# Cybersafety

University of Phoenix®

# 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.

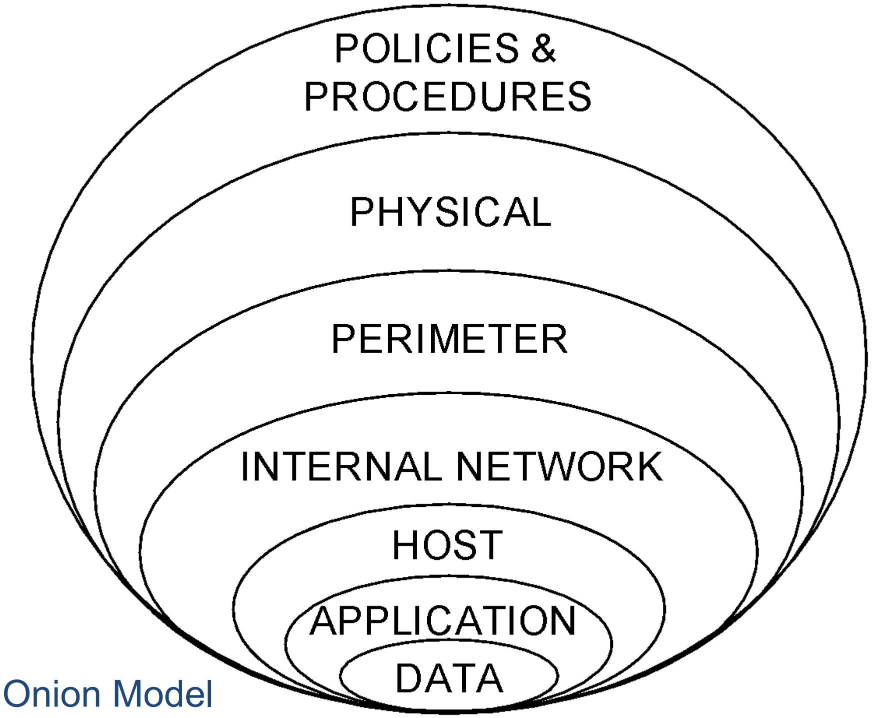
# Review of Concepts

- Progression of Terminology

| | |
|---|---|
| Computer Security (COMPUSEC) | Legacy Term (no longer used). |
| ⇩ | |
| Information Security (INFOSEC) | Legacy Term (still used). |
| ⇩ | |
| Information Assurance (IA) | Term widely accepted today with focus on Information Sharing. |
| ⇩ | |
| Cyber Security | Broad Term quickly being adopted. |

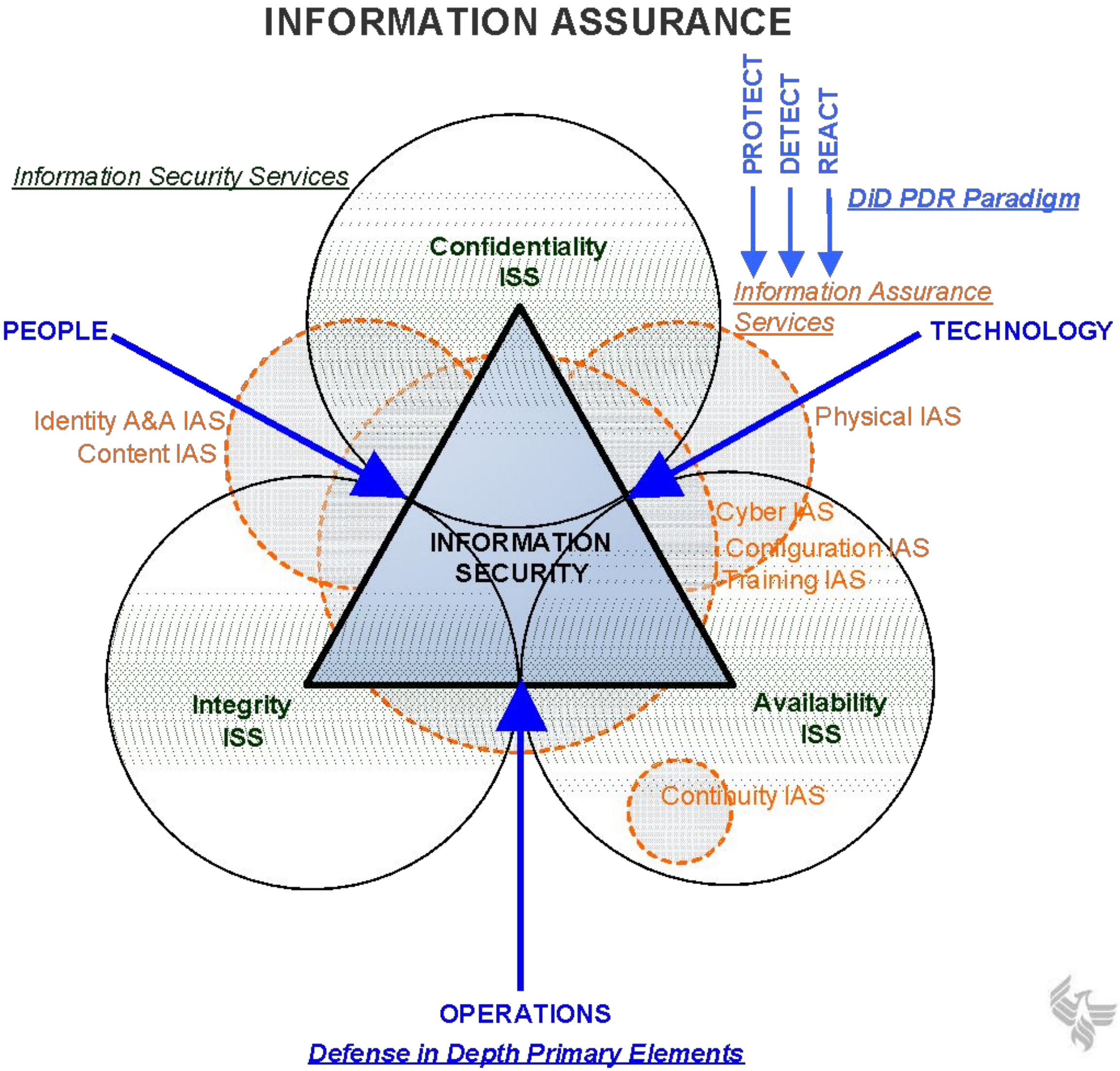
# Review of Concepts

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



Onion Model

# Review of Concepts



# 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*,

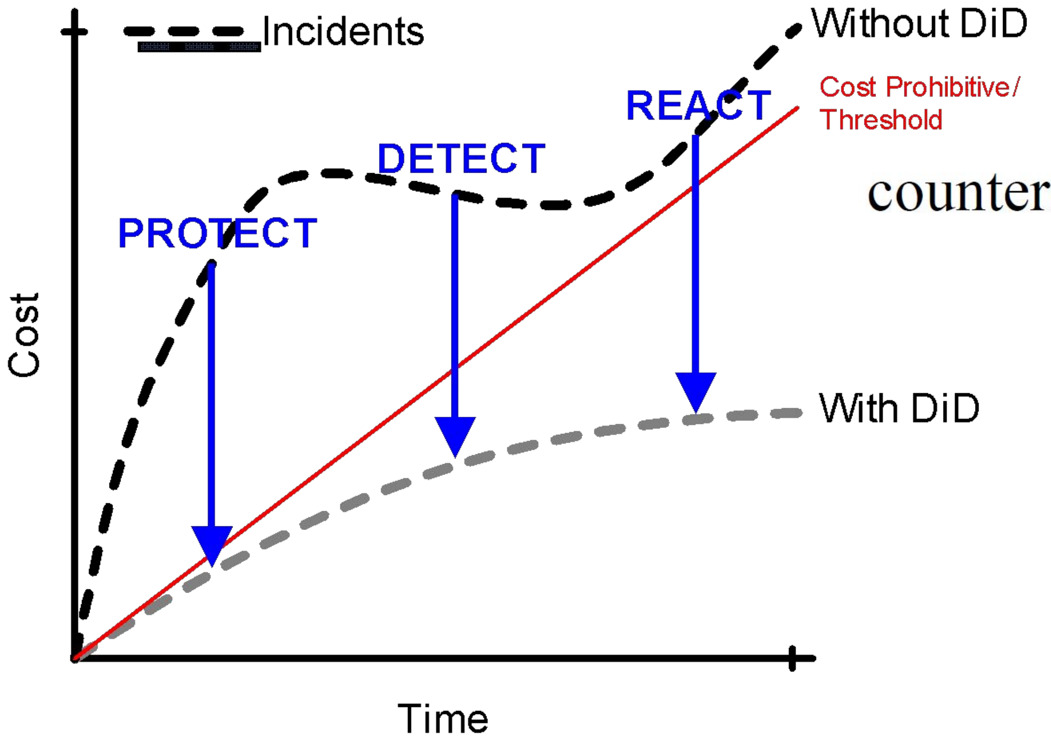
- Information Systems are valuable.

*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



countermeasure costs < potential loss

# Advanced Topics: Measuring Risk

- What is Risk?

$$\text{Risk} = -\text{Opportunity}$$

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

*thus*

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

- 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.

$$\text{Risk} \neq \boxed{\text{Threats} \times \text{Vulnerabilities}} \times \text{Impact}$$

$$\begin{aligned}\text{Risk}_{\text{EV}} &\neq \sum_{n} \omega_{i,n} \cdot \mathrm{P}_i\left(\lambda_i\right) \cdot \mathrm{P}_i\left(\theta_i\right) \\ &= \sum_{n} \omega_{i,n} \cdot \mathrm{P}_i(\lambda_i | \theta_i)\end{aligned}$$

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

# Advanced Topics: Measuring Risk

- Quantitative, time-dependent (continuous),

Risk Distribution Function:

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

*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

$$\mathrm{Risk}_{\mathrm{EV}} = \prod_{i}^{N} R_i$$

- Risk is never zero

$$\lim_{N \to \infty} \mathrm{Risk}_{\mathrm{EV}} \simeq 0$$

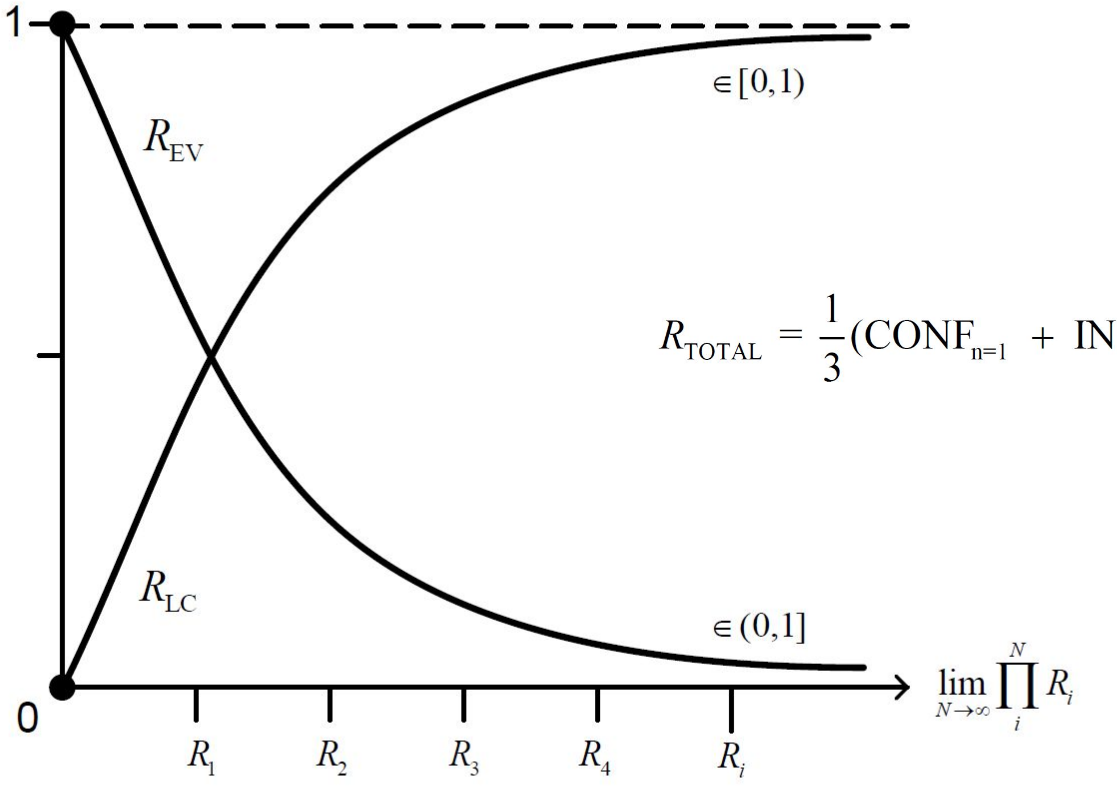
$$\mathrm{Risk} \neq 0$$

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

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

# Advanced Topics: Measuring Risk

- Expected Value and Risk Loss Confidence vs Cumulative Risk Product



$$R_{\mathrm{TOTAL}} = \frac{1}{3}(\mathrm{CONF}_{\mathrm{n=1}} + \mathrm{INT}_{\mathrm{n=2}} + \mathrm{AVAIL}_{\mathrm{n=3}})$$

$$\mathrm{R}_{\mathrm{LC}} = 1 - \mathrm{R}_{\mathrm{EV}}$$

# Advanced Topics: Measuring Risk

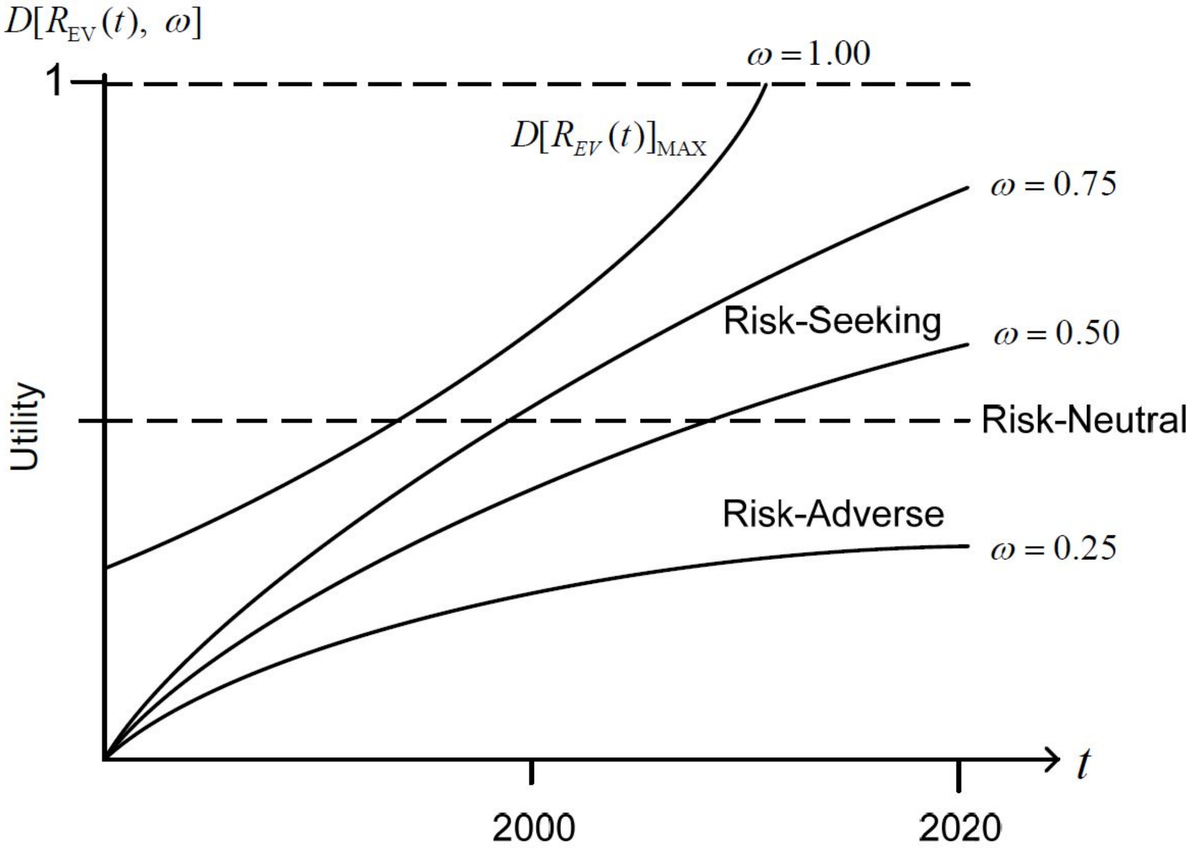
- Quantitative Risk Determination Expression

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

- Risk Rate & Risk Variability
- Adjudication of Risk

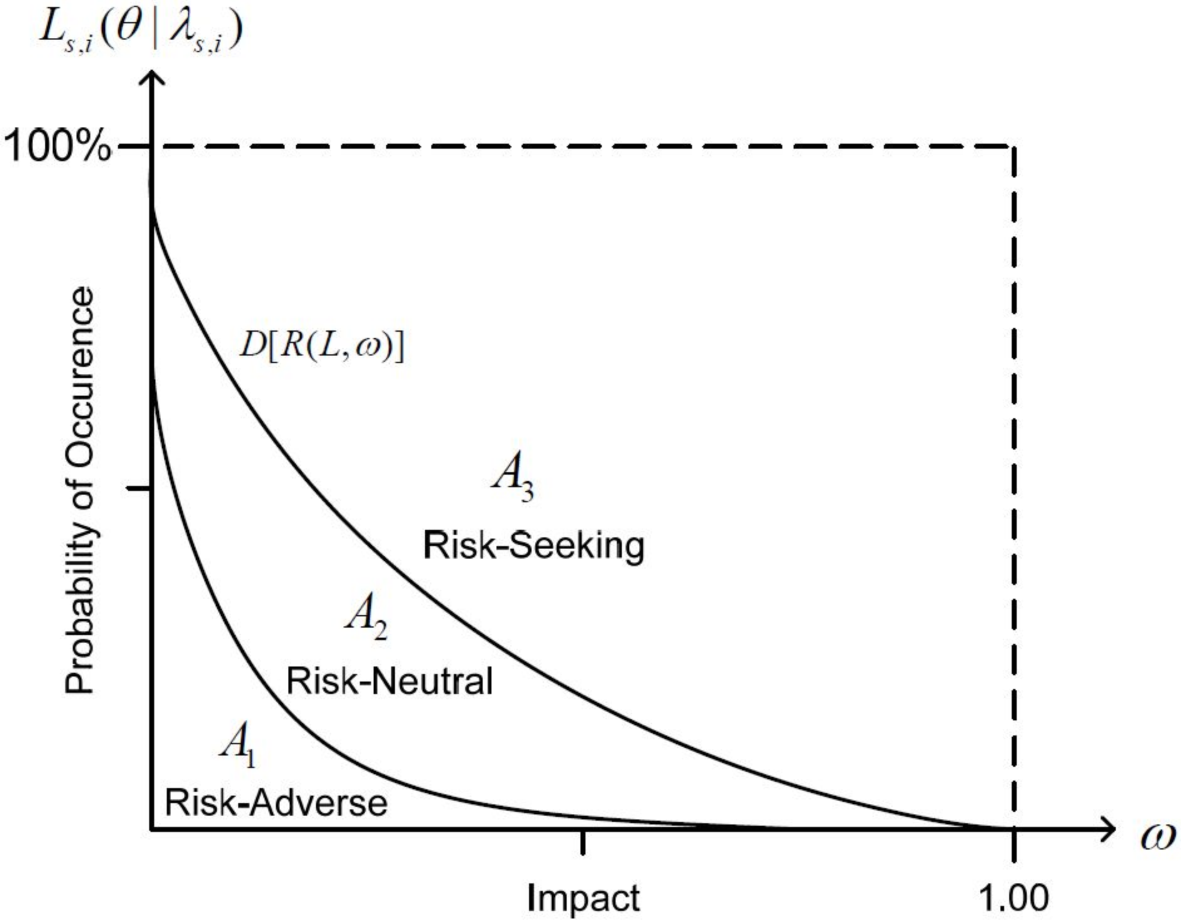
# Advanced Topics: Measuring Risk

- Determining Risk Tolerance / Threshold Levels



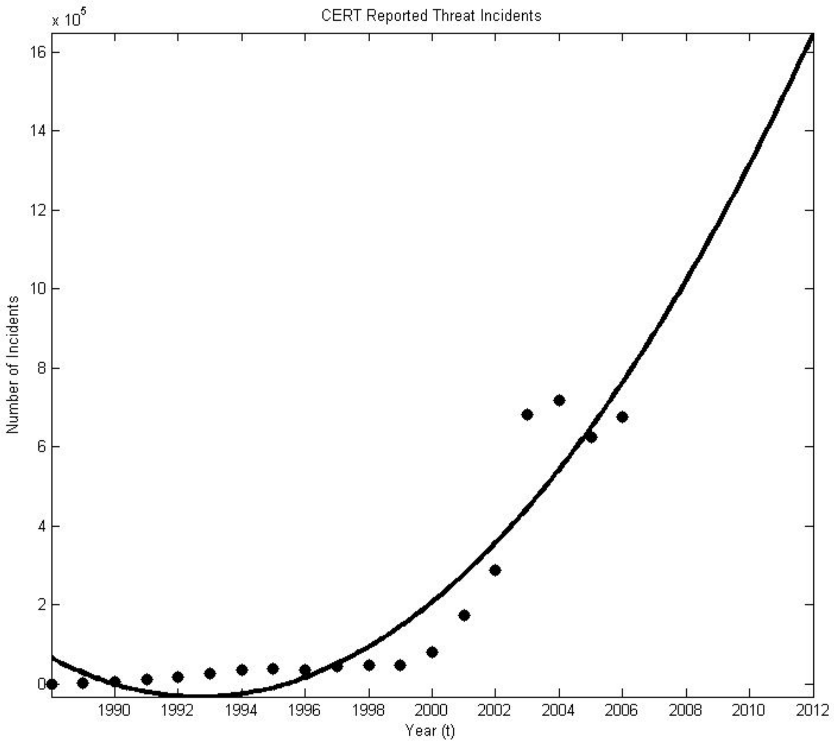
# Advanced Topics: Measuring Risk

- Risk Areas as a function of Probability and Impact



# Present Challenges

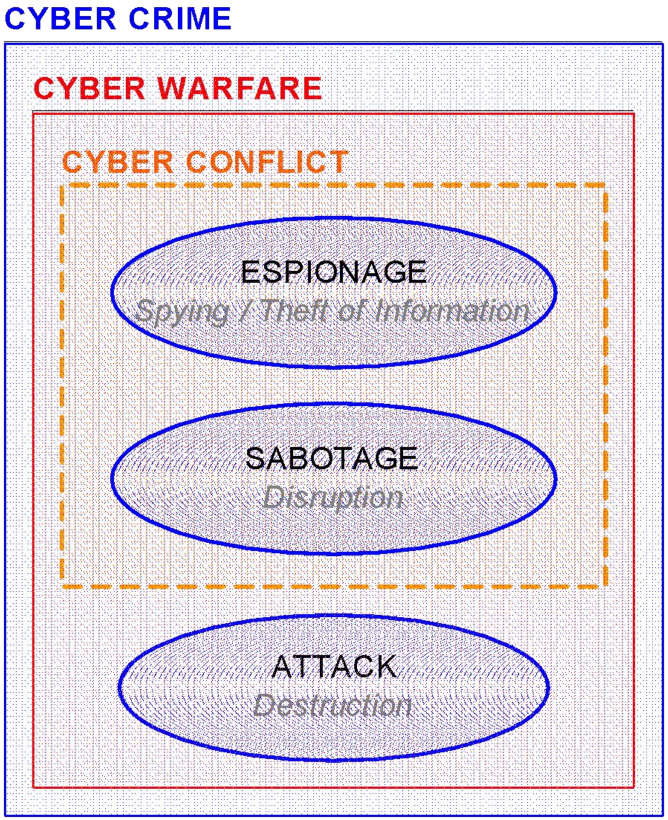
- Rapid growth of Advanced Persistent Threats (APTs)
- Half million cases of cyber related incidents in 2012.
- Is this a problem?
- What about vulnerabilities associated with interconnections?



*Source:* US-CERT

# Future Challenges

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



# 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