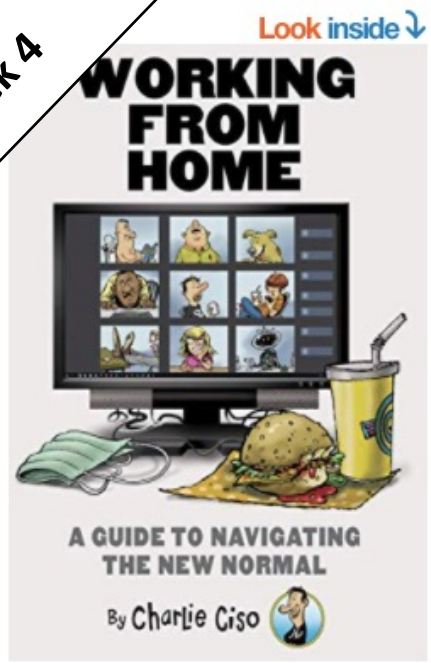
An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso
eamoroso@tag-cyber.com

Week 4



Working from Home: A Guide to Navigating the New Normal

Kindle Edition

by Edward Amoroso (Author), Rich Powell (Author) | Format: Kindle Edition

★★★★★ 16 ratings

› See all formats and editions

Kindle
$4.99

Read with Our Free App

If you are in need of some Pandemic entertainment and world-class comic relief, then "Working from Home: A Guide to Navigating the New Normal" is for you! This step-by-step guide, written by a fictitious social media sensation (and sometimes cybersecurity expert) named Charlie Ciso, will teach you to:

•Build a fake Zoom backdrop that will get you promoted to senior VP in ten days or less

‹ Read more

Kindle Price: $4.99

Read Now

You already own this item. Read anytime on your Kindle apps and devices.

Buy for others

Give as a gift or purchase for a team or group. Learn more

Quantity: 1 Buy for others

Add to List

Enter a promotion code or Gift Card

Share <Embed>

READ ON ANY DEVICE
›Get free Kindle app

Follow the Author

Edward G. Amoroso

+ Fol

Week 4

Required Text – $9.99 Download from Amazon.com

$25.00 Printed Paperback Book from Amazon.com

From CIA to APT: An Introduction to Cyber Security

Edward G. Amoroso & Matthew E. Amoroso

Week 4

Required Week Four Readings

1. "A Man-in-the-Middle Attack on UMTS," U. Meyer and S. Wetzel https://www.cs.stevens.edu/~swetzel/publications/mim.pdf

2. **Chapters 12 through 16: *From CIA to APT: An Introduction to Cyber Security*, E. Amoroso & M. Amoroso**

Twitter: @hashtag_cyber
LinkedIn: Edward Amoroso

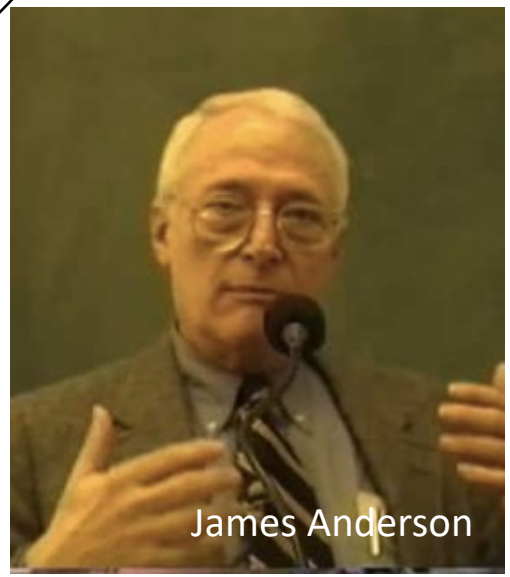
Week 4

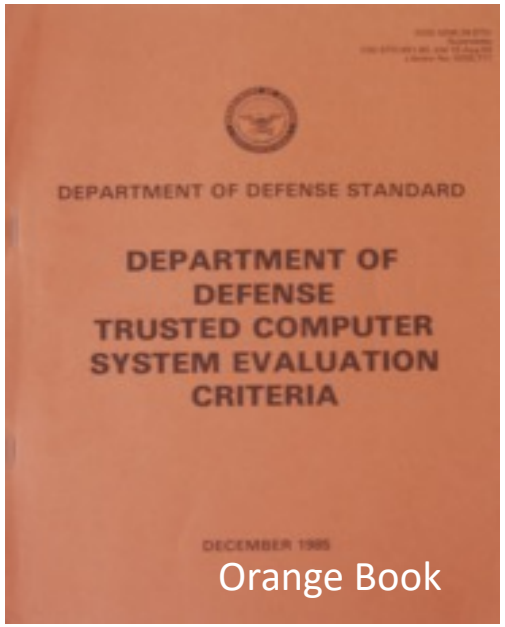
<u>Required Additional Reading</u>: https://www.tag-cyber.com/advisory/quarterly

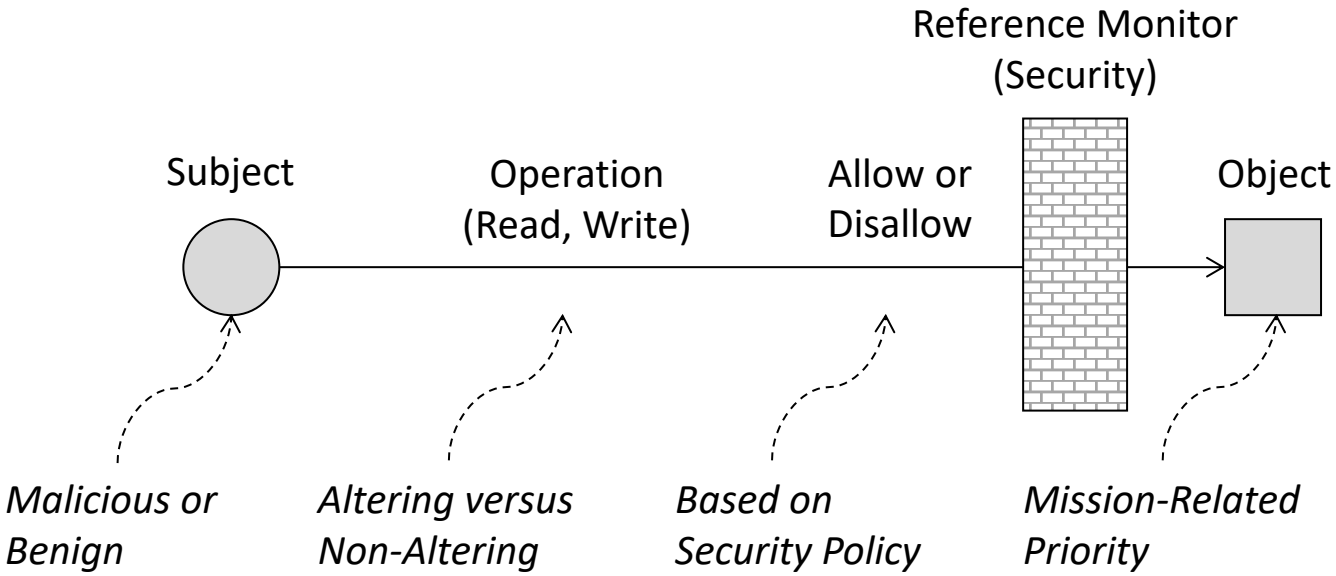
Week 4: Threat-Vulnerability Analysis

What are the Foundational Issues in Cyber Security?

Week 4

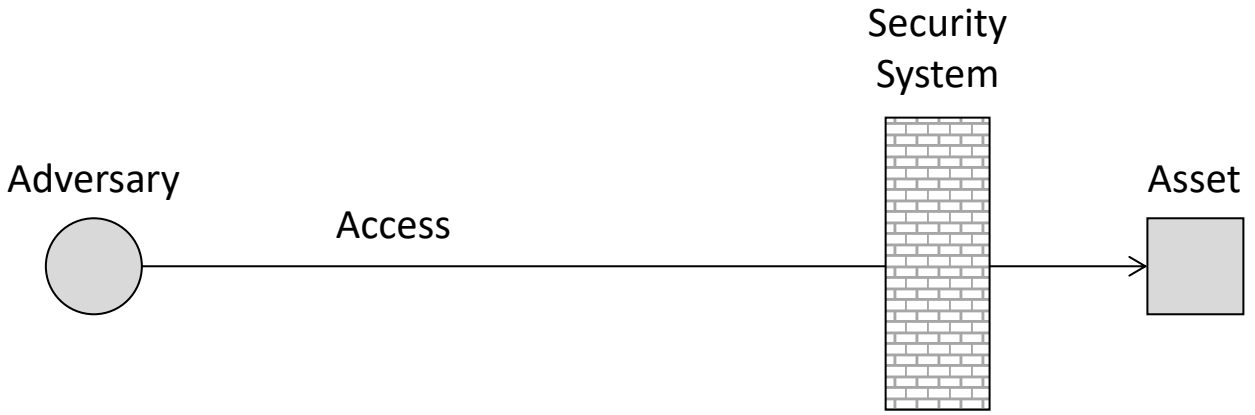






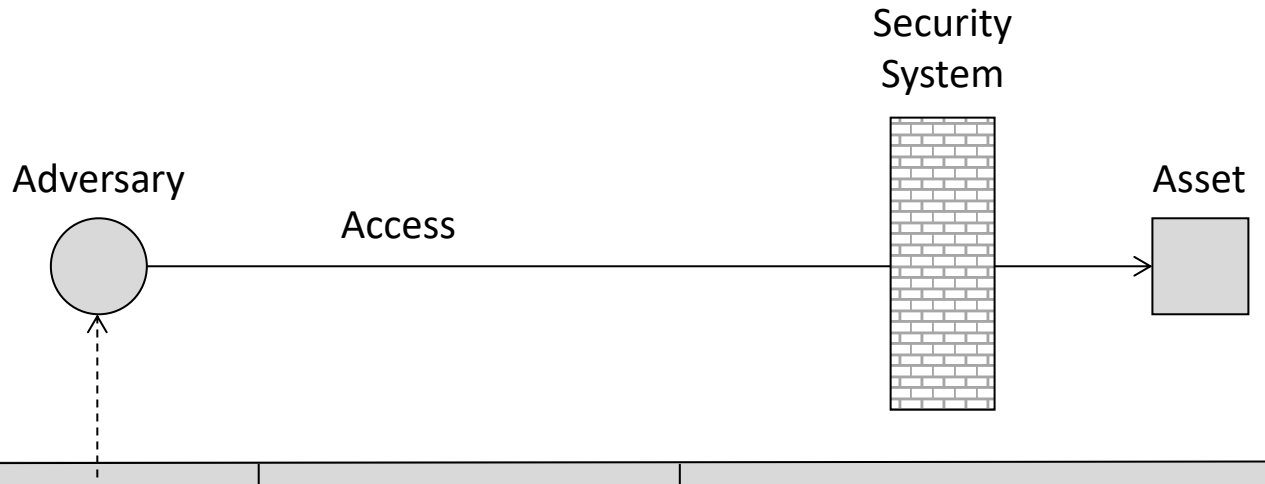
Cyber Security: Subject-Object Reference Model

Week 4



Cyber Security: Basic Operational Framework

Week 4

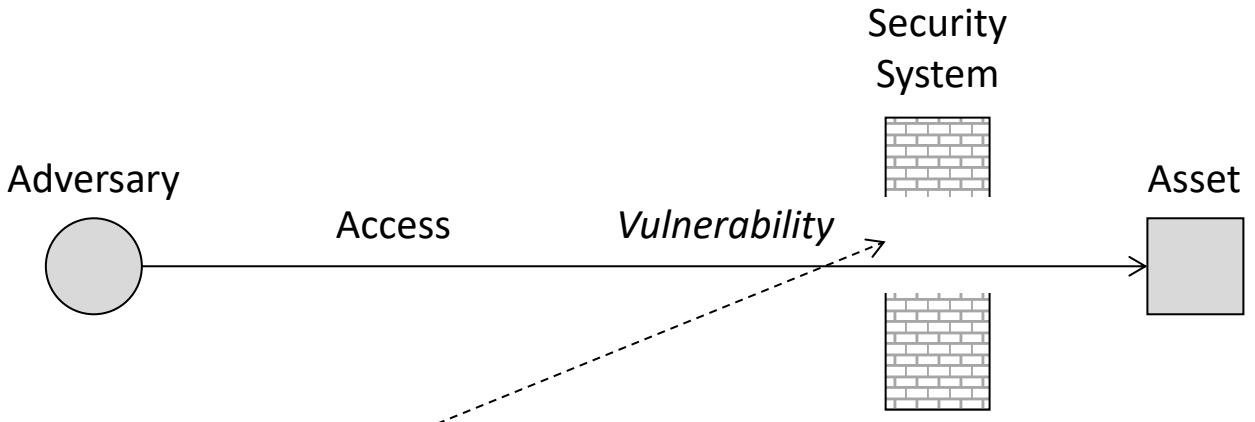


Incomplete List

Adversary Type	*Motivation*	*Defining Attributes*
Hacker	Mischief	Individually Capable, Predictable
Hacktivist	Anger	Group Capable, Unpredictable
Criminal	Greed	Well Funded, Financial Motivation
Nation-State	Dominance	World Class Capability and Support

Cyber Security: Adversary Types

Week 4

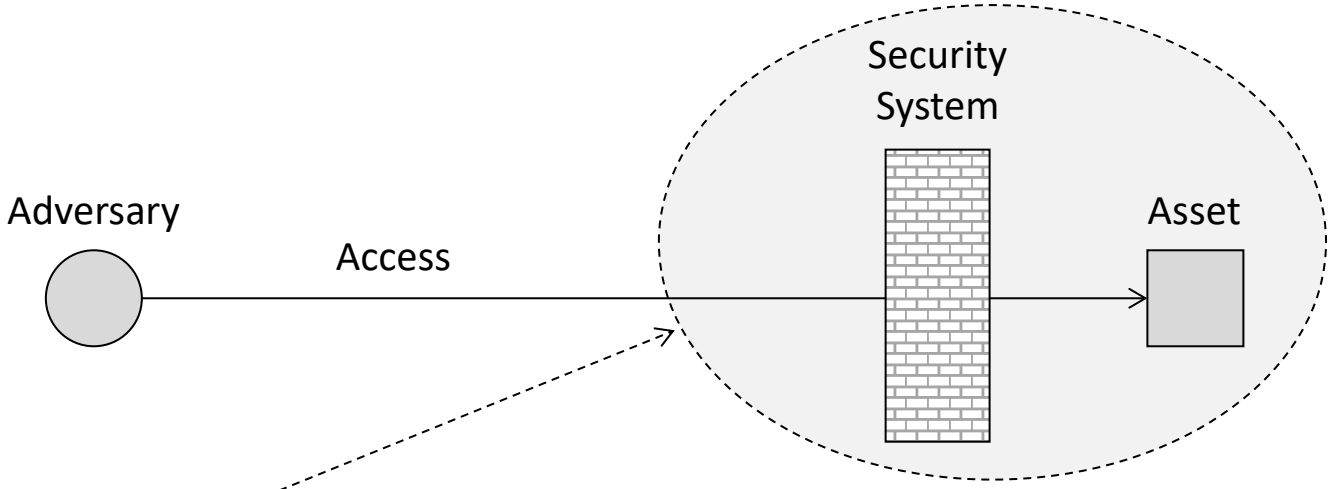


Incomplete List

Vulnerability Type	*Root Cause*	*Defining Attributes*
System Flaw	Complexity	Insufficient design, test, build, operate
Lack of Security	Budget	Attention not paid to proper protection
Human Actions	Ignorance	Lack of security awareness and training
Organizational	Irresponsibility	Inadequate staff, procedures, and process

Cyber Security: Vulnerability Types

Week 4



Threat Type	*Motivation*	*Defining Attributes*
Disclosure	Secrets	Personal and Business Information
Integrity	Degradation	Remote Operational Control/Change
Denial of Service	Disruption	Distributed Botnet Attacks Common
Theft/Fraud	Money/Goods	Ingenious and Clever Means for Theft

Complete List

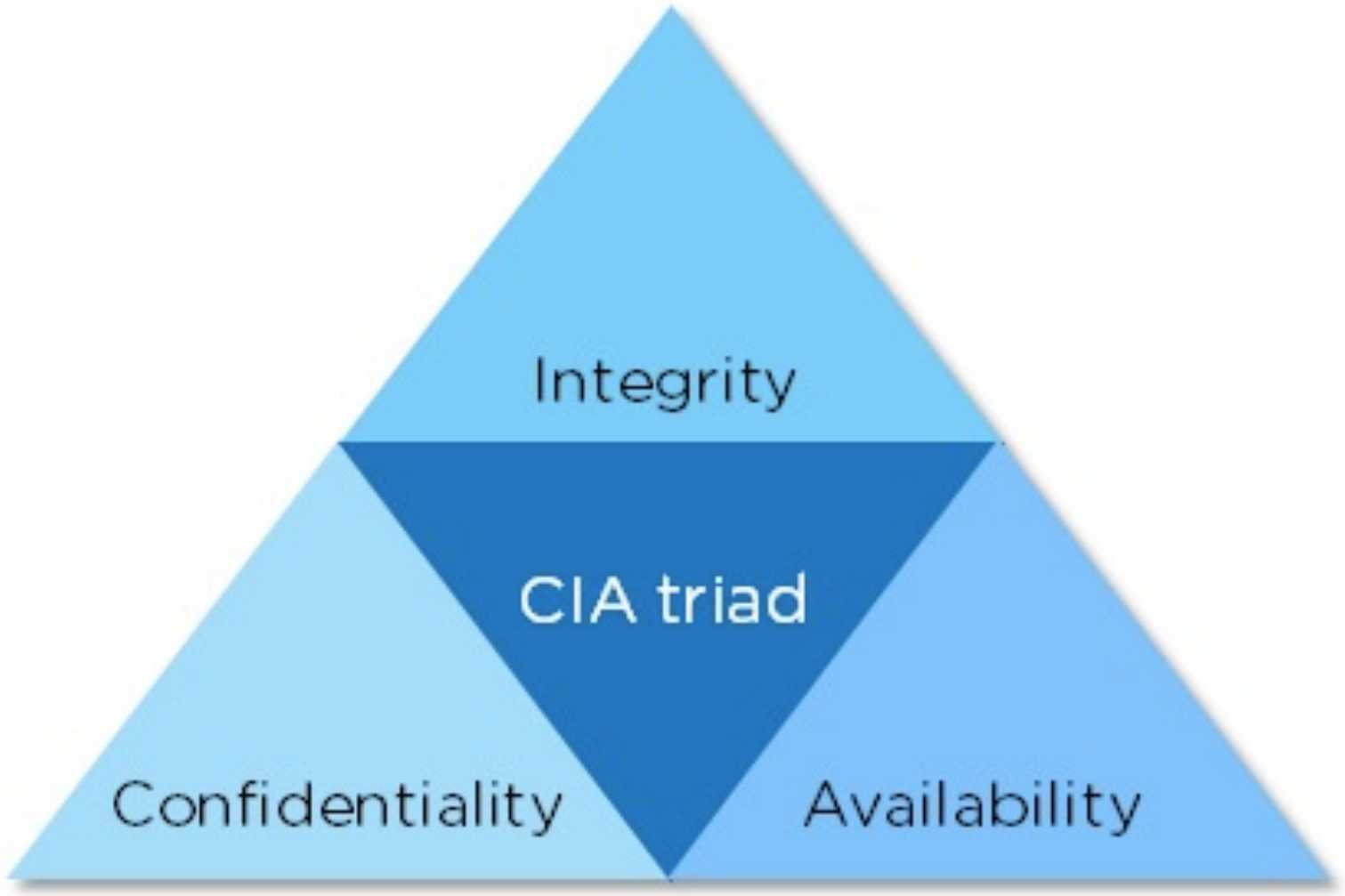
Cyber Security: Threat Types

What Cyber Security Definitions Should I Memorize?

Week 4

Def: <u>Assets</u> – Resources required for organization to meet its mission.

Week 4



Def: <u>Threats</u> – Malicious outcomes levied against assets.

Week 4

Def: <u>Confidentiality Threat</u> – Information disclosed to unauthorized parties.

Week 4

Def: <u>Privacy Threat</u> – *Personal information* disclosed to unauthorized parties.

Week 4

Def: <u>Integrity Threat</u> – Asset maliciously altered (includes destroyed).

Week 4

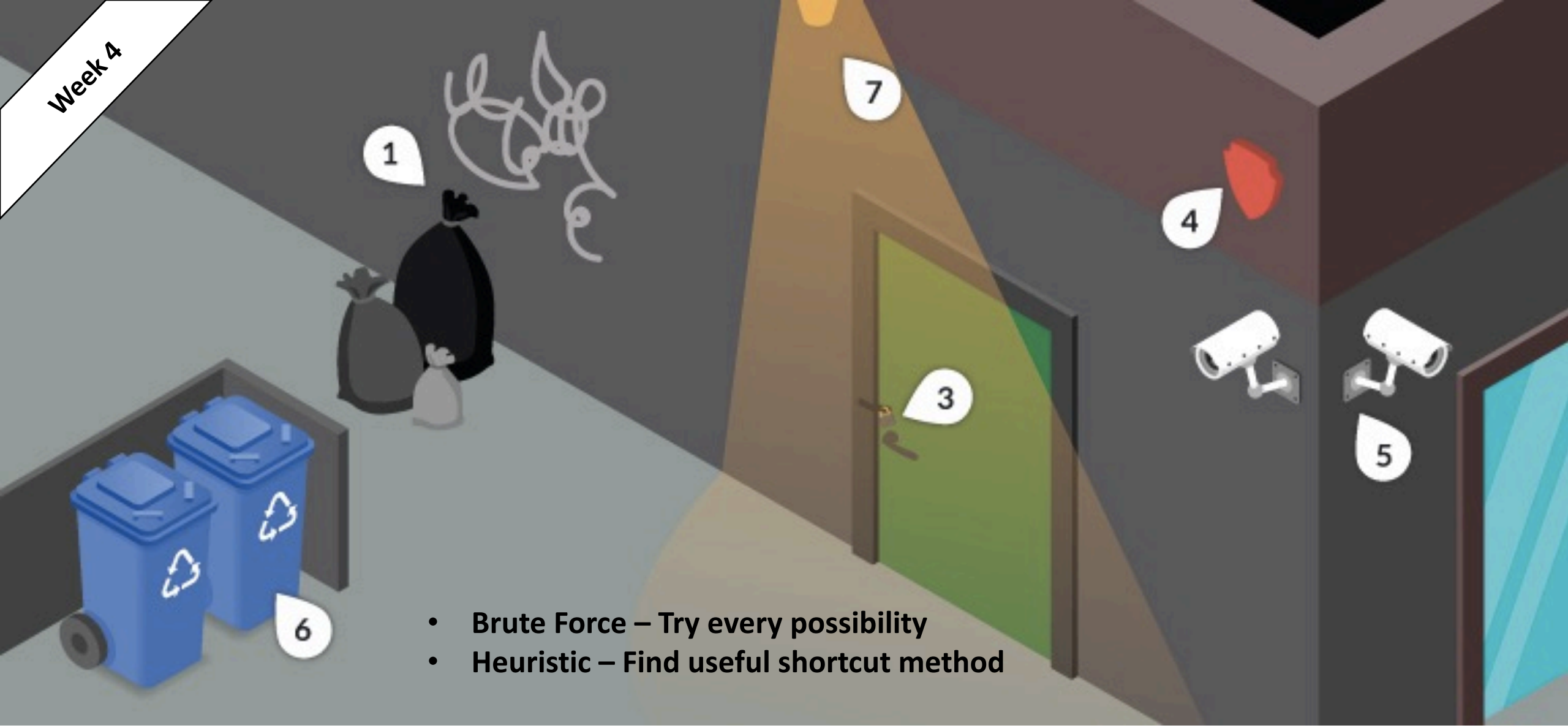
Def: <u>Availability Threat</u> – Asset maliciously blocked from authorized use.

Week 4

Def: <u>Theft/Fraud</u> – Stealing service or product without paying.

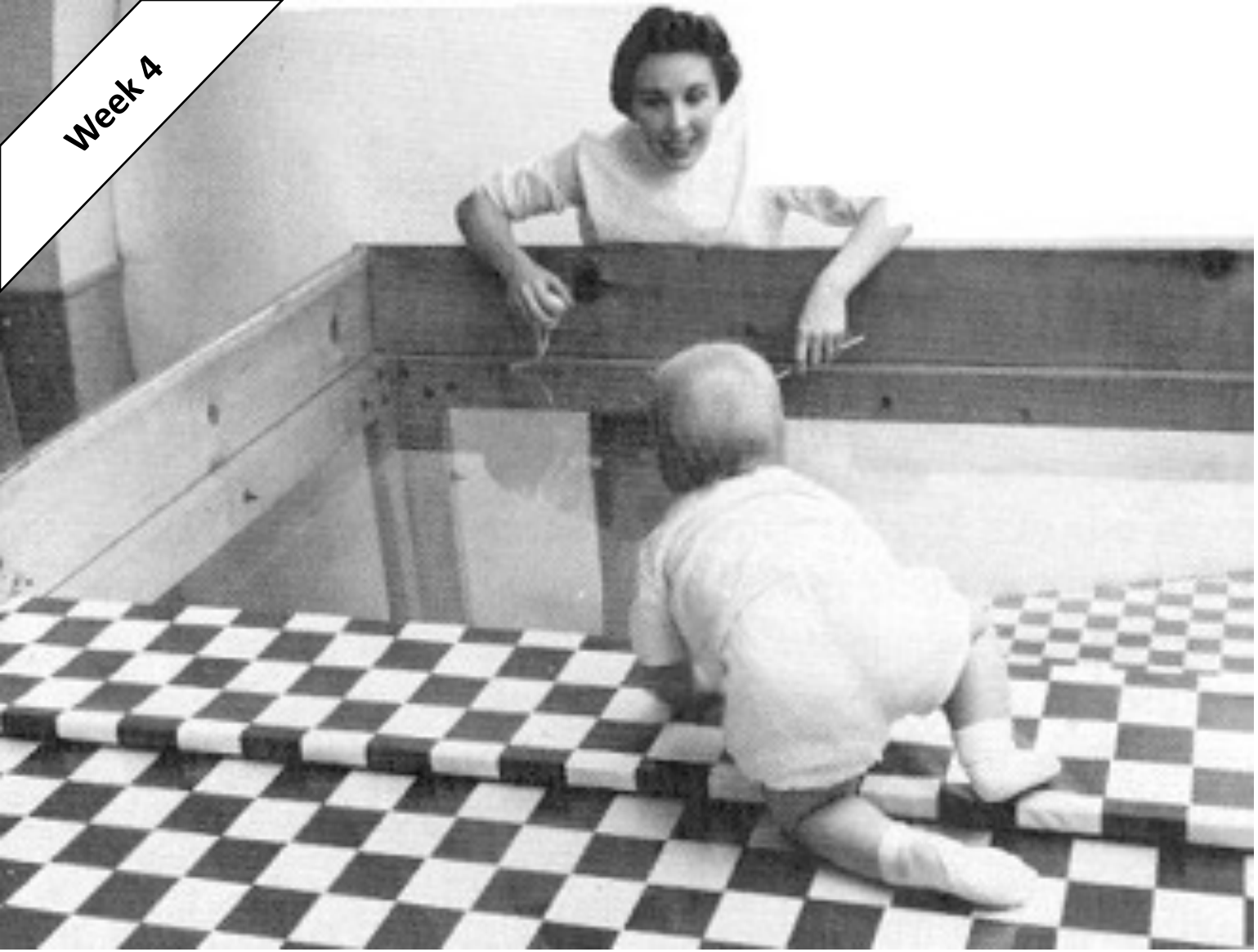
Week 4

Def: <u>Vulnerability</u> – System bug or attribute that can be maliciously exploited.



Def: <u>Attack</u> – Sequence of steps to exploit a vulnerability.

Week 4

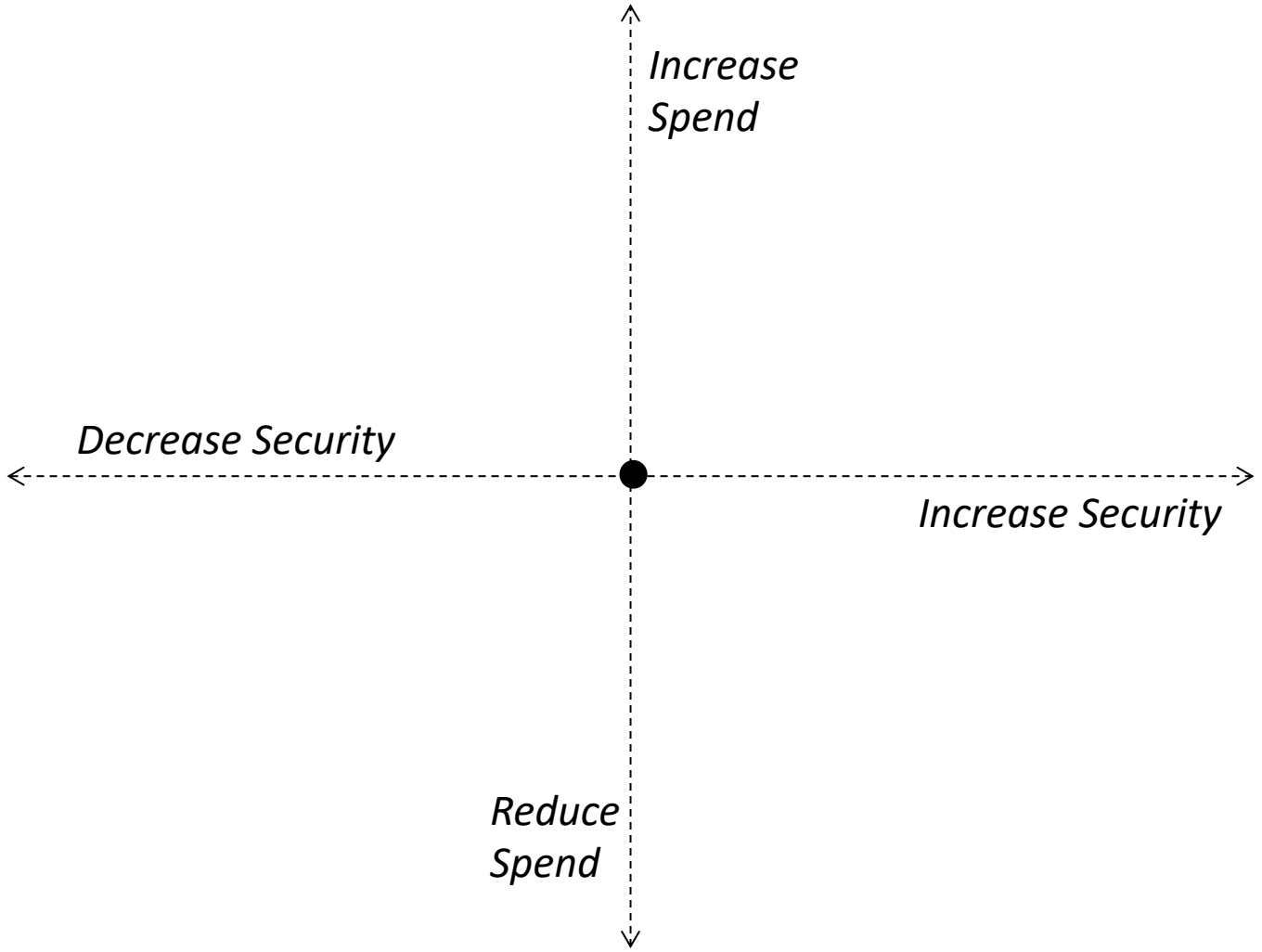


Risk (R) equals
Probability (P) of Threat
times
Consequence (C) of Threat

R = P * C

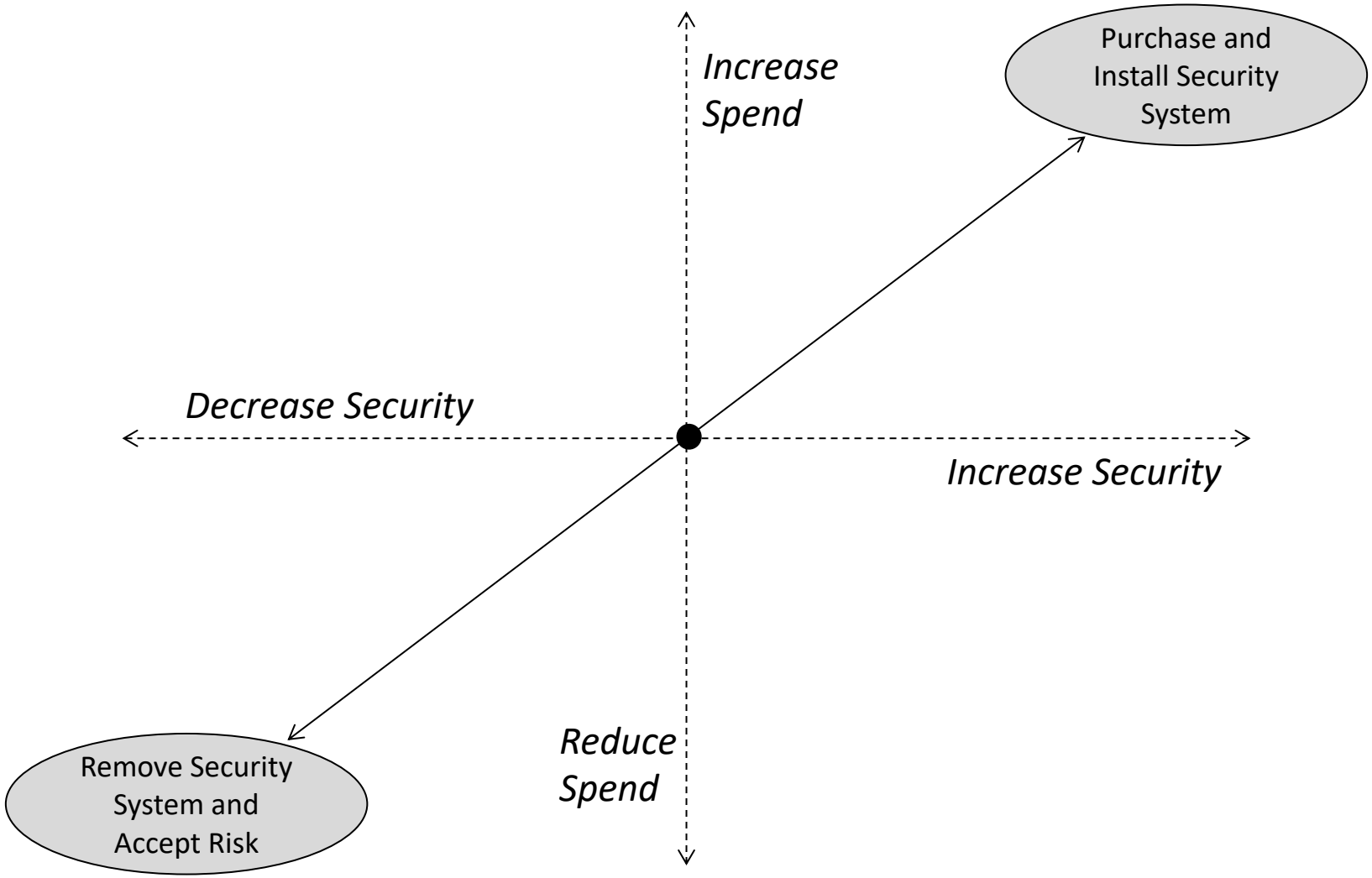
Def: <u>Risk</u> – Probability “Times” Consequence

Week 4



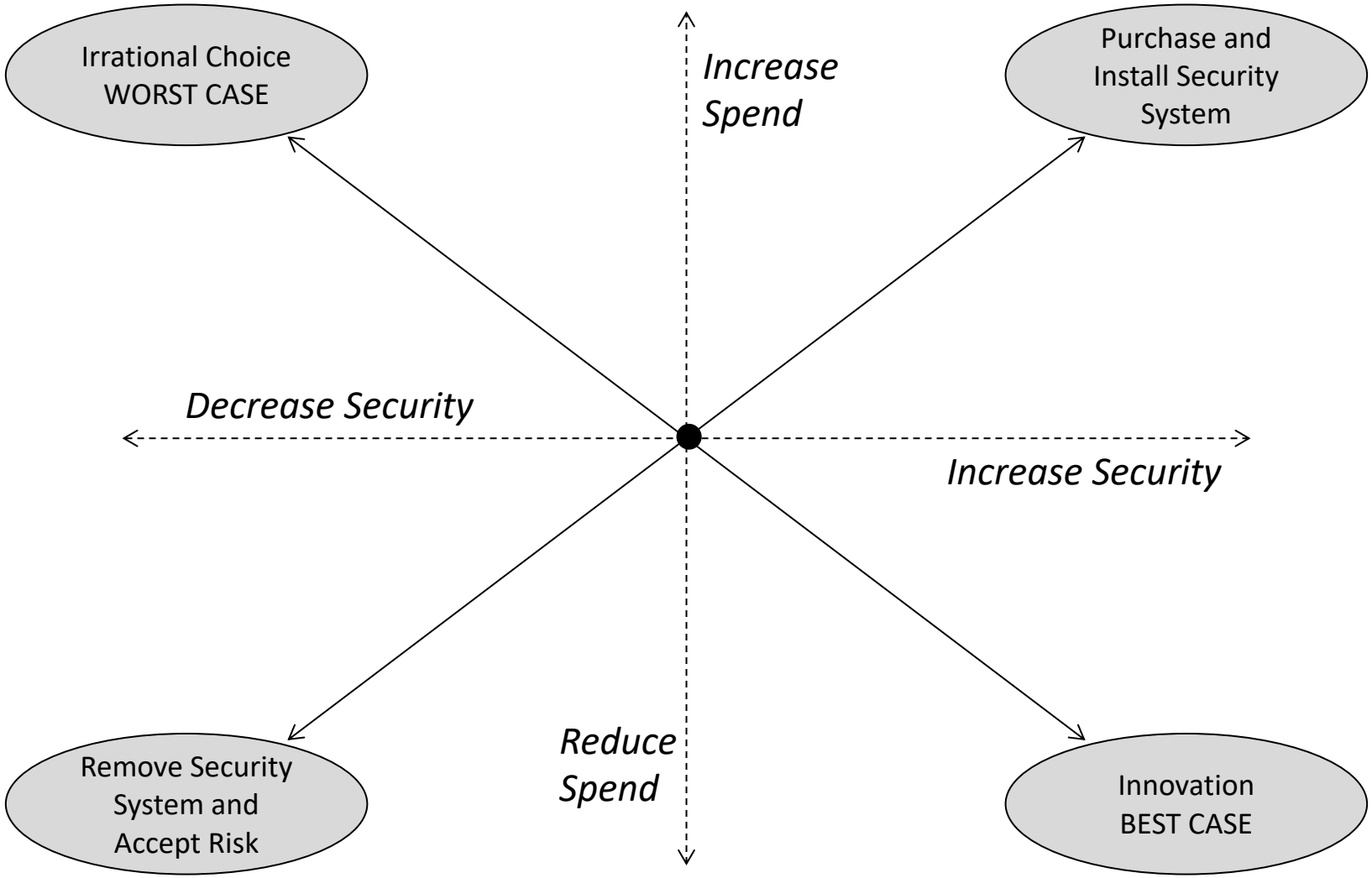
Security Risk Assessment – Decision Framework

Week 4



Security Risk Assessment – Decision Framework

Week 4



Security Risk Assessment – Decision Framework

How Are Assets Prioritized?

Week 4

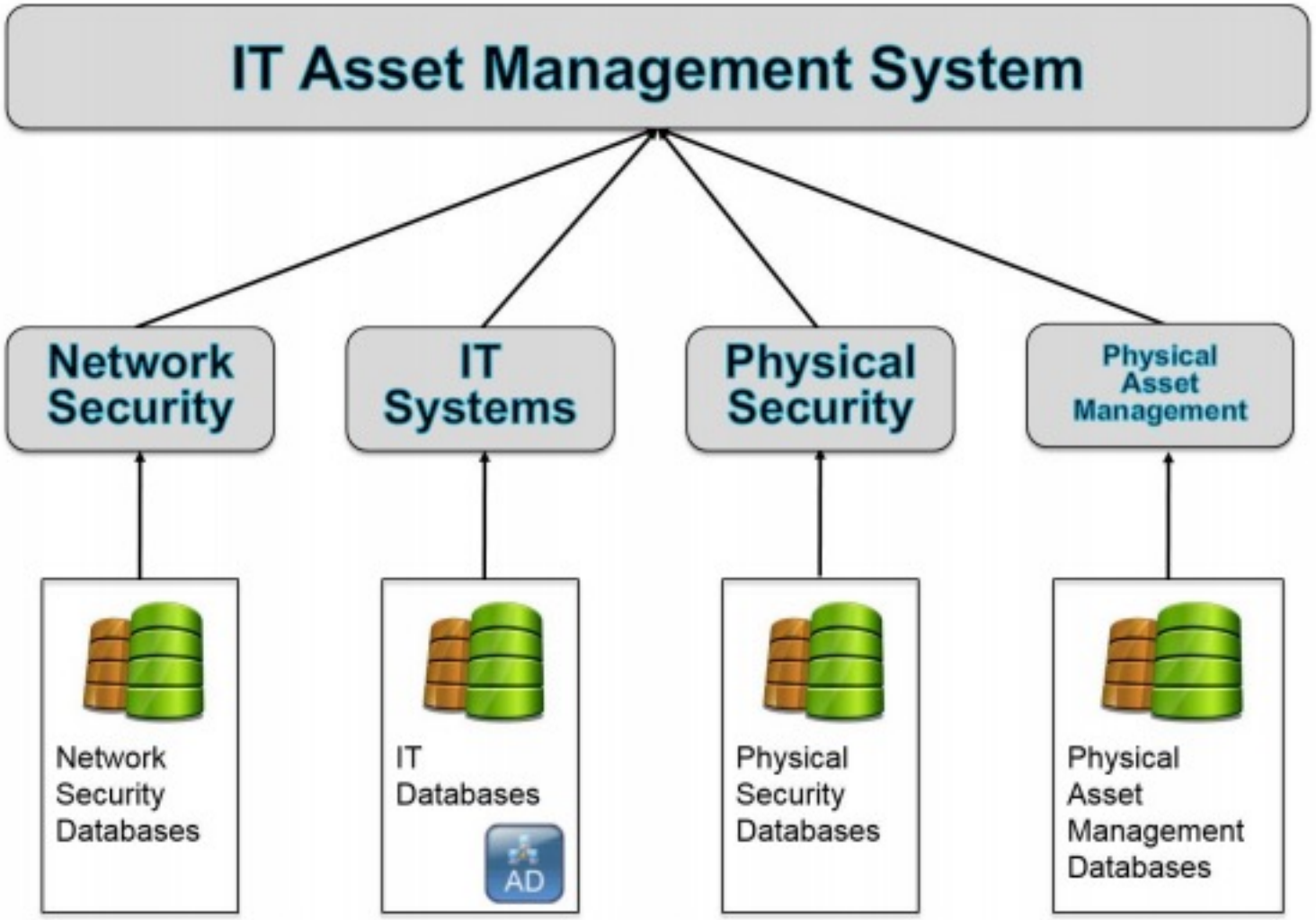
Illustrating Tiered Prioritization of Assets

Week 4

- ☑ Replaceability
- ☑ Convenience
- ☑ Sensitivity
- ☑ Emotion
- ☑ Dependence
- ☑ Liability
- ☑ Stewardship
- ☑ Finance
- ☑ Preference

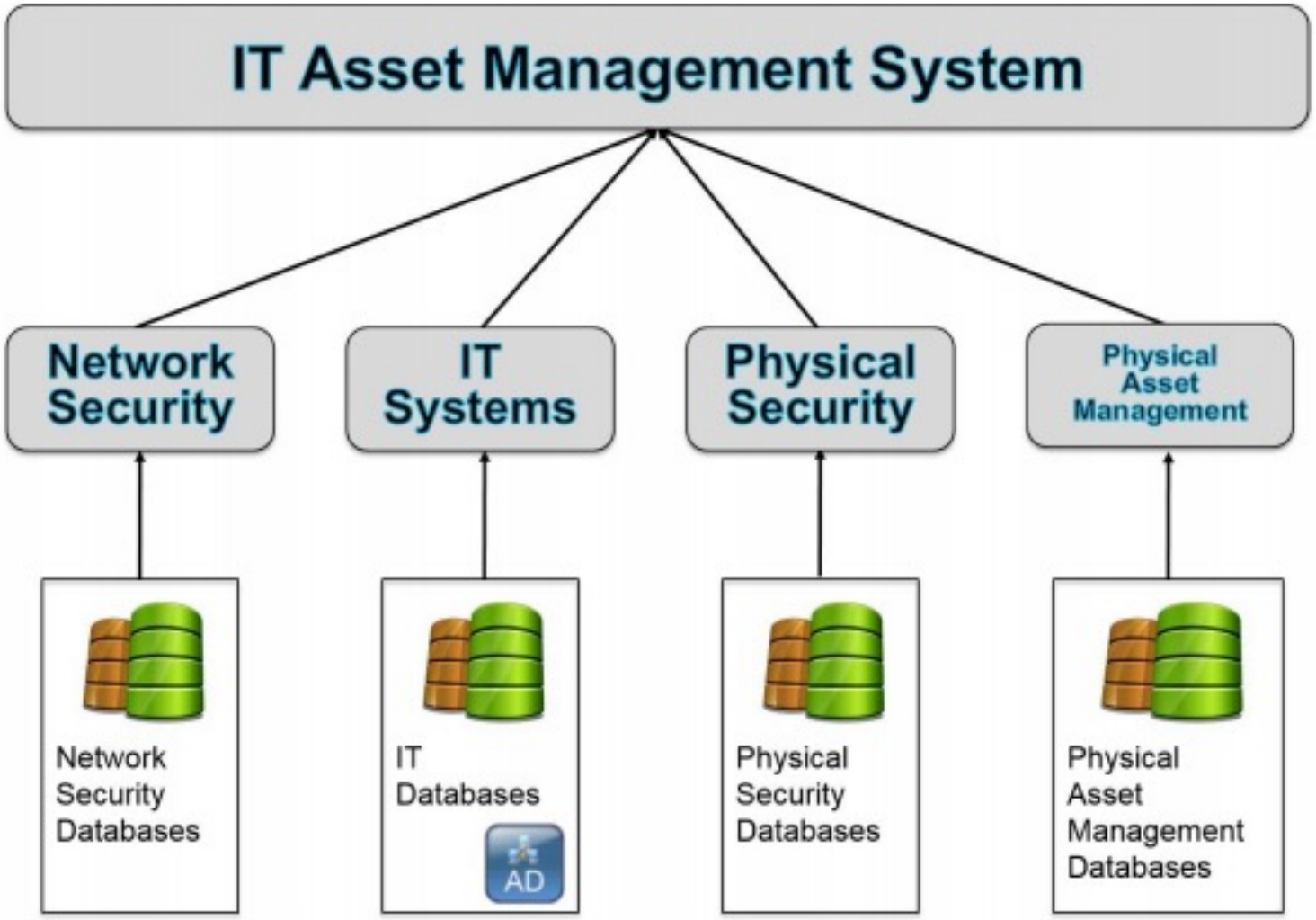
Illustrating Tiered Prioritization of Assets

Week 4



NIST IT Asset Management System Model

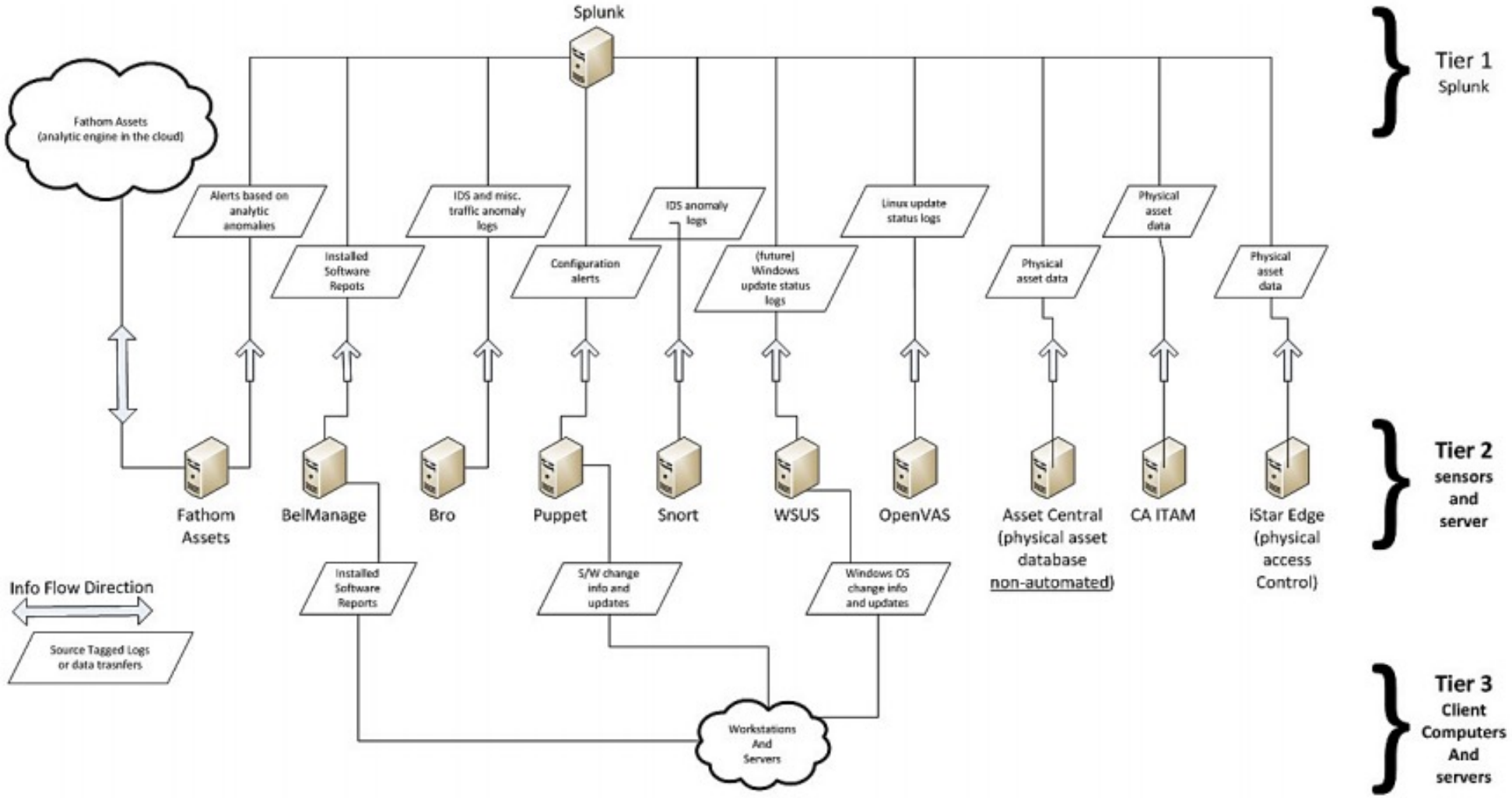
Week 4



NIST IT Asset Management System Model

- ☑ Replaceability
- ☑ Convenience
- ☑ Sensitivity
- ☑ Emotion
- ☑ Dependence
- ☑ Liability
- ☑ Stewardship
- ☑ Finance
- ☑ Preference

Week 4



NIST IT Asset Management (ITAM) Dataflow Reference Architecture

Week 4

Premise

- Routers
- Switches
- Hosts
- Vulnerability Data
- . . .
- Load Balancers

Cloud

- Workloads
- Applications
- . . .
- Google, Microsoft, AWS, VMWare, Cisco

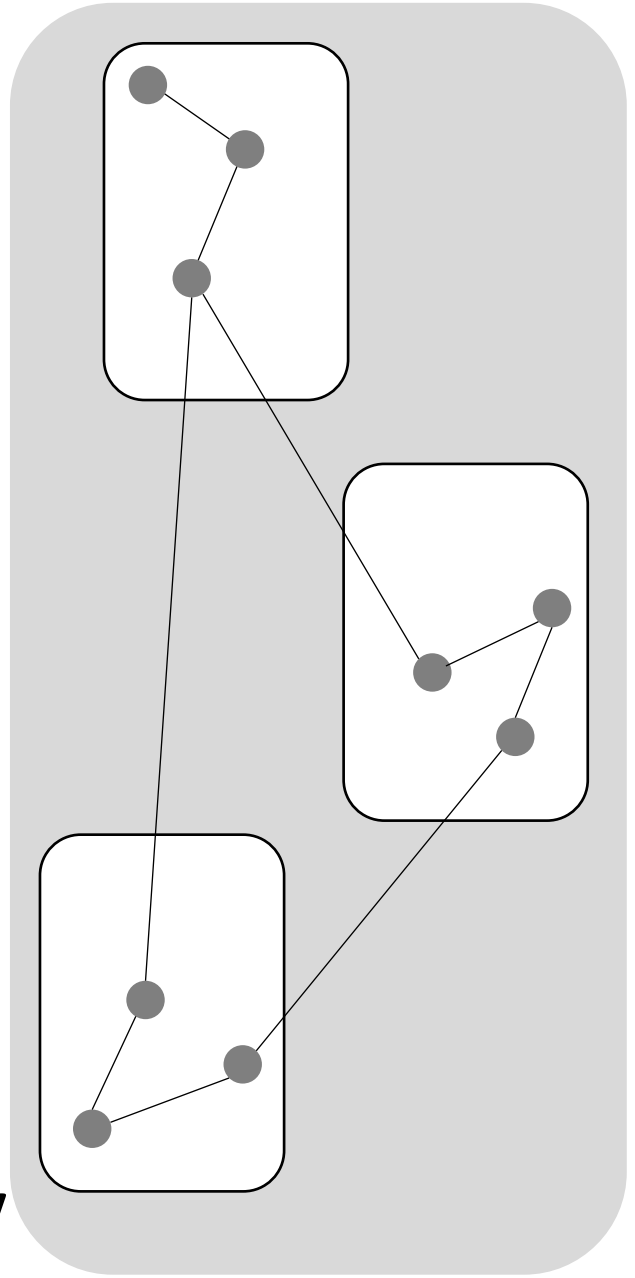
Collect Network Data

Process and Analyze

Asset Discovery Platform (Network Data)

Generate Connection Model

Network Device Connectivity Map



Typical Automated Asset Discovery

What is a Threat Asset Matrix?
(Hint: It is Your Midterm Assignment)

Week 4

	Threat 1	Threat 2	. . .	Threat m	*List the threats (Probably CIA)*
Asset 1					
Asset 2					
.					
.					
.					
Asset n					
List the assets (Based on mission)					

Developing a Threat-Asset Matrix

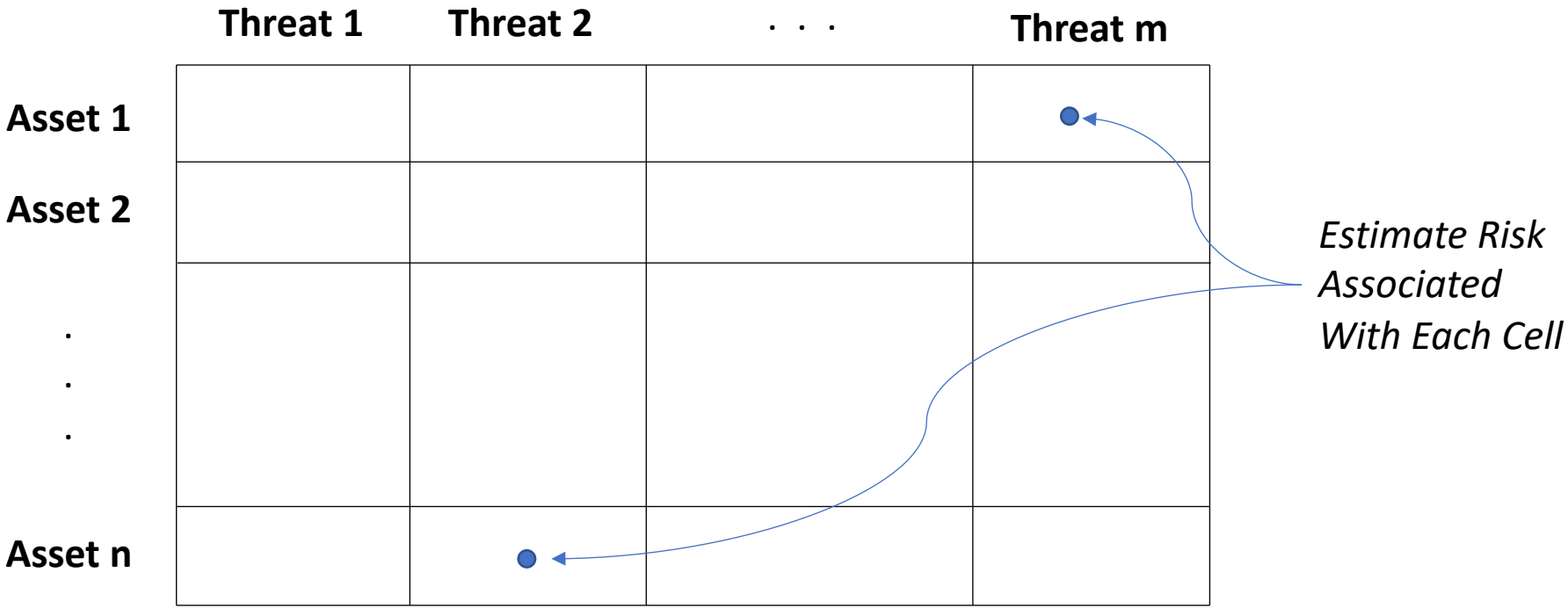
Week 4

Developing a Threat-Asset Matrix

	Threat 1	Threat 2	. . .	Threat m
Asset 1				
Asset 2				
. . .				
Asset n				

Create (m x n) Matrix of Threat-Asset Pairs

Week 4



Developing a Threat-Asset Matrix

Week 4

Developing a Threat-Asset Matrix

	Confidentiality	Integrity	Availability
Hardware			P = 3, 2, 1 C = 3, 2, 1 R = P * C
Software			
Information			

Estimate probability P and consequence C on simple scale (3, 2, 1)

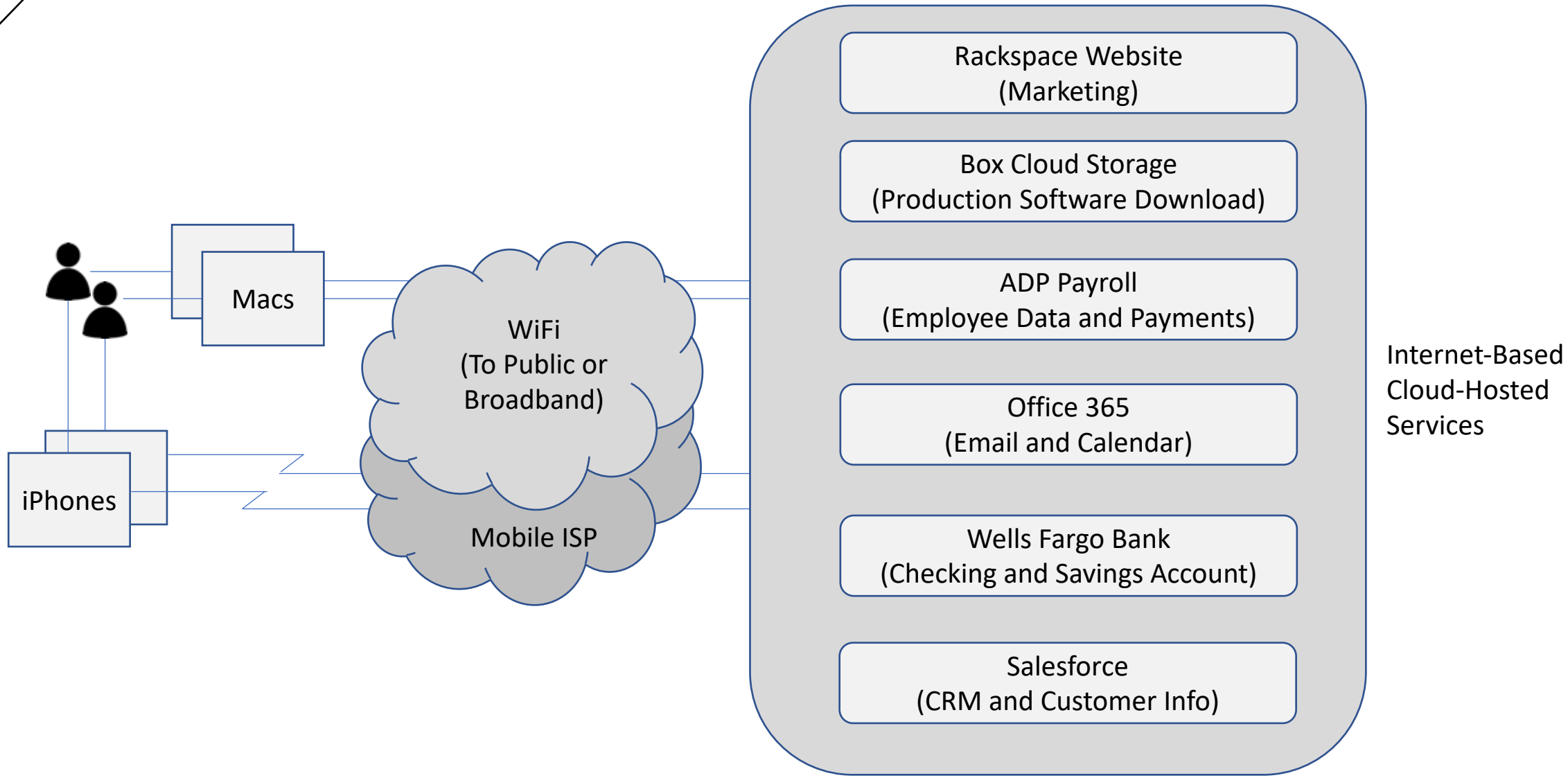
Week 4

Developing a Threat-Asset Matrix

	Confidentiality	Integrity	Availability
Hardware	P = 3, 2, 1 C = 3, 2, 1 R = P * C	P = 3, 2, 1 C = 3, 2, 1 R = P * C	P = 3, 2, 1 C = 3, 2, 1 R = P * C
Software	P = 3, 2, 1 C = 3, 2, 1 R = P * C	P = 3, 2, 1 C = 3, 2, 1 R = P * C	P = 3, 2, 1 C = 3, 2, 1 R = P * C
Information	P = 3, 2, 1 C = 3, 2, 1 R = P * C	P = 3, 2, 1 C = 3, 2, 1 R = P * C	P = 3, 2, 1 C = 3, 2, 1 R = P * C

Perform risk estimates one-by-one for entire threat-asset matrix

Week 4



Case Study: Manage and Secure Assets for ACME Software-R-Us Inc.

Week 4

Developer MACs (Software, etc.)

Developer iPhones (Email, Photos, etc.)

Rackspace Website (Papers, PDFs, etc.)

Box Cloud Storage (Production Software)

ADP Payroll (Employee PII, etc.)

Office 365 (Email, Calendars, etc.)

Wells Fargo Bank (Checking Acct, etc.)

Salesforce (CRM, Customer Data, etc.)

Eight major asset types

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

Week 4

	Confidentiality	Integrity	Availability	Theft/Fraud
Developer MACs (Software, etc.)				
Developer iPhones (Email, Photos, etc.)				
Rackspace Website (Papers, PDFs, etc.)				
Box Cloud Storage (Production Software)				
ADP Payroll (Employee PII, etc.)				
Office 365 (Email, Calendars, etc.)				
Wells Fargo Bank (Checking Acct, etc.)				
Salesforce (CRM, Customer Data, etc.)				

Four major threat types

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

Week 4

	Confidentiality	Integrity	Availability	Theft/Fraud
Developer MACs (Software, etc.)				
Developer iPhones (Email, Photos, etc.)				
Rackspace Website (Papers, PDFs, etc.)				
Box Cloud Storage (Production Software)				
ADP Payroll (Employee PII, etc.)				
Office 365 (Email, Calendars, etc.)				
Wells Fargo Bank (Checking Acct, etc.)				
Salesforce (CRM, Customer Data, etc.)				

Create an (8 X 4) matrix = 32 cells to analyze

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

Week 4

Cell 1: Software (source code) in development on the Mac is valuable to a competitor, but Mac is reasonably well protected against malware:
Estimate: **P = 2, C = 3, R = 6**

	Confidentiality	Integrity	Availability	Theft/Fraud
Developer MACs (Software, etc.)	6			
Developer iPhones (Email, Photos, etc.)				
Rackspace Website (Papers, PDFs, etc.)				
Box Cloud Storage (Production Software)				
ADP Payroll (Employee PII, etc.)				
Office 365 (Email, Calendars, etc.)				
Wells Fargo Bank (Checking Acct, etc.)				
Salesforce (CRM, Customer Data, etc.)				

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

Week 4

Cell 2: Contacts and email are somewhat valuable to a competitor, but iPhone is biometrically well-protected against physical access:
Estimate: **P = 1, C = 2, R = 2**

	Confidentiality	Integrity	Availability	Theft/Fraud
Developer MACs (Software, etc.)	6			
Developer iPhones (Email, Photos, etc.)	2			
Rackspace Website (Papers, PDFs, etc.)				
Box Cloud Storage (Production Software)				
ADP Payroll (Employee PII, etc.)				
Office 365 (Email, Calendars, etc.)				
Wells Fargo Bank (Checking Acct, etc.)				
Salesforce (CRM, Customer Data, etc.)				

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

Week 4

Cell 3: Website reasonably well-administered but nothing all that sensitive is stored in the marketing oriented site (no eCommerce).
Estimate: **P = 1, C = 1, R = 1**

	Confidentiality	Integrity	Availability	Theft/Fraud
Developer MACs (Software, etc.)	6			
Developer iPhones (Email, Photos, etc.)	2			
Rackspace Website (Papers, PDFs, etc.)	1			
Box Cloud Storage (Production Software)				
ADP Payroll (Employee PII, etc.)				
Office 365 (Email, Calendars, etc.)				
Wells Fargo Bank (Checking Acct, etc.)				
Salesforce (CRM, Customer Data, etc.)				

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

Week 4

Cell 4: This represents public cloud storage and customer download support for the company's production software, thus high risk estimated. Estimate: **P = 3, C = 3, R = 9**

	Confidentiality	Integrity	Availability	Theft/Fraud
Developer MACs (Software, etc.)	6			
Developer iPhones (Email, Photos, etc.)	2			
Rackspace Website (Papers, PDFs, etc.)	1			
Box Cloud Storage (Production Software)	9			
ADP Payroll (Employee PII, etc.)				
Office 365 (Email, Calendars, etc.)				
Wells Fargo Bank (Checking Acct, etc.)				
Salesforce (CRM, Customer Data, etc.)				

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

Week 4

Cells 5 - 8: These are well-managed SaaS services with sensitive data stored and accessible to hackers. Estimated suitable risk profiles for each.

	Confidentiality	Integrity	Availability	Theft/Fraud
Developer MACs (Software, etc.)	6			
Developer iPhones (Email, Photos, etc.)	2			
Rackspace Website (Papers, PDFs, etc.)	1			
Box Cloud Storage (Production Software)	9			
ADP Payroll (Employee PII, etc.)	P = 1, C = 2, R = 2			
Office 365 (Email, Calendars, etc.)	P = 2, C = 3, R = 6			
Wells Fargo Bank (Checking Acct, etc.)	P = 1, C = 2, R = 2			
Salesforce (CRM, Customer Data, etc.)	P = 2, C = 3, R = 6			

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

Week 4

	Confidentiality	Integrity	Availability	Theft/Fraud
Developer MACs (Software, etc.)	6			
Developer iPhones (Email, Photos, etc.)	2			
Rackspace Website (Papers, PDFs, etc.)	1			
Box Cloud Storage (Production Software)	9			
ADP Payroll (Employee PII, etc.)	2			
Office 365 (Email, Calendars, etc.)	6			
Wells Fargo Bank (Checking Acct, etc.)	2			
Salesforce (CRM, Customer Data, etc.)	6			

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

Week 4

	Confidentiality	Integrity	Availability	Theft/Fraud
Developer MACs (Software, etc.)	6	6	2	2
Developer iPhones (Email, Photos, etc.)	2	2	2	2
Rackspace Website (Papers, PDFs, etc.)	1	6	3	1
Box Cloud Storage (Production Software)	9	9	9	9
ADP Payroll (Employee PII, etc.)	2	2	2	2
Office 365 (Email, Calendars, etc.)	6	6	3	1
Wells Fargo Bank (Checking Acct, etc.)	2	2	1	3
Salesforce (CRM, Customer Data, etc.)	6	6	1	4

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

Week 4

Business Asset	Estimated Risk
Box Cloud Storage (Production Software)	Total Risk = 36 – 1st Highest Risk Asset
Salesforce (CRM, Customer Data, etc.)	Total Risk = 17 – 2nd Highest Risk Asset
Developer MACs (Software, etc.)	Total Risk = 16 – 3rd Highest Risk Asset
Office 365 (Email, Calendars, etc.)	Total Risk = 16 – 3rd Highest Risk Asset
Rackspace Website (Papers, PDFs, etc.)	Total Risk = 11 – 4th Highest Risk Asset
Developer iPhones (Email, Photos, etc.)	Total Risk = 8 – Lowest Risk Asset
ADP Payroll (Employee PII, etc.)	Total Risk = 8 – Lowest Risk Asset
Wells Fargo Bank (Checking Acct, etc.)	Total Risk = 8 – Lowest Risk Asset

Illustrating a Threat-Asset Matrix: ACME Software-R-US Inc.

What is Our Midterm Assignment?

Week 4

- Identify and describe a fictitious enterprise network (you can draw or describe) and carefully list the valued assets for this network.
- (It would be recommended to keep the number of assets more than 10 but less than 25.)
- Then, create a threat-asset matrix for your fictitious example and estimate the security risk for each individual cell in the matrix.
- Write a 1-2 sentence justification for each risk estimate.
- You are welcome to draw the matrix by hand (scan and cut the image into your paper) or you can use a tool such as Excel or PowerPoint.
- Submit your assignment via the Course Site

Assignment 1: Due October 18th