Unit #0b
Threat Environment

MIS5214 – Security Architecture

Unit 0b – The Threat Environment

Readings

- Boyle and Panko: Chapter 1 The Threat Environment
- Ross, J.W., Weill P., and Robertson D.C. (2008), "Implement the Operating Model Via Enterprise Architecture" (in the Harvard Business Publishing course pack)
- NIST SP 800-100 "Information Security Handbook: A Guide for Managers", Chapter 10 Risk Management pp.84-95

Agenda

- Terminology
- Threat environment
- Hacker mindset
- More terminology
- Security architecture
- Next steps…

Introductory Terminology

"Information security" is protection of…

- Confidentiality, integrity, and availability ("CIA") of data and information
- Data, information and information systems from unauthorized…
  - Access, use, disclosure = **Confidentiality**
  - Modification = **Integrity**
  - Disruption or destruction = **Availability**

INTEGRITY
AVAILABILITY
CONFIDENTIALITY

Terminology: Security Goals

Confidentiality

- Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network

Terminology: Security Goals

Integrity

- ➢Integrity means that attackers cannot change or diminish information, either while it is on a computer or while it is traveling across a network
- ➢Or, at least, if information is changed or diminished, then the receiver can detect the change and possibly restore the data

Terminology: Security Goals

Availability

- ➢People who are authorized to use information are not prevented from doing so

Terminology: Compromises

- Successful attacks
- Also called incidents
- Also called breaches (not breeches)

Terminology: Countermeasures

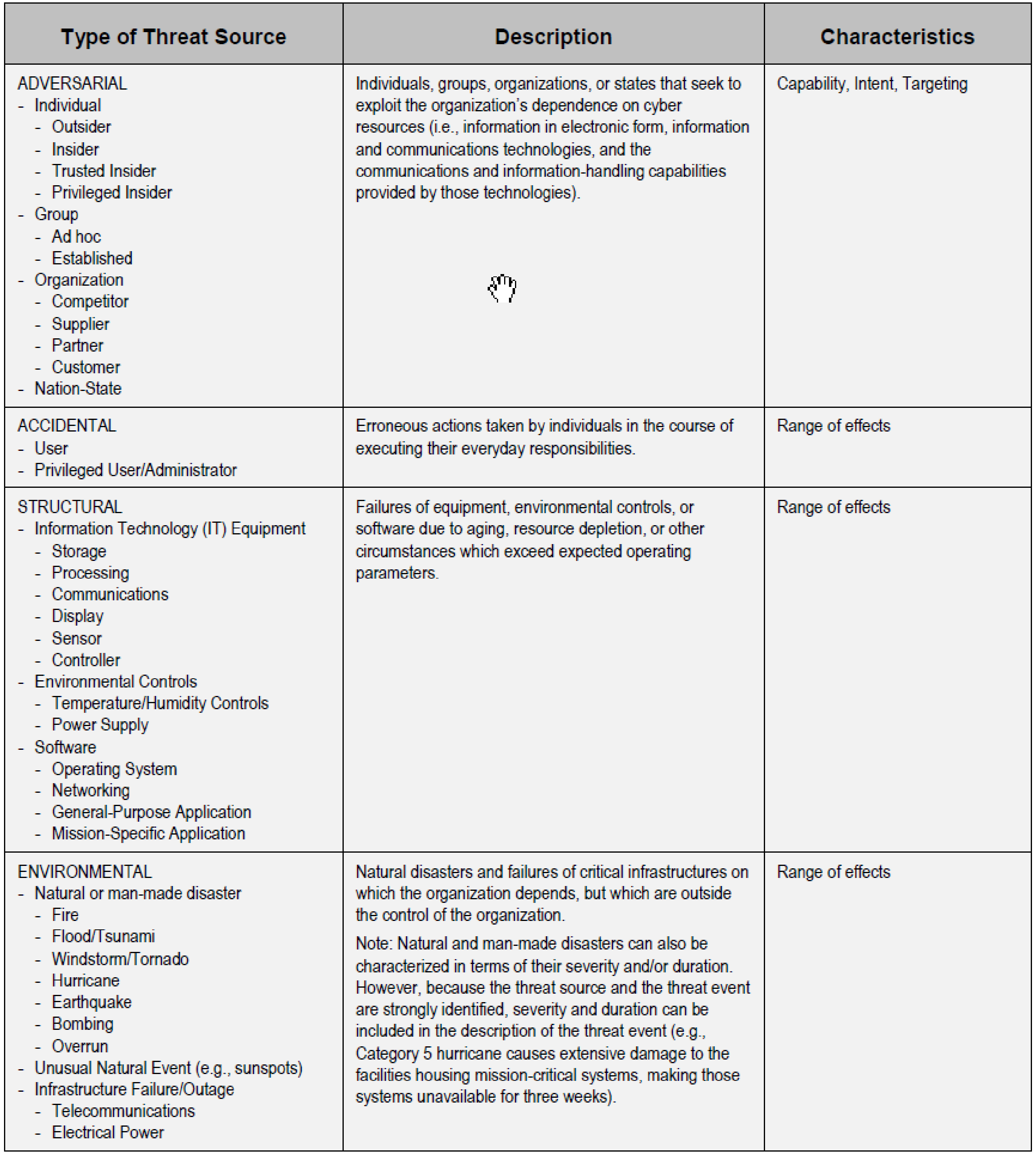
- Tools used to thwart attacks
- Also called safeguards, protections, and controls
- Types of countermeasures
  - Preventative
  - Detective
  - Corrective

Agenda

✓Terminology
- Threat environment
- More terminology
- Security architecture
- Next steps…

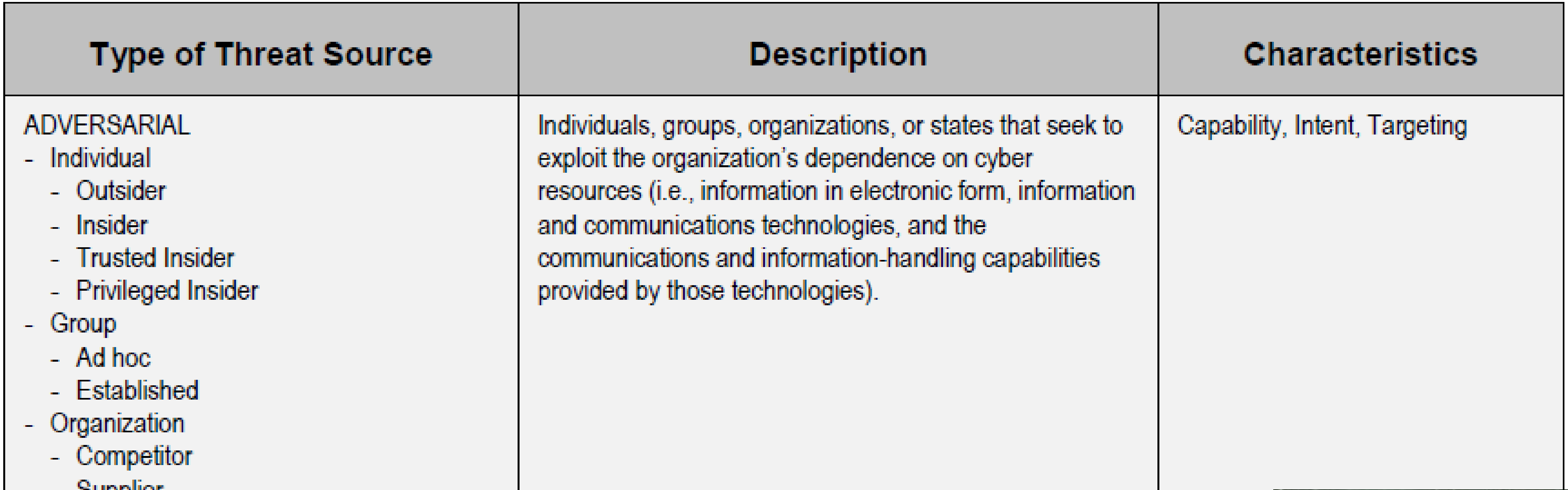
The Threat Environment

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66



Type of Threat Source	Description	Characteristics
ADVERSARIAL - Individual - Outsider - Insider - Trusted Insider - Privileged Insider - Group - Ad hoc - Established - Organization - Competitor - Supplier - Partner - Customer - Nation-State	Individuals, groups, organizations, or states that seek to exploit the organization’s dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting
ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects
STRUCTURAL - Information Technology (IT) Equipment - Storage - Processing - Communications - Display - Sensor - Controller - Environmental Controls - Temperature/Humidity Controls - Power Supply - Software - Operating System - Networking - General-Purpose Application - Mission-Specific Application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects
ENVIRONMENTAL - Natural or man-made disaster - Fire - Flood/Tsunami - Windstorm/Tornado - Hurricane - Earthquake - Bombing - Overrun - Unusual Natural Event (e.g., sunspots) - Infrastructure Failure/Outage - Telecommunications - Electrical Power	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).	Range of effects

Adversarial (i.e. purposeful) threat sources



Type of Threat Source	Description	Characteristics
ADVERSARIAL - Individual - Outsider - Insider - Trusted Insider - Privileged Insider - Group - Ad hoc - Established - Organization - Competitor - Supplier - Partner - Customer - Nation-State	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

NIST SP 800-30r1 "Guide for Conducting Risk Assessments", page 66

What type of Hacker are you?

"You need to decide if you're going to aspire to safeguarding the common good or settle for pettier goals. Do you want to be a mischievous, criminal hacker or a righteous, powerful defender?

…the best and most intelligent hackers work for the good side. They get to exercise their minds, grow intellectually, and not have to worry about being arrested. They get to work on the forefront of computer security, gain the admiration of their peers, further human advancement in the name of all that is good, and get well paid for it."

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

Most Hackers Aren’t Geniuses

“…readers often assume” bad-guy hackers are super smart, “…because they appear to be practicing some advanced black magic that the rest of the world does not know. In the collective psyche of the world, it’s as if ‘malicious hacker‘ and ‘super-intelligence’ have to go together.

A few are smart, most are average, and some aren’t very bright at all, just like the rest of the world. Hackers simply know some facts and processes that other people don’t, just like a carpenter, plumber, or electrician.”

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

Defenders are Hackers Plus

“If we do an intellectual comparison alone, the defenders on average are smarter than the attackers. A defender has to know everything a malicious hacker does plus how to stop the attack. And that defense won’t work unless it has almost no end-user involvement, works silently behind the scenes, and works perfectly (or almost perfectly) all the time.

Show me a malicious hacker with a particular technique, and I’ll show you more defenders that are smarter and better. It’s just that the attacker usually gets more press.” It’s time for equal time for the defender!

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

Hackers are Special

While not all are super-smart, “they all share a few common traits:”

- Broad intellectual curiosity
- Willingness to try things outside the given interface or boundary
- Not afraid to make their own way
- Usually they are life hackers:
  - Hacking all sorts of things beyond computers
  - Questioning the status quo and exploring all the time

- Most useful trait:
  - Persistence
  - Malicious hackers look for defensive weaknesses
  - Both malicious hackers and defenders are looking for weaknesses, just from opposite sides of the system
  - Both sides participate in an ongoing war with many battles, wins and losses. The most persistent side wins

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

The Secret to Hacking

“If there is a secret to how hackers hack, it’s that there is no secret to how they hack. It’s a process of learning the right methods and using the right tools for the job…. There isn’t even one way to do it. There is, however, a definitive set of steps that describe the larger, encompassing process”

Hacking Methodology Model

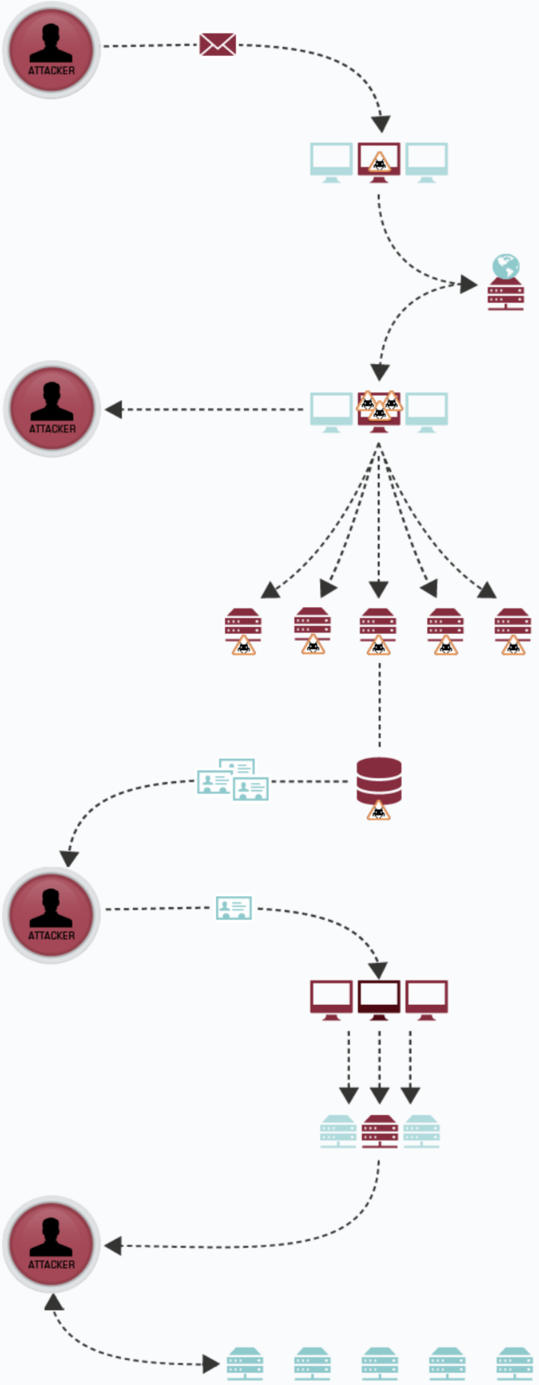
1. Information gathering (“reconnaissance”)
2. Penetration
3. *Optional: Guaranteeing future easier access*
4. Internal reconnaissance
5. *Optional: Movement*
6. Intended action execution (e.g. data exfiltration)
7. *Optional: Covering Tracks*

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

Anatomy of an Attack

(MANDIANT, 2015)

Threat landscape



1. **Attacker sends spear phishing e-mail**
2. **Victim opens attachment**
    - Custom malware is installed
3. **Custom malware communicates to control web site**
    - Pulls down additional malware
4. **Attacker establishes multiple backdoors**
5. **Attacker accesses system**
    - Dumps account names and passwords from domain controller
6. **Attacker cracks passwords**
    - Has legitimate user accounts to continue attack undetected
7. **Attacker reconnaissance**
    - Identifies and gathers data
8. **Data collected on staging server**
9. **Data ex-filtrated**
10. **Attacker covers tracts**
    - Deletes files
    - Can return any time

Advanced persistent threats (APT) *usually maintain remote access to target environments for 6-18 months before being detected (i.e. they are persistent)*

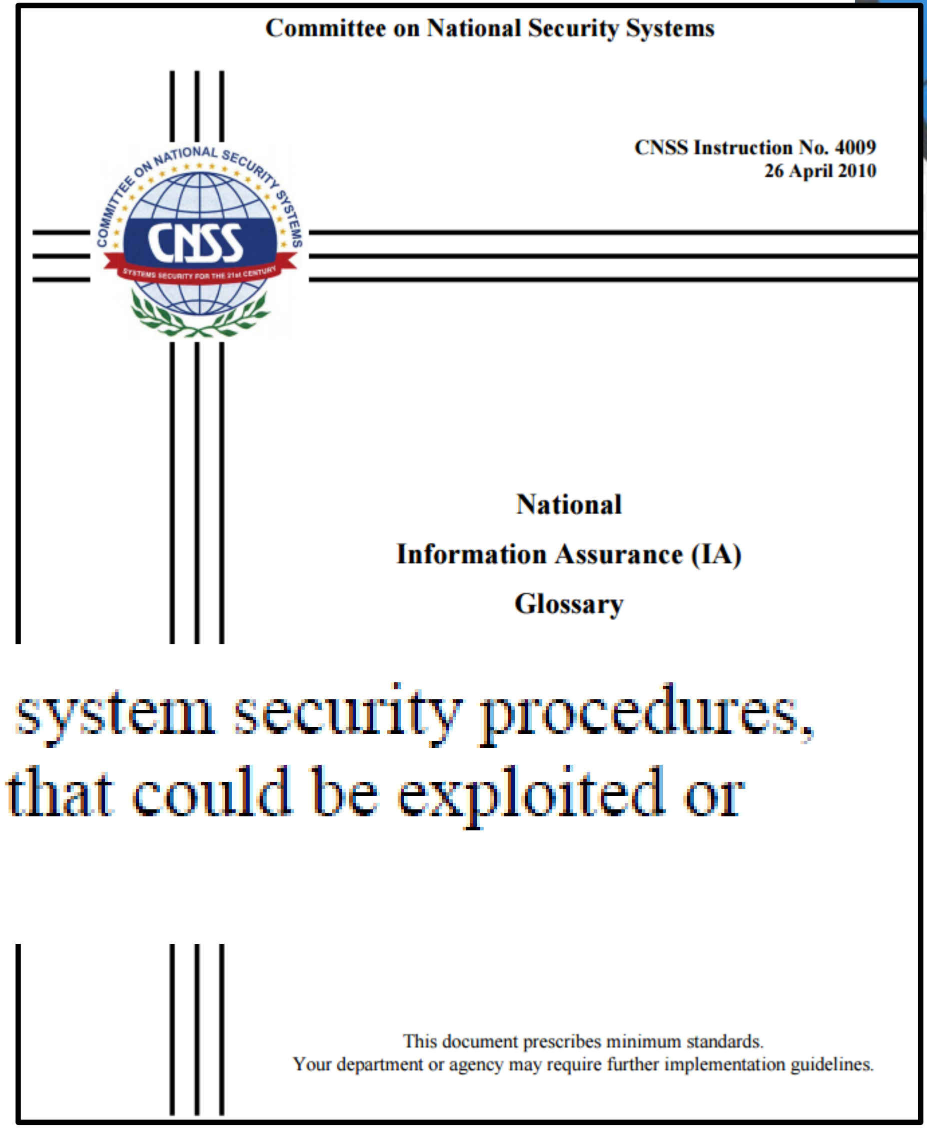
(Holcomb & Stapf, 2014)

Agenda

- ✓Terminology
- ✓Threat environment
- More terminology
- Security architecture
- Next steps…

What is a Vulnerability?

Any unaddressed susceptibility to a physical, technical or administrative information security threat



Committee on National Security Systems

CNSS Instruction No. 4009
26 April 2010

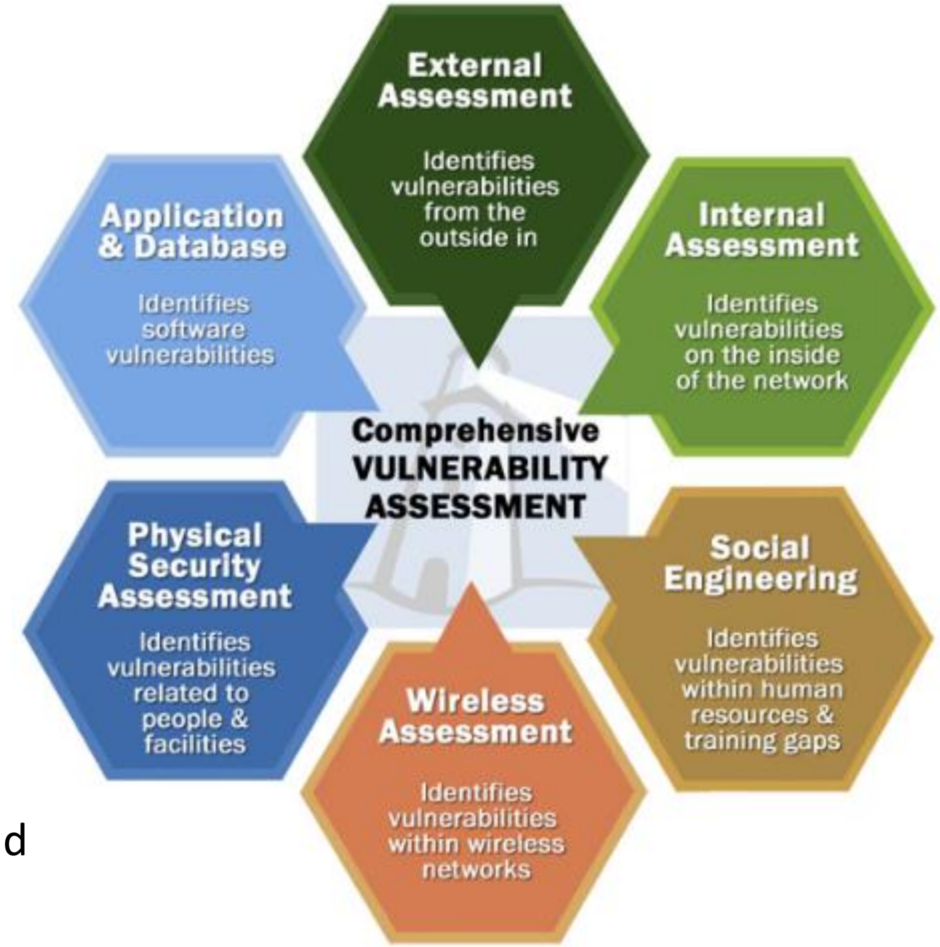
National
Information Assurance (IA)
Glossary

This document prescribes minimum standards.
Your department or agency may require further implementation guidelines.

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

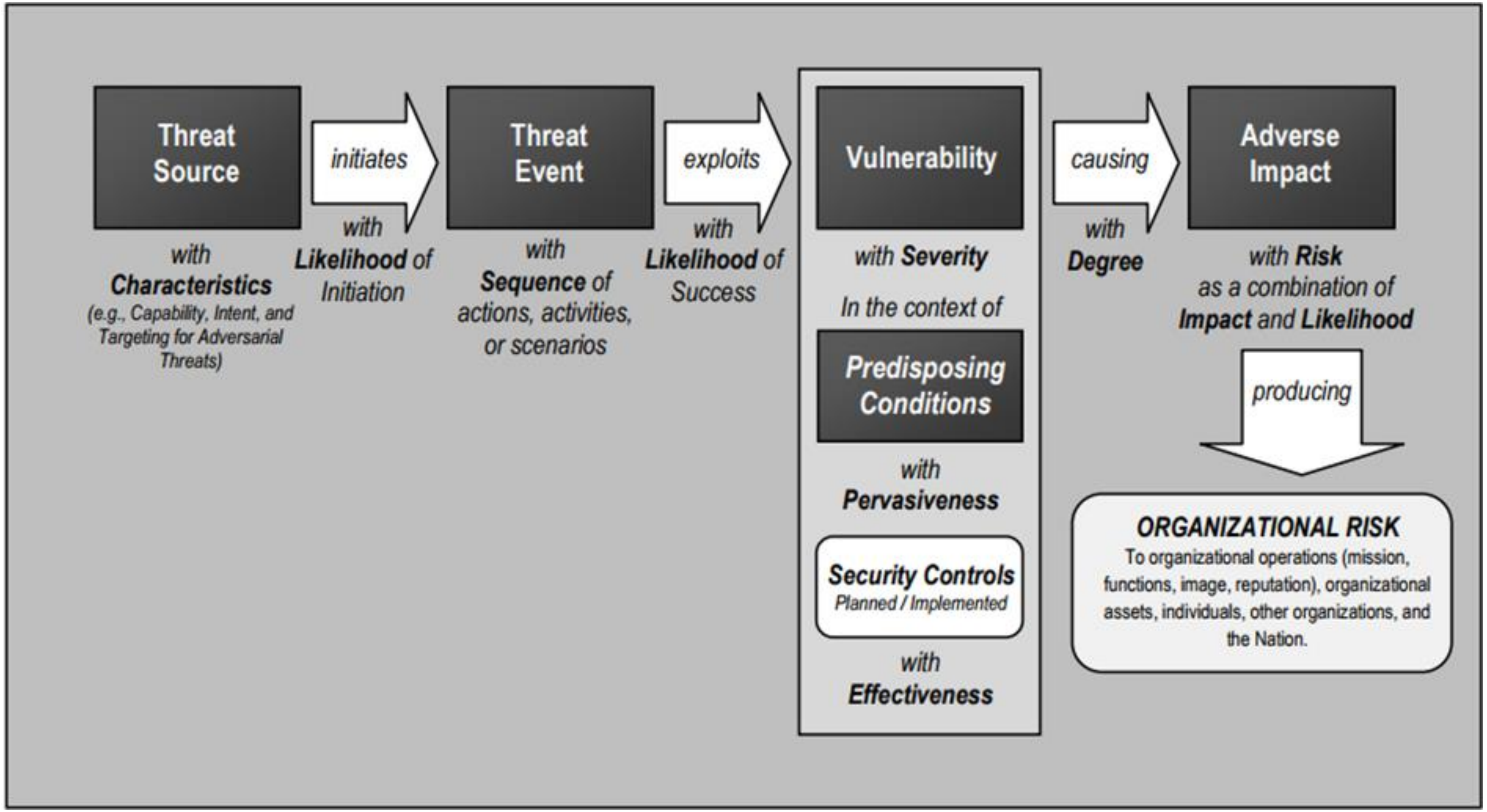
Vulnerabilities can be classified by asset class

- Physical examples
    - Buildings in environmental hazard zones (e.g. low floor in flood zone)
    - Unlocked and unprotected doors to data center
    - Unreliable power sources
- Technical examples
    - Hardware – susceptibility to humidity, dust, soiling, unprotected storage
    - Software – insufficient testing, lack of audit trail, poor or missing user authentication and access control
    - Data – unencrypted transfer or storage, lack of backup
    - Network – Unprotected communication lines, insecure architecture
- Organizational examples
    - Inadequate screening and recruiting process, lack of security awareness and training
    - Lack of regular audits
    - Lack of security and IT related business continuity plans


External Assessment
Identifies vulnerabilities from the outside in
Application & Database
Identifies software vulnerabilities
Internal Assessment
Identifies vulnerabilities on the inside of the network
Comprehensive VULNERABILITY ASSESSMENT
Physical Security Assessment
Identifies vulnerabilities related to people & facilities
Social Engineering
Identifies vulnerabilities within human resources & training gaps
Wireless Assessment
Identifies vulnerabilities within wireless networks

http://www.infosightinc.com/collaterals/CVA-PT_March2016.pdf

Security architects think about the interactions among threats, vulnerabilities, impacts and risks


Threat Source
initiates
with Likelihood of Initiation
with Characteristics (e.g., Capability, Intent, and Targeting for Adversarial Threats)
Threat Event
exploits
with Likelihood of Success
with Sequence of actions, activities, or scenarios
Vulnerability
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls Planned / Implemented
with Effectiveness
causing
with Degree
Adverse Impact
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

From NIST 800-30r1 **Guide for Conducting Risk Assessment p. 12**

What is a Risk?

A measure of threat

Potential loss resulting from unauthorized:

- *Access, use, disclosure*
- *Modification*
- *Disruption or destruction*

…of an enterprises' information

Can be expresses in ***quantitative*** *and* ***qualitative*** *terms*

Steps in a risk assessment methodology

1. What are the business assets ?
2. What possible threats put the business assets at risk ?
3. Which vulnerabilities and weaknesses may allow a threat to exploit the assets ?
4. For each threat, if it materialized, what would be the business impact on the assets ?

Assessing risk – quantitative method

1. **Estimate potential losses (SLE)**—This step involves determining the single loss expectancy (SLE). SLE is calculated as follows:

   - **Single loss expectancy (SLE) = Asset value X Exposure factor**

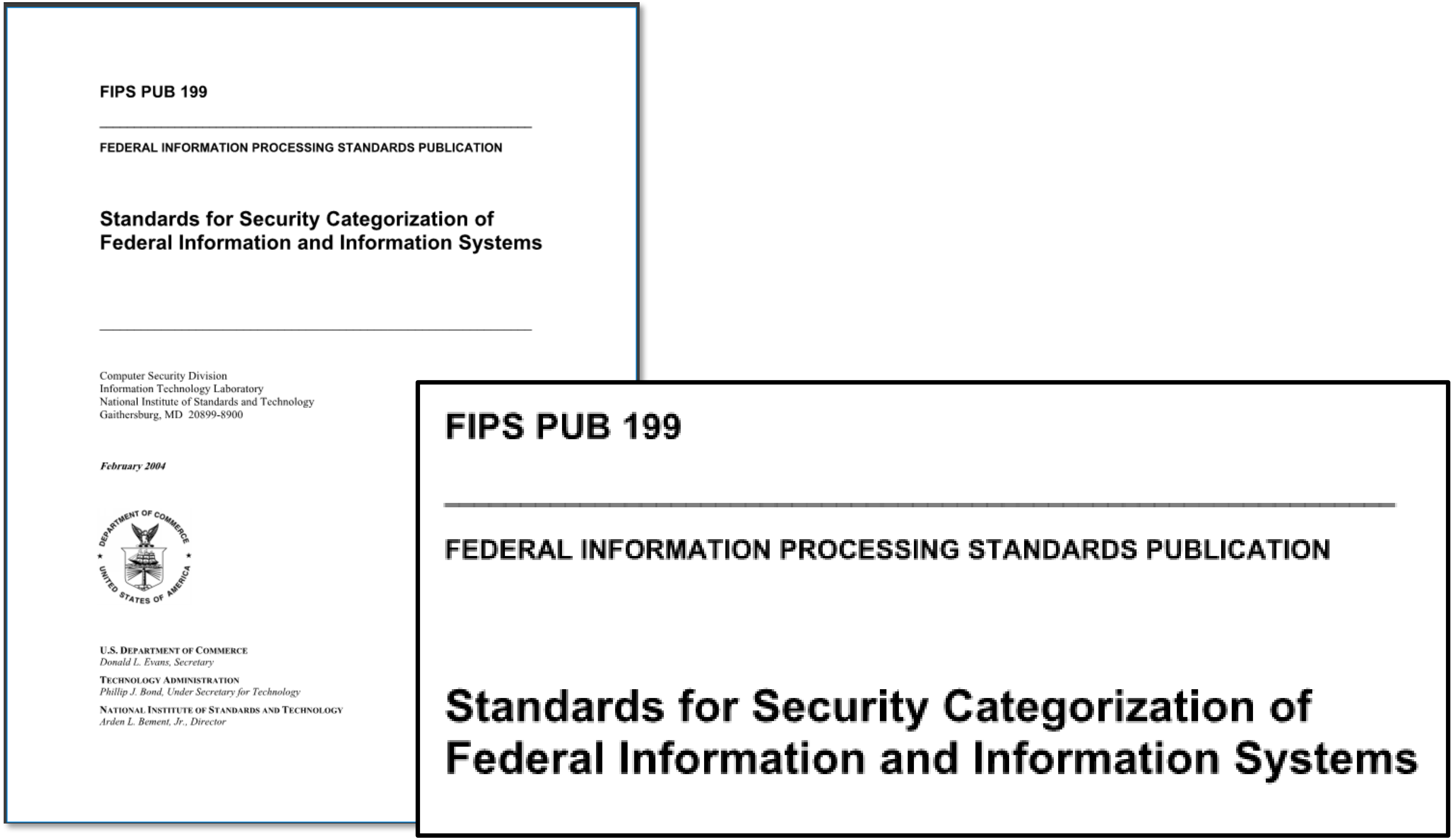
   Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

2. **Conduct a threat analysis (ARO)**—The purpose of a threat analysis is to determine the likelihood of an unwanted event. The goal is to estimate the **annual rate of occurrence (ARO**). Simply stated, **how many times is this expected to happen in one year?**

3. **Determine annual loss expectancy (ALE)**—This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:

   - **Annualized loss expectancy (ALE) = Single loss expectancy (SLE) X Annualized rate of occurrence (ARO)**

Assessing risk – qualitative method



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

What is NIST?

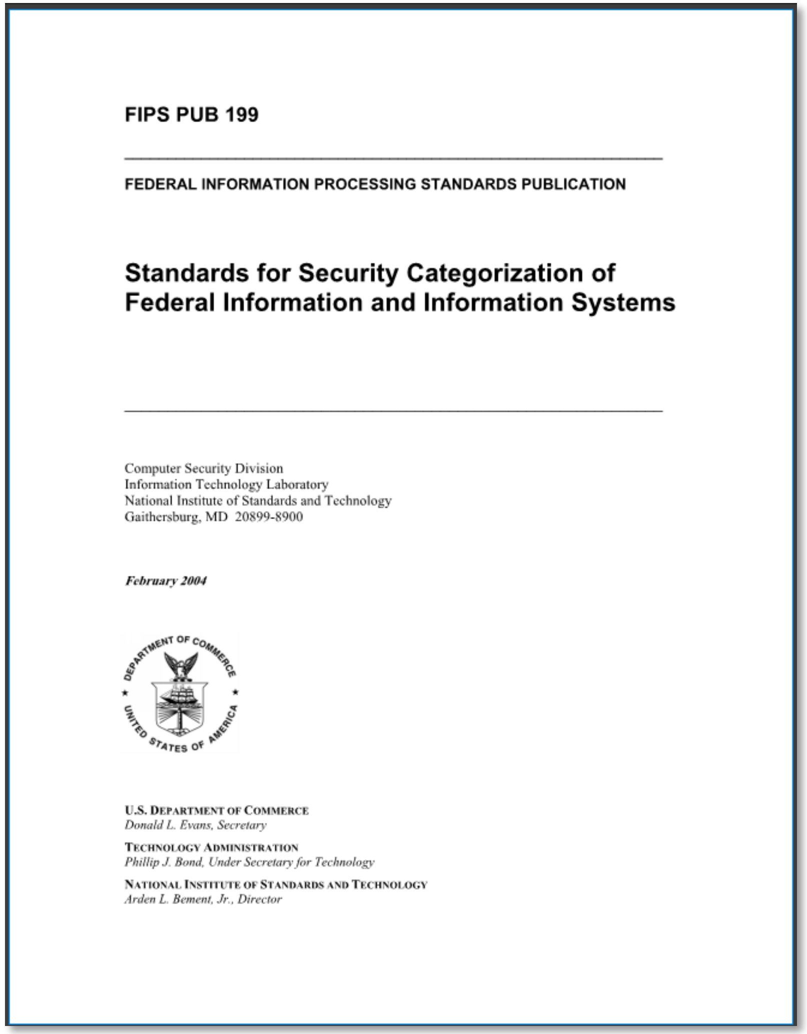
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- Non-regulatory agency of the United States Department of Commerce
- Measurement standards laboratory

Mission: *Promote innovation and industrial competitiveness*

NIST is responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets (excluding national security systems)

FIPS 199: Risk assessment based on security objectives and impact ratings



FIPS PUB 199

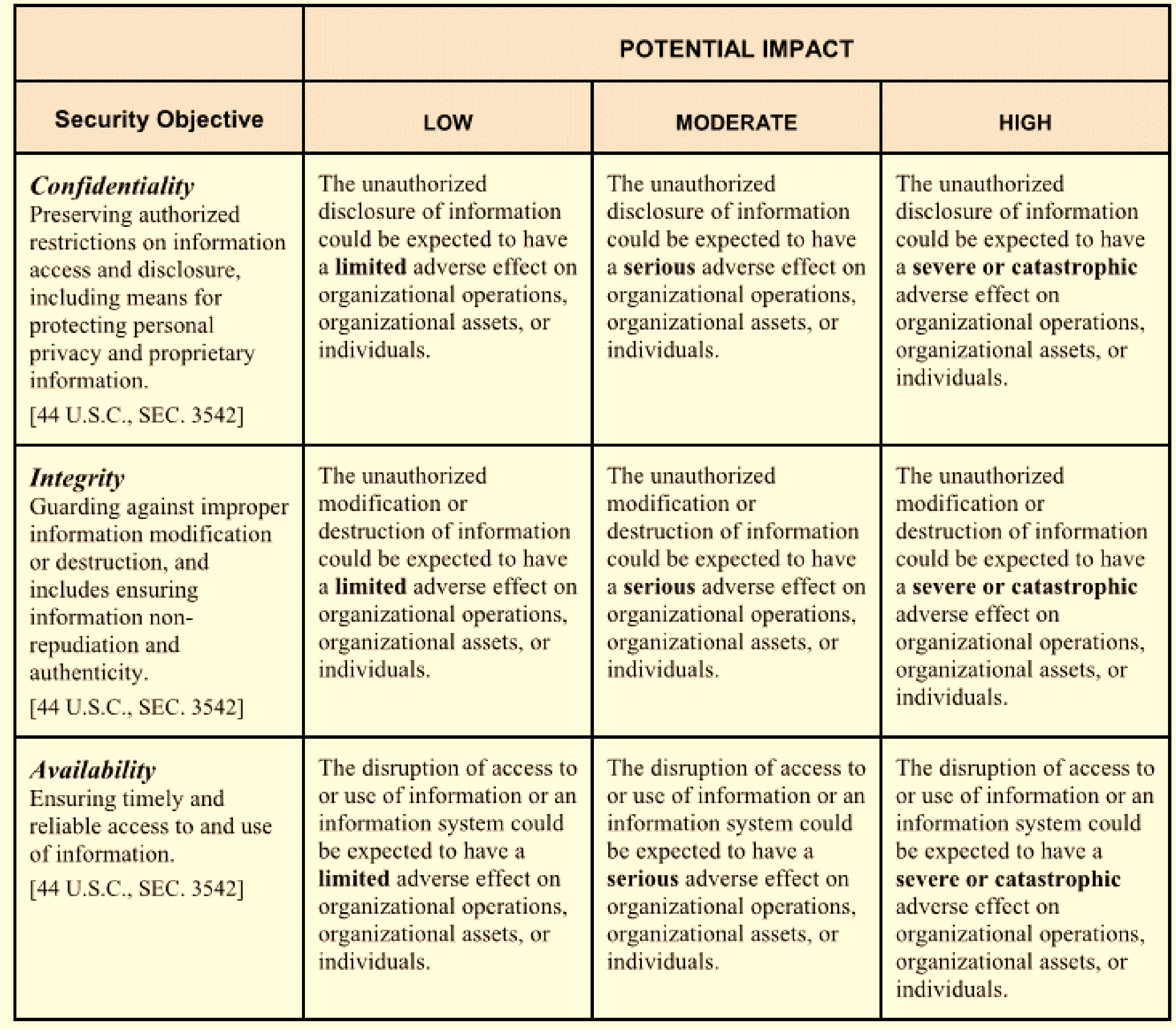
FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Agenda

- ✓Terminology
- ✓Threat environment
- ✓More terminology
- Security architecture
- Next steps…

Security Architecture

A comprehensive and rigorous method to plan, design and describe current and desired future structure and behavior of an organization's:

- Business sub-units
- Processes and Personnel
- Information security systems

…so they align with the organization's core goals and strategic direction

Wikipedia: https://en.wikipedia.org/wiki/Enterprise_information_security_architecture

Security Architecture

"…the art and science of designing and supervising the construction of business systems, usually business information systems, which are:

- Free from danger, damage, etc.
- Free from fear, care, etc.
- In safe custody
- Not likely to fail
- Able to be relied upon
- Safe from attack"

Sherwood et al. (2005) Enterprise Security Architecture: A Business-Driven Approach

Defenders must be perfect

“One mistake by the defender essentially renders the whole defense worthless”

…every computer and software program must be patched, every configuration appropriately secure, and every end-user perfectly trained. Or at least that is the goal.

The defender knows that applied defenses may not always work or be applied as instructed, so they create “defense-in-depth” layers.”

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

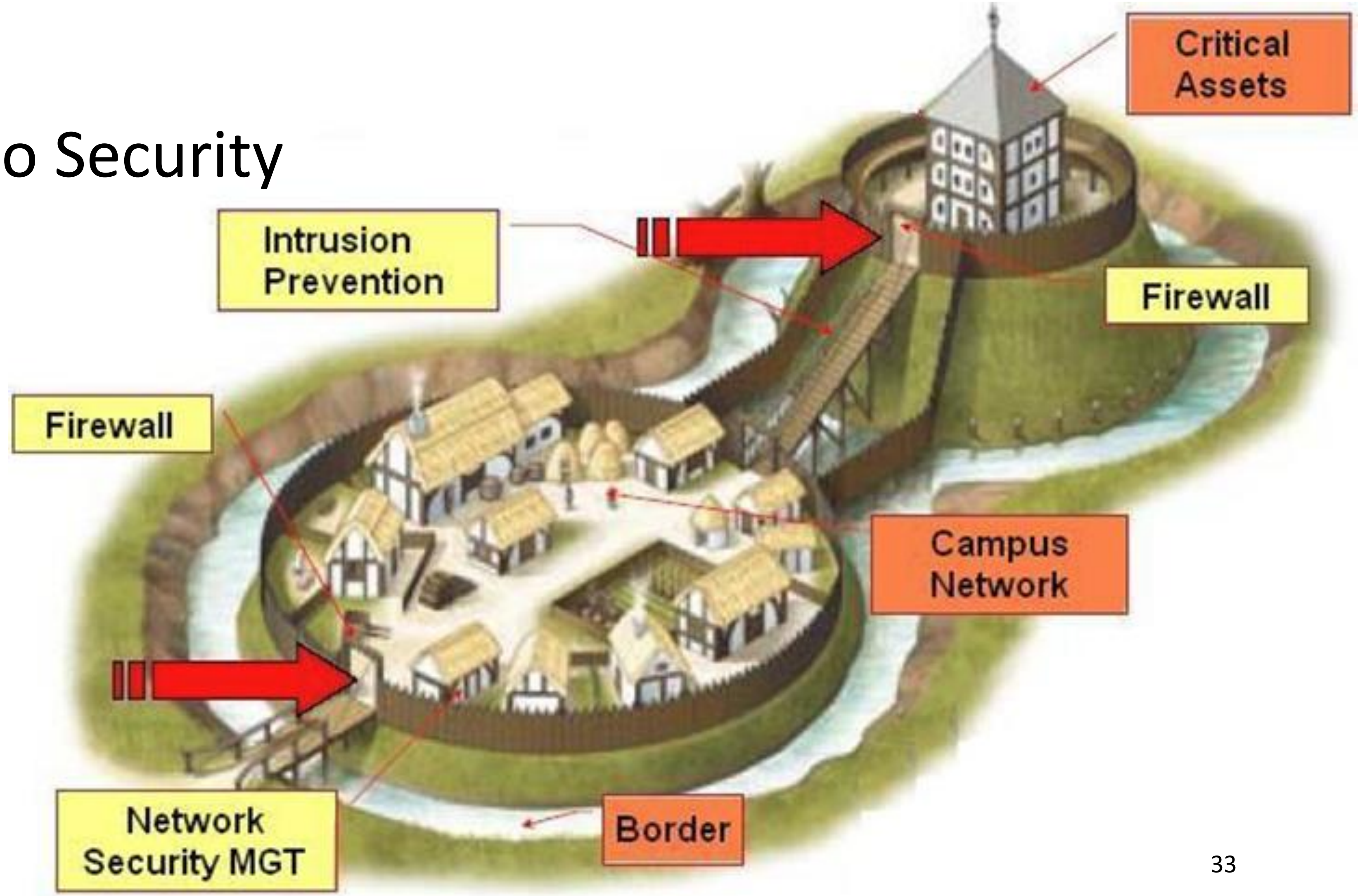
Security Architecture

Thinking about security architecture enables understanding enterprise information systems the way attackers do – as large diverse attack surfaces

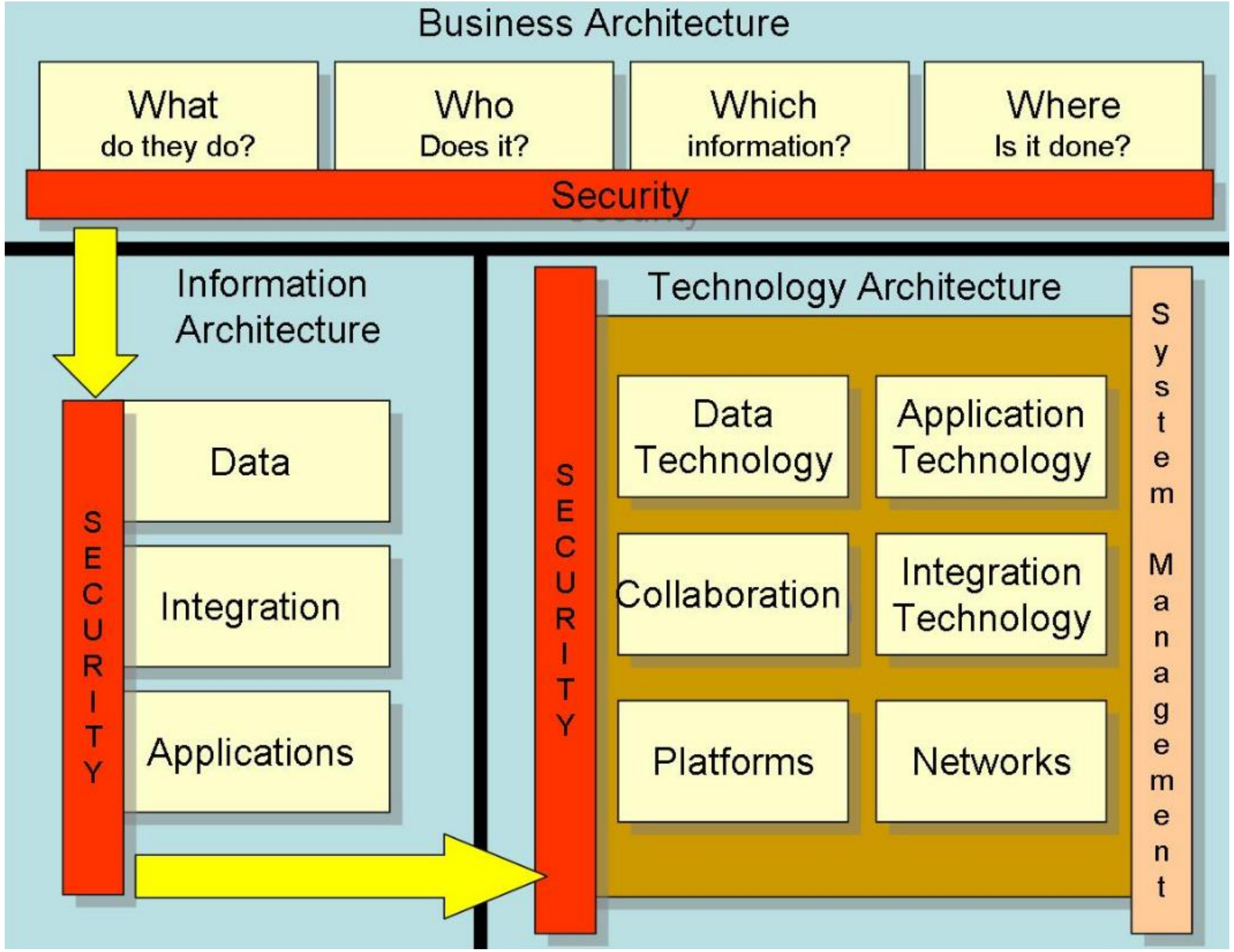
https://graquantum.com/blog/cyber-basics-cyber-attack-surface/

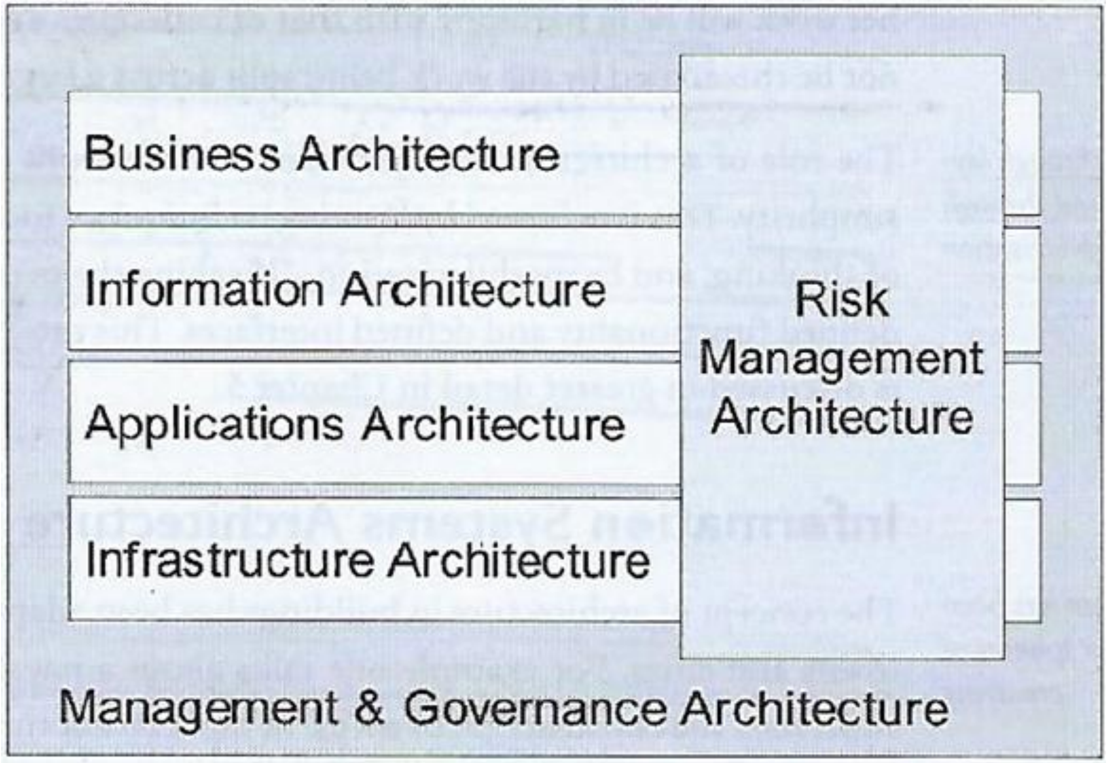
Defense in Depth

- Also known as:
  - Layered Security
  - Castle Approach to Security



Enterprise Information and Security Architecture

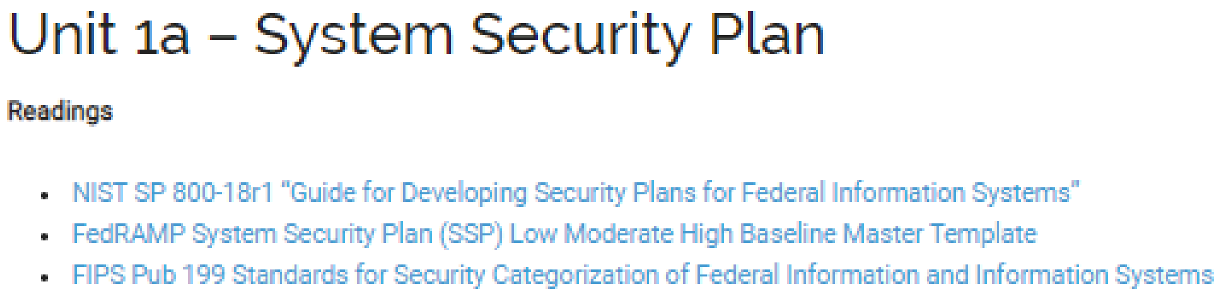



Business Architecture
Information Architecture
Applications Architecture
Infrastructure Architecture
Risk
Management
Architecture
Management & Governance Architecture

Sherwood et al. (2005) Enterprise Security Architecture: A Business-Driven Approach

Huxham, H. (2006) “Own view of Enterprise Information Security Architecture (EIS))Framework”
Wikipedia: https://en.wikipedia.org/wiki/Enterprise_information_security_architecture, accessed 2017-1-19

Next steps…



Unit 1a – System Security Plan

Readings

- NIST SP 800-18r1 "Guide for Developing Security Plans for Federal Information Systems"
- FedRAMP System Security Plan (SSP) Low Moderate High Baseline Master Template
- FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems

Agenda

- ✓Terminology
- ✓Threat environment
- ✓Hacker mindset
- ✓More terminology
- ✓Security architecture
- ✓Next steps…