Information Assurance and Security:

An Introduction

El-Sayed M. El-Alfy

Associate Professor and ISRG Coordinator
King Fahd University of Petroleum and Minerals
alfy@kfupm.edu.sa

SEC 511 – Fall 2015 (151)

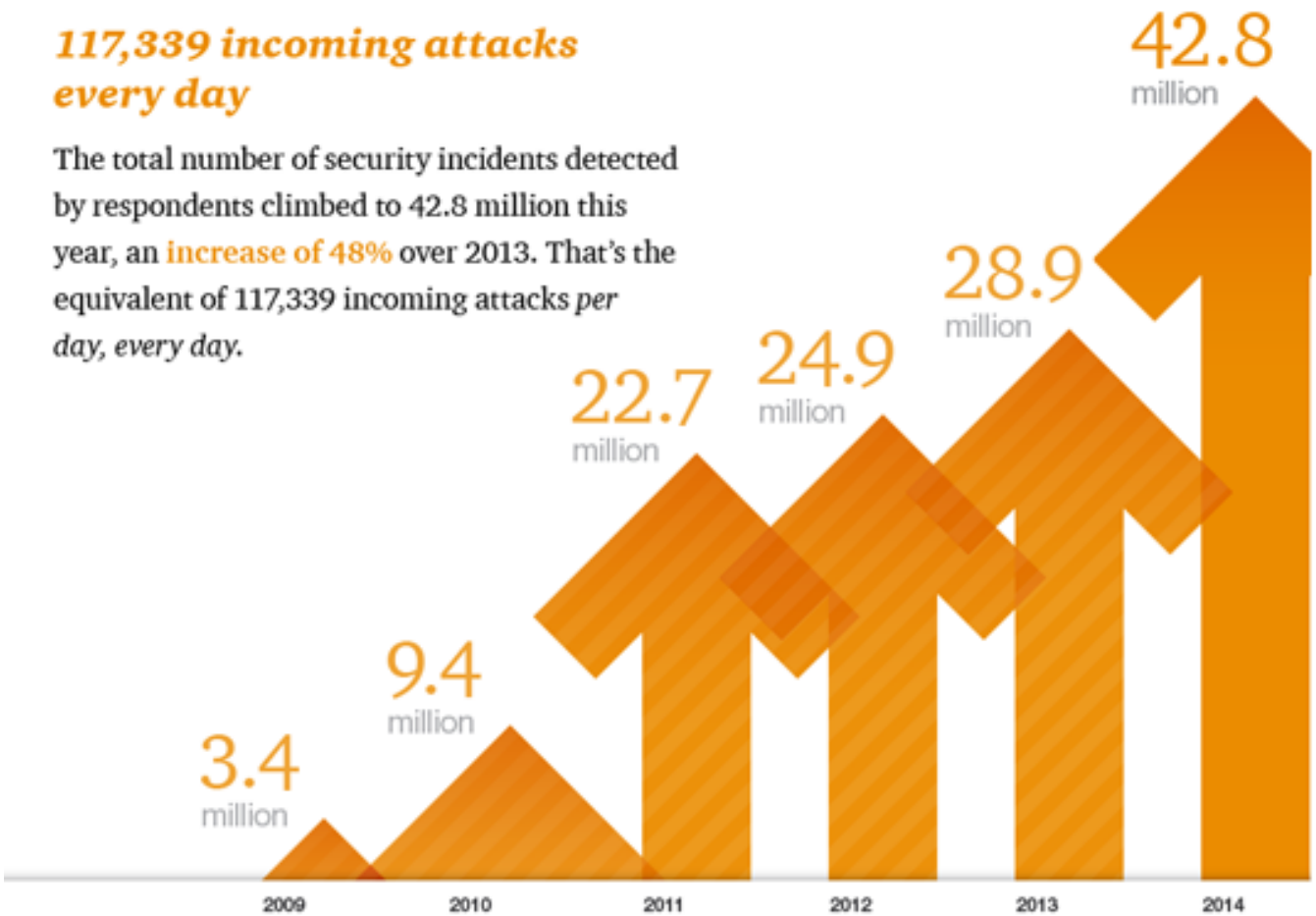
Presentation Outline

Warm-UP: Question & Attendance

Socrative Student

Teacher

Volume & Trend



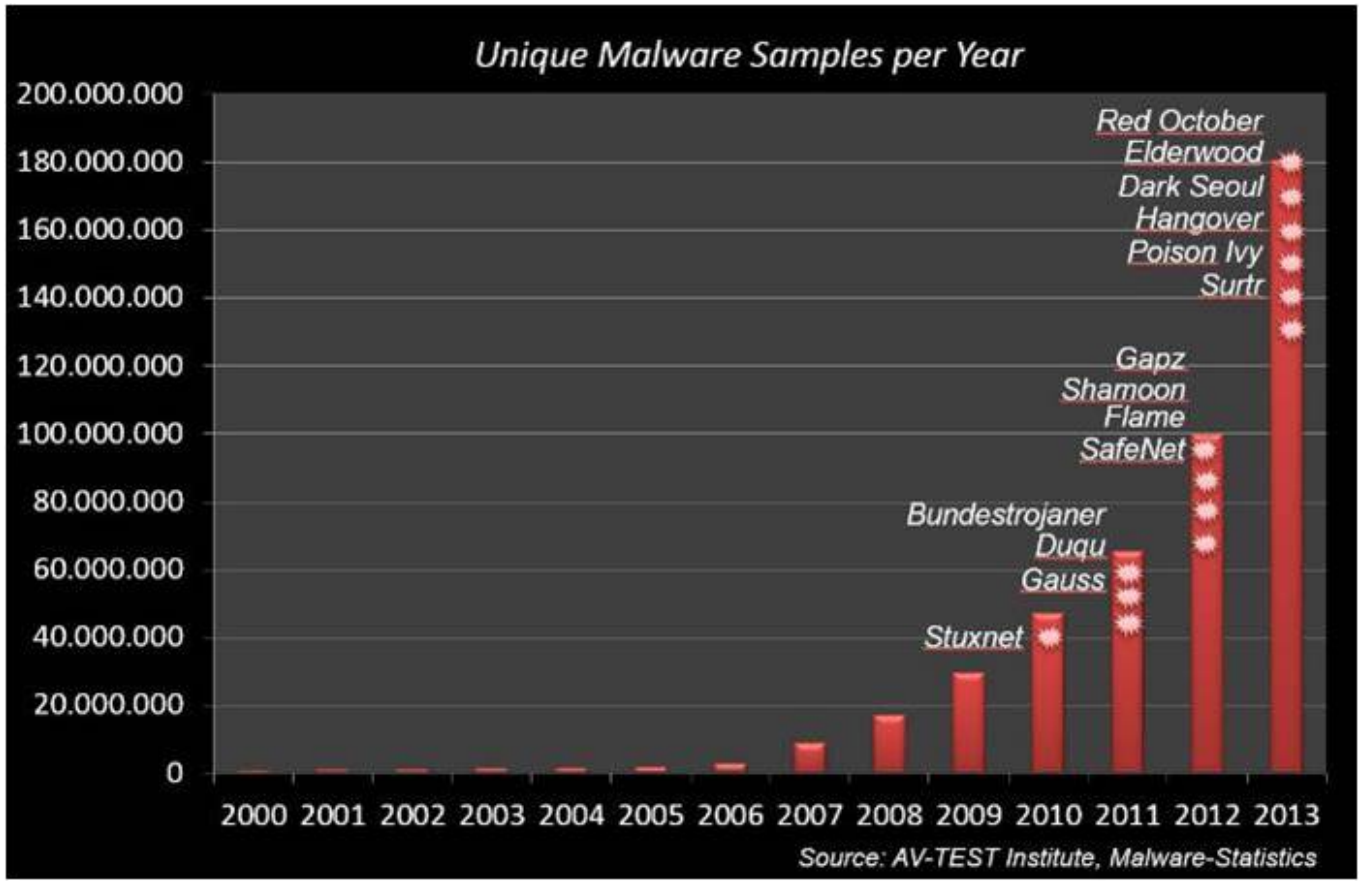
Src: Global State of Information Security Survey 2015

Some Figures

- $8.9 million the annual avg cost of cyber crime for a global company.
- $300 billion – $1 trillion the low to high cost estimate of how much is lost globally through cyber crime on an annual basis, as calculated by McAfee in 2012.
- 55% of UK companies have been a victim of data theft in the past year.
- £600,000 to £1.2 million the average cost of a large UK organization's worst data breach last year
- 556 million individuals victims of cyber crime in 2012
- $110 billion the amount of money stolen from consumers on the web around $197 per person.
- 1509934 new viruses appeared in the first half of 2013 (20% higher than the second half of 2012)

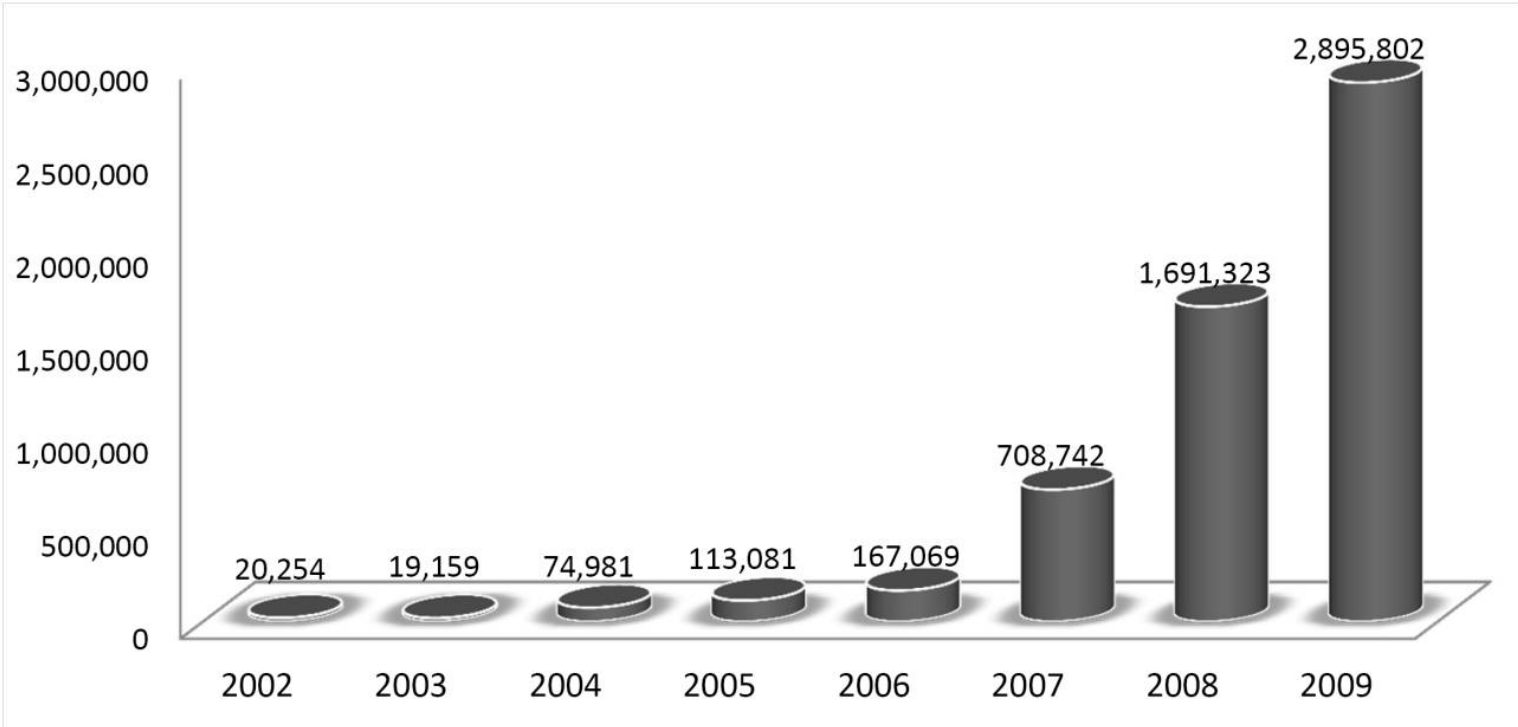
Src: Infographic

Trend & Some Reported Incidents



Trend & Some Reported Incidents

New malware signatures



Src: : Symantic Corp

Trend & Some Reported Incidents

Regional incidents

40% of IT decision makers in Saudi Arabia have been exposed to DDoS

Read more

Trend & Some Reported Incidents

Regional incidents

Hack on Saudi Aramco hit 30,000 workstations on August 15, 2012, ... Read more

Trend & Some Reported Incidents

Regional incidents

In June 2010 Stuxnet computer worm infected the software of at least 14 industrial sites in Iran ...

Watch TED video to learn more

Read more at wikipedia ... and IEEE Spectrum

Trend & Some Reported Incidents

Historical global incidents

- Oct 2013: Adobe servers penetrated (code as well as details of 38 million customer accounts are compromised)
- Sept. 2013: A file containing 2 million customers' data is stolen from Vodafone Germany
- Oct. 2012: Creation of a citizen's cyber defense network in France (organization of volunteers and experts, comprised of 6 WGs) to communicate and advise nation and French army on cyber defense and security
- May 2012: Elysee (the official residence of the French president) becomes victim of a cyber attack between the two rounds of presidential elections

Trend & Some Reported Incidents

More historical global incidents

- Apr 2011: Sony's PlayStation network becomes victim of a major cyber attack (network stays closed for over a month after 77 million items of data, including banking information, are stolen)
- Jun 2010: Stuxnet infected Siemens equiement at Iranian nuclear plants
- 1994: Vladimir Levin, a Russian mathematician, managed to penetrate the database for Citibank (moved $10 million into foreign accounts before being arrested)
- 1983: Kevin Mitnick is arrested by US police after getting into the internal network of the Pentagon

Definitions

IA Definition
Debra Herrmann View

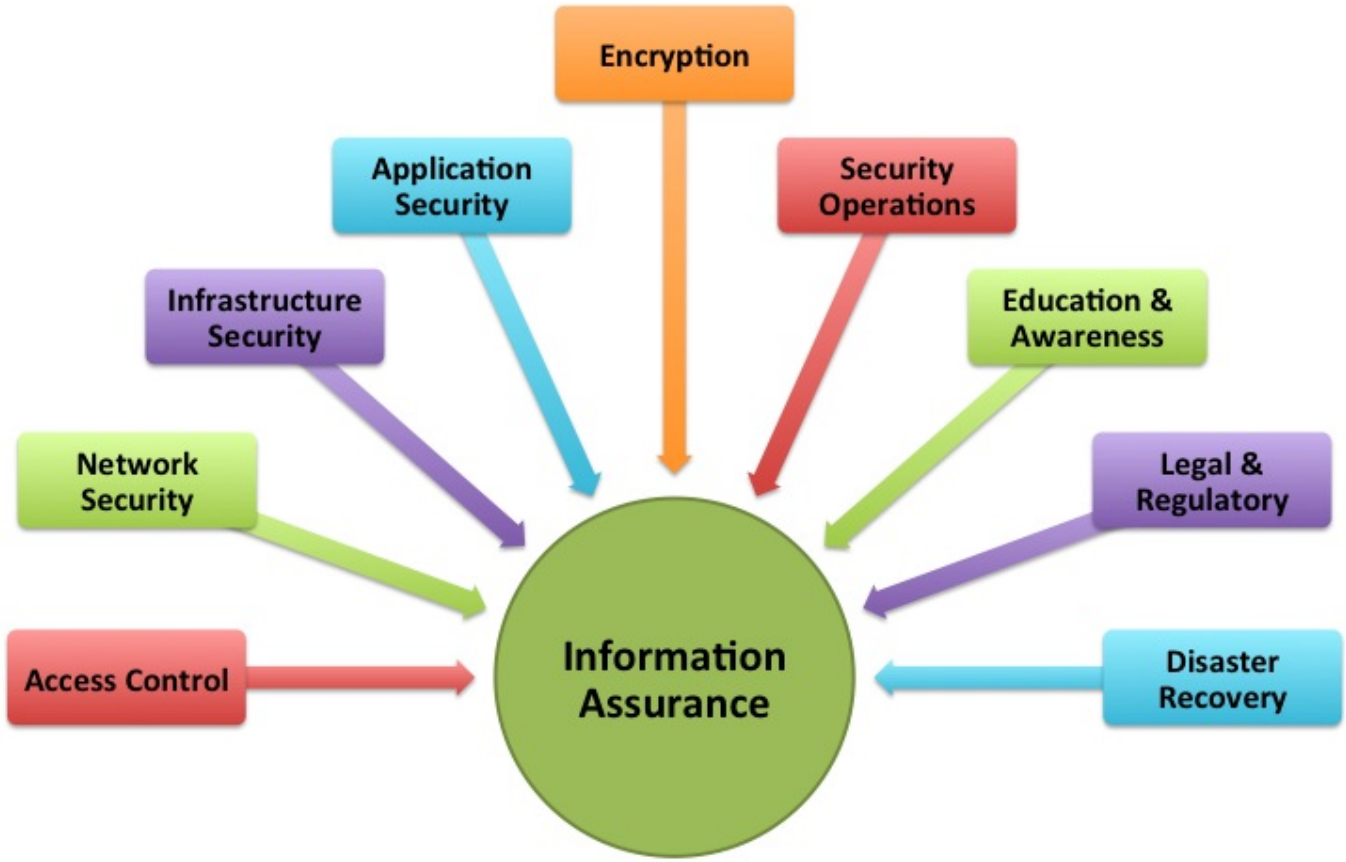
→ IA is a broad field that there is no universally accepted definition.
→ Researchers often give their own spin to IA, usually reflecting their own concerns.
→ e.g. Debra Hermann: IA should be viewed as spanning four security engineering domains:

- physical security
- personnel security
- IT security
- operational security

Debra S. Herrmann, Complete Guide to Security and Privacy Metrics: Auerbach, 2007.

IA Definition

Another view



IA Definition
US DoD View

According to US DoD, IA involves: Actions taken that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

- protect information assets from destruction, degradation, manipulation, and exploitation
- also capability to recover if any of those happen
- both proactive and reactive

Src: NIST Glossary of Information Security Terms

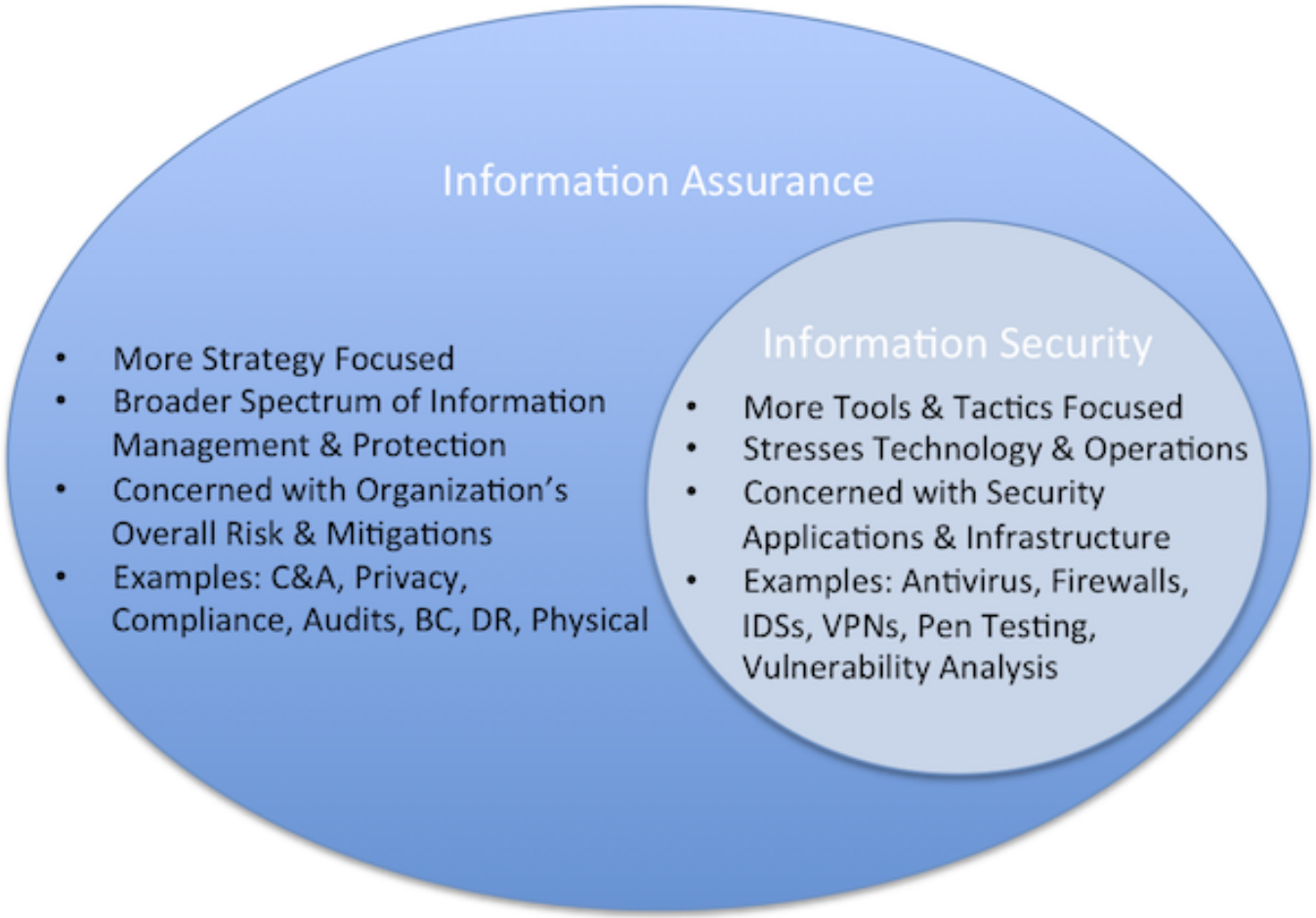
IS Definition

According to NIST Glossay of IS Terms:
The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, destruction in order to provide:

- confidentiality
- integrity
- availability

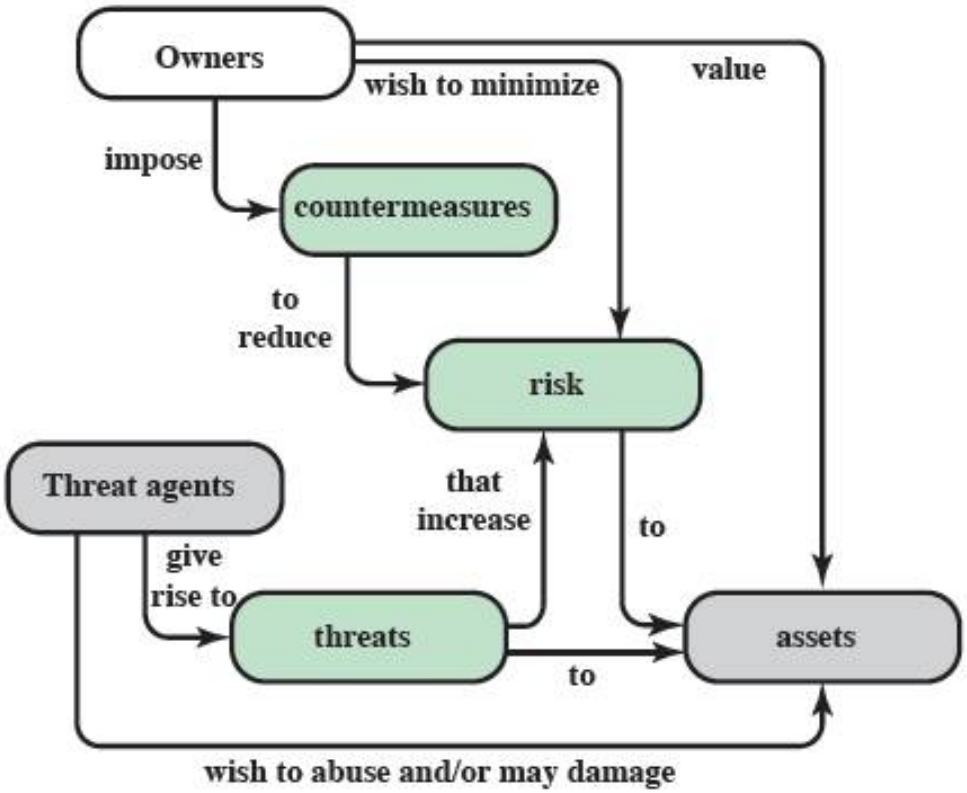
Src: NIST Glossary of Information Security Terms

IA vs. IS



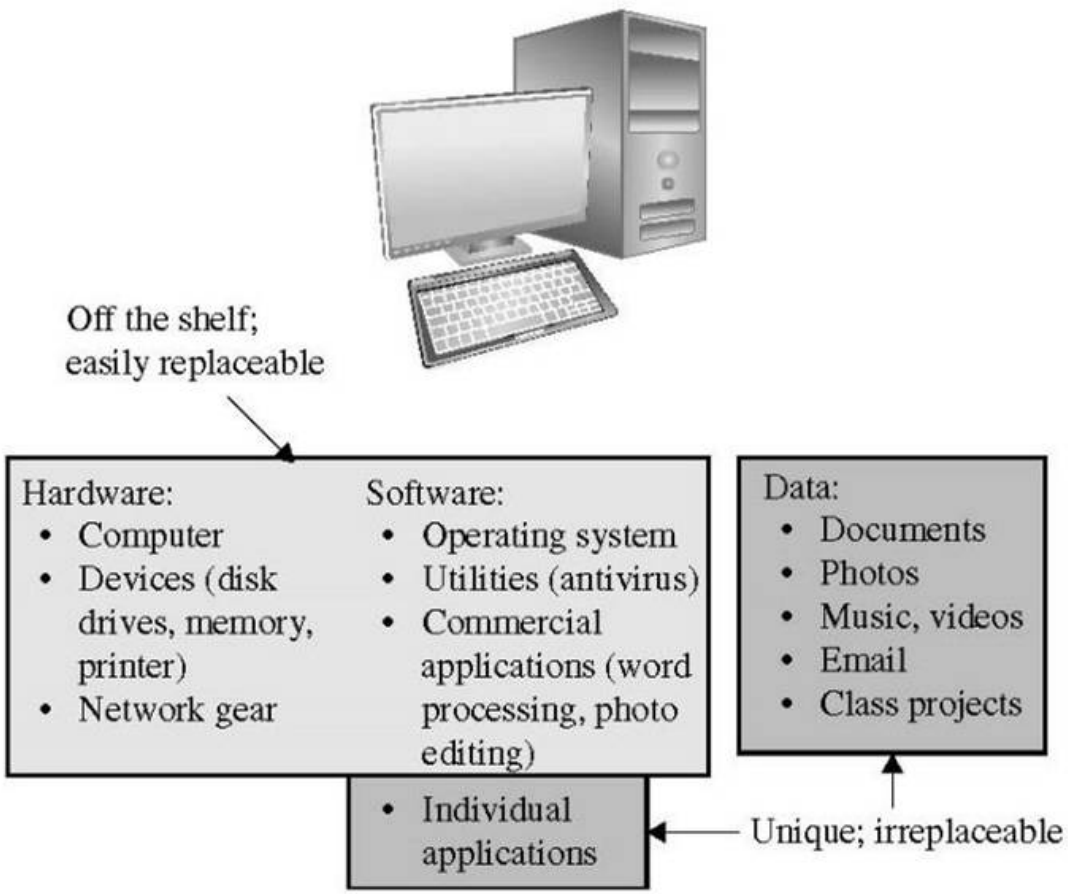
Src: NoVa InfoSec

Whole Picture



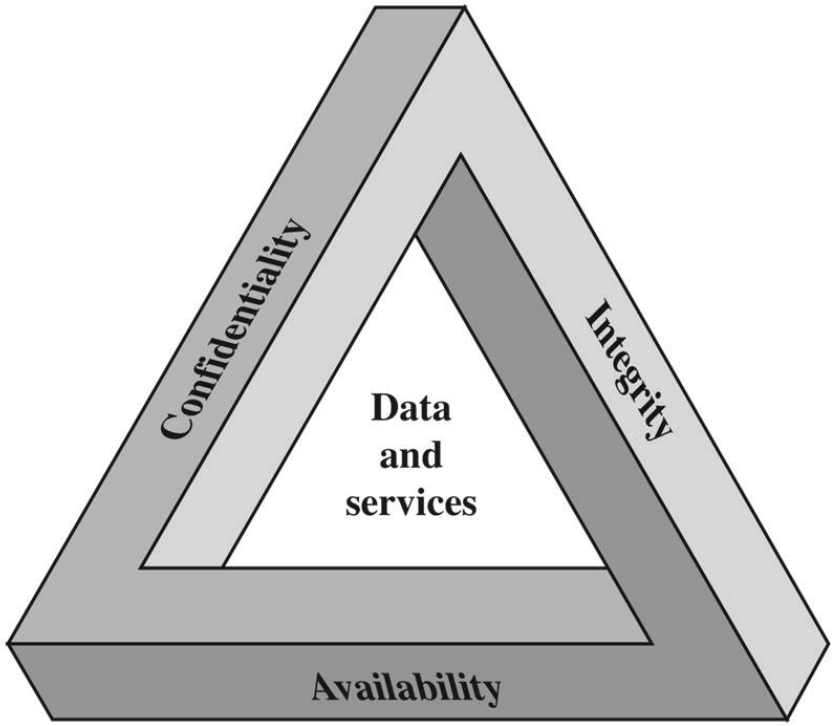
Src: Computer Security: Principles and Practice, 3/E, Stallings & Brown, 2014

Assets & Values



Src: Analyzing Computer Security, Charles Pfleegerand Lawrence Pfleeger, 2012

Goals: CIA Triad



Src: Analyzing Computer Security, Charles Pfleegerand Lawrence Pfleeger, 2012

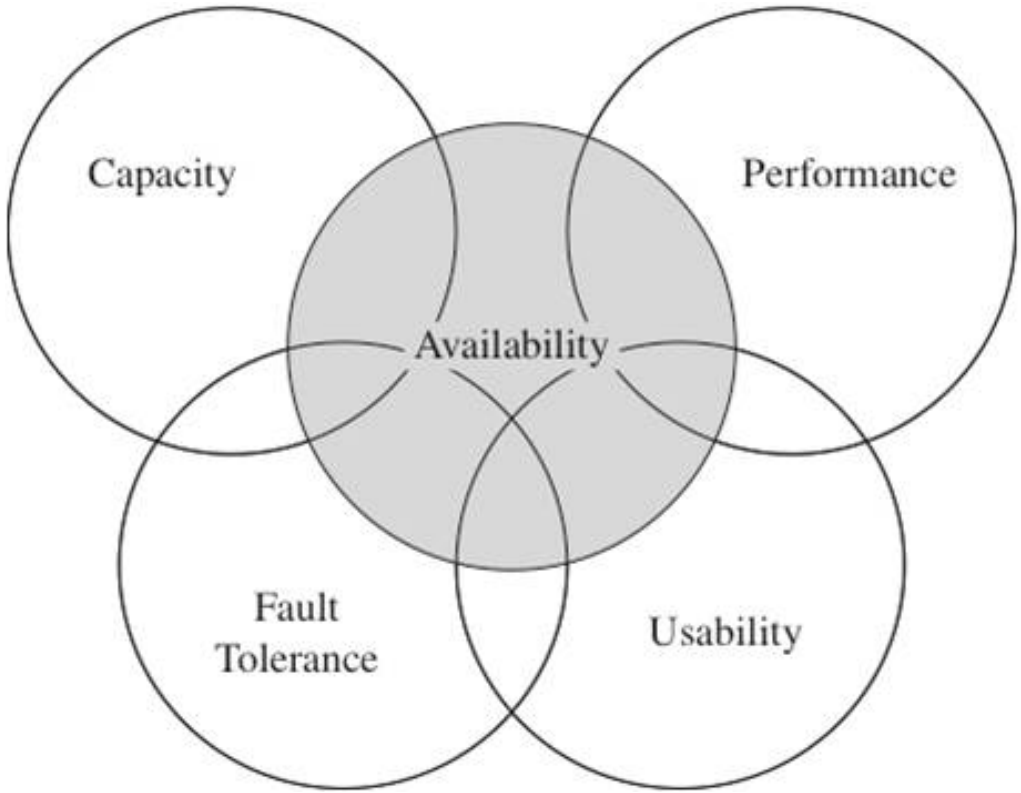
Goals: CIA Triad

CIA and More

- Availability: timely, reliable access to data and information services for authorized users
- Integrity: protection against unauthorized modification or destruction of information
- Confidentiality: assurance that information is not disclosed to unauthorized persons
- Authentication: security measures to establish the validity of a transmission, message, or originator
- Non-repudiation: assurance that the sender is provided with proof of a data delivery and recipient is provided with proof of the senderŠs identity, so that neither can later deny having processed the data.

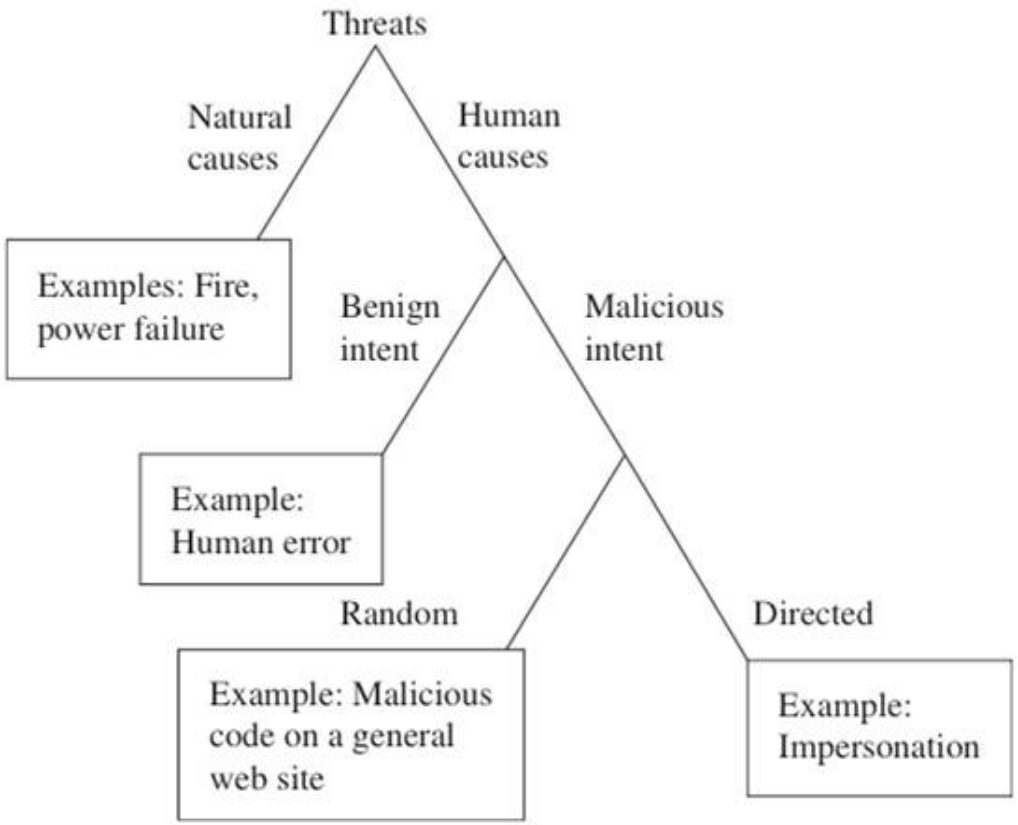
Goals: CIA Triad

Availability overlap with other quality factors



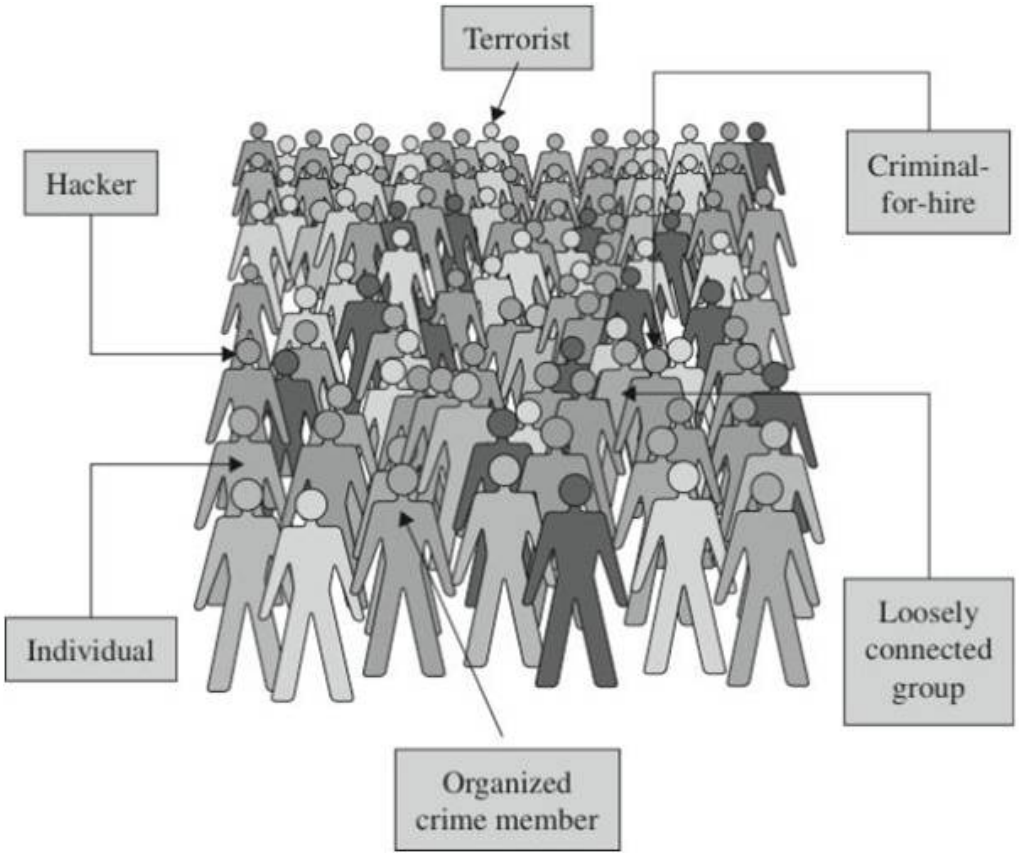
Src: Analyzing Computer Security, Charles Pfleegerand Lawrence Pfleeger, 2012

Kinds of Threats



Src: Analyzing Computer Security, Charles Pfleeger & Lawrence Pfleeger, 2012

Attackers Categories

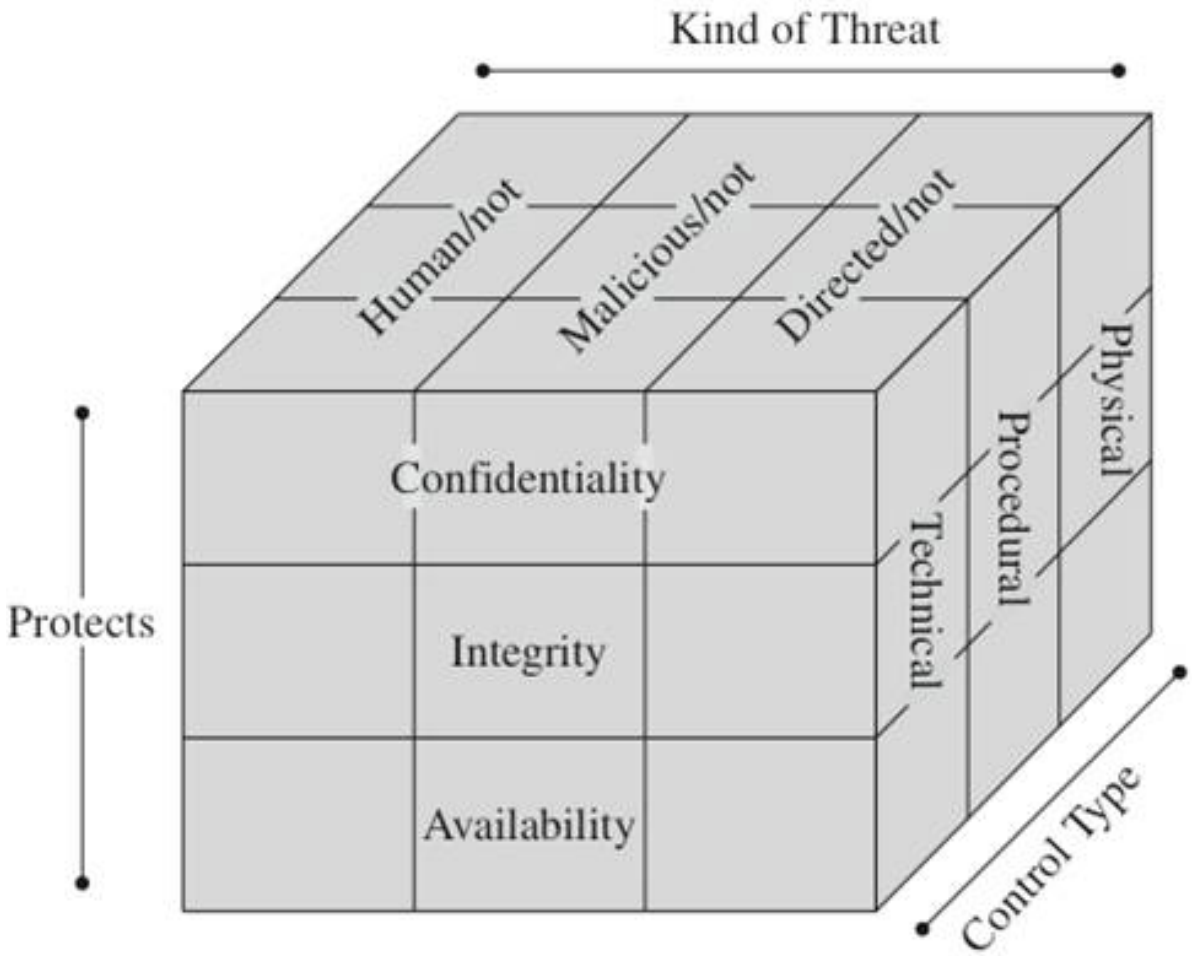


Src: Analyzing Computer Security, Charles Pfleeger & Lawrence Pfleeger, 2012

Motive-Opportunity-Method

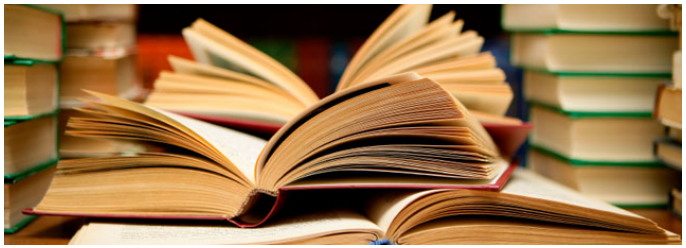
Src: Analyzing Computer Security, Charles Pfleeger & Lawrence Pfleeger, 2012

Threat-Goals-Control



Src: Analyzing Computer Security, Charles Pfleeger & Lawrence Pfleeger, 2012

Reading Assignment



Reading: Read Chapter 1: Principles of Information Security
Reference: NIST Glossary of Key Information Security Terms and other reports at NIST Computer Security Division