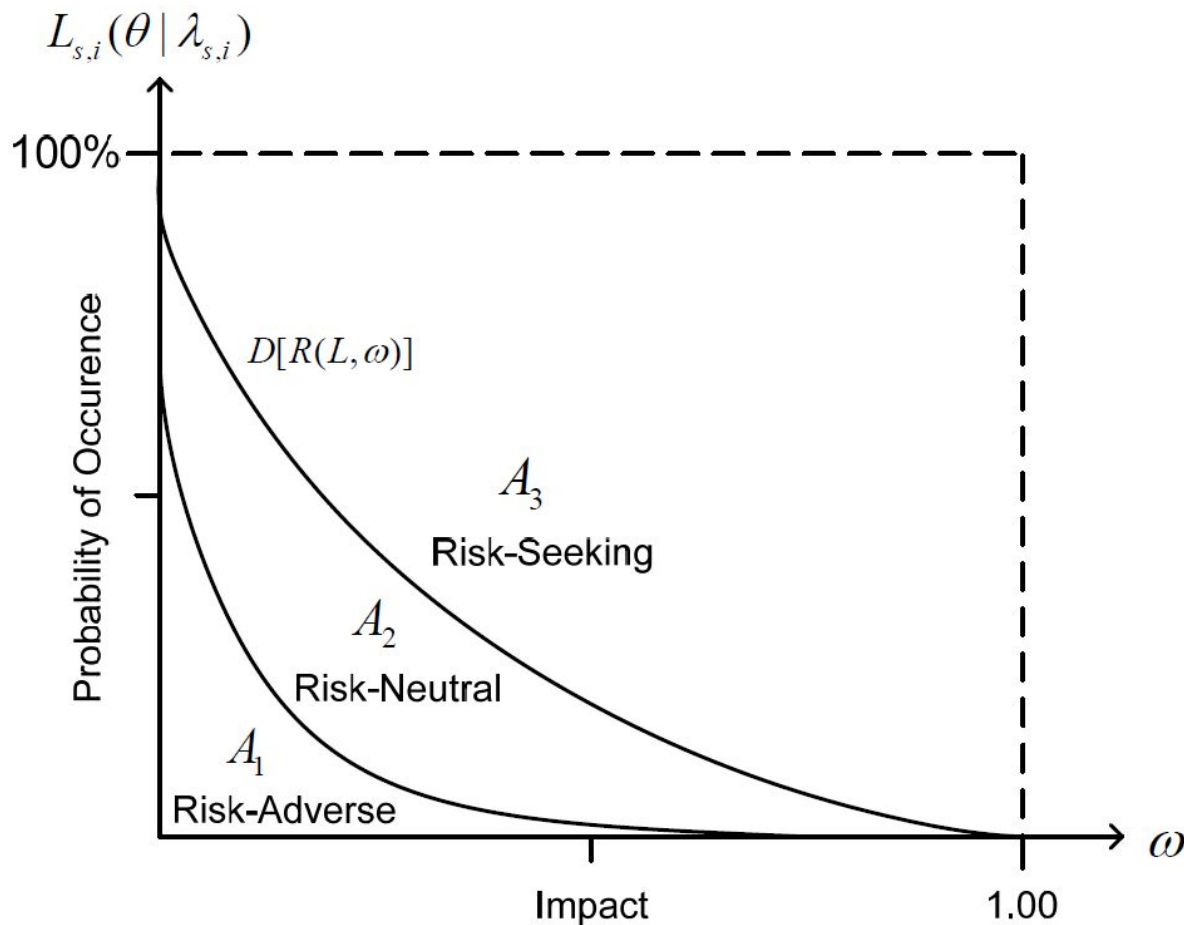
# Advanced Topics: Measuring Risk

- Determining Risk Tolerance / Threshold Levels



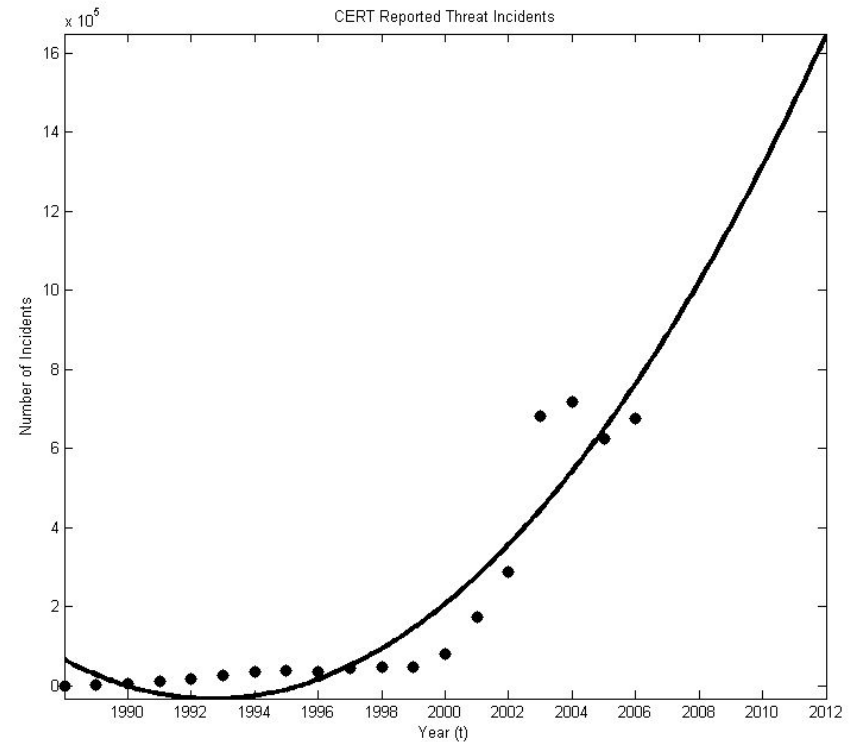
# Advanced Topics: Measuring Risk

- Risk Areas as a function of Probability and Impact



# Present Challenges

- Rapid growth of Advanced Persistent Threats (APTs)
- Half million cases of cyber related incidents in 2012.
- Is this a problem?
- What about vulnerabilities associated with interconnections?

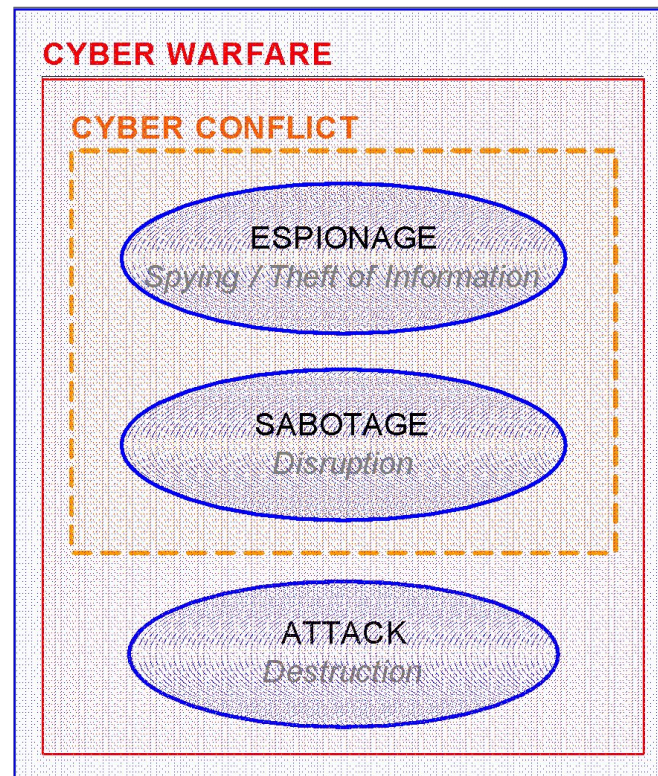


Source: US-CERT

# Future Challenges

- Cyberspace: Are we at war?
- **Cyber Crime** vs **Cyber Warfare** vs **Cyber Conflict**

## CYBER CRIME



# Closing Thoughts

- Information Systems Security (Cyber Security) is an *explosive* field.
  - Spanning Commercial, Private and Government Sectors
  - Demand >> Capacity: Strategies, solutions, workforce
  - \$
  - Evolving field (not fully matured)
- Security will change our communications landscape
  - Efficiencies (centralization of services, technology)
  - Intelligent design of network interconnections and interdependencies
  - Regulations