

Week 4



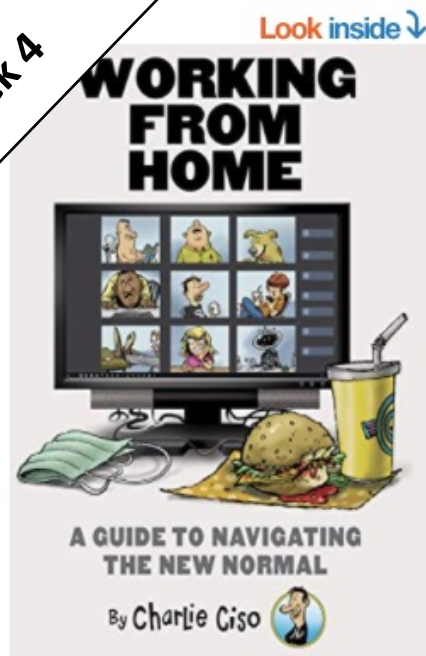
**STEVENS**  
INSTITUTE of TECHNOLOGY  
THE INNOVATION UNIVERSITY®



# **An Introduction to Cyber Security – CS 573**

Instructor: Dr. Edward G. Amoroso  
[eamoroso@tag-cyber.com](mailto: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 [Email](#) [Facebook](#) [Twitter](#) [Pinterest](#) [Embed](#)

Follow the Author



[Edward G. Amoroso](#)

+ Follow

## Charlie Ciso



READ ON  
ANY DEVICE

[Get free Kindle app](#)



# 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



Books ▾ from cia to apt 🔍

[Shop Back to School](#)

[Departments ▾](#)
[Browsing History ▾](#)
[Edward's Amazon.com](#)
[Today's Deals](#)
[Gift Cards & Registry](#)
[Sell](#)
[Help](#)

[Books](#)
[Advanced Search](#)
[New Releases](#)
[NEW! Amazon Charts](#)
[Best Sellers & More](#)
[The New York Times® Best Sellers](#)
[Children's Books](#)
[Textbooks](#)
[Textbook Rentals](#)
[Sell Us Your Books](#)
[Best Books of the Month](#)

[Back to search results for "from cia to apt"](#)

[From CIA to APT: An Introduction to Cyber Security](#) and over one million other books are available for **Amazon Kindle**. [Learn more](#)



[Look inside ↴](#)

Kindle

\$0.00 **kindleunlimited**

Paperback

**\$25.00**

This title and over 1 million more available with **Kindle Unlimited**  
\$9.99 to buy

2 New from **\$25.00**

Most introductory books on cyber security are either too technical for popular readers, or too casual for professional ones. This book, in contrast, is intended to reside somewhere in the middle. That is, while concepts are explained in a friendly manner for any educated adult, the book also necessarily includes network diagrams with the obligatory references to clouds, servers, and packets. But don't let this scare you. Anyone with an ounce of determination can get through every page of this book, and will come out better informed, not only on cyber security, but also on computing, networking, and software. While it is true that college students will find the material particularly accessible, any adult with the desire to learn will find this book part of an exciting new journey. A great irony is that the dizzying assortment of articles, posts, and books currently available on cyber security makes it difficult to navigate the topic.

[Read more](#)

[Report incorrect product information.](#)

[Share](#)
[✉](#)
[f](#)
[t](#)
[p](#)

Buy New

\$25.00

Qty:

[FREE Shipping.](#)

In Stock.

Ships from and sold by Amazon.com.  
Gift-wrap available.

☐ Yes, I want **FREE Two-Day Shipping** with **Amazon Prime**



[Turn on 1-Click ordering for this browser](#)

Want it **Wednesday, Aug. 30**? Order within **19 hrs 39 mins** and choose **Two-Day Shipping** at checkout. [Details](#)

Ship to:

Edward Amoroso- Sparta - 07871 ▾




[See all 2 images](#)

## **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

## 2021 TAG CYBER SECURITY QUARTERLY



### 2021 TAG Cyber Security Quarterly Report

Insights, Perspectives, and Commentary on Cyber Risks, Security Safeguards, and Technology Innovations

[DOWNLOAD REPORT - 1ST QUARTER 2021](#)

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

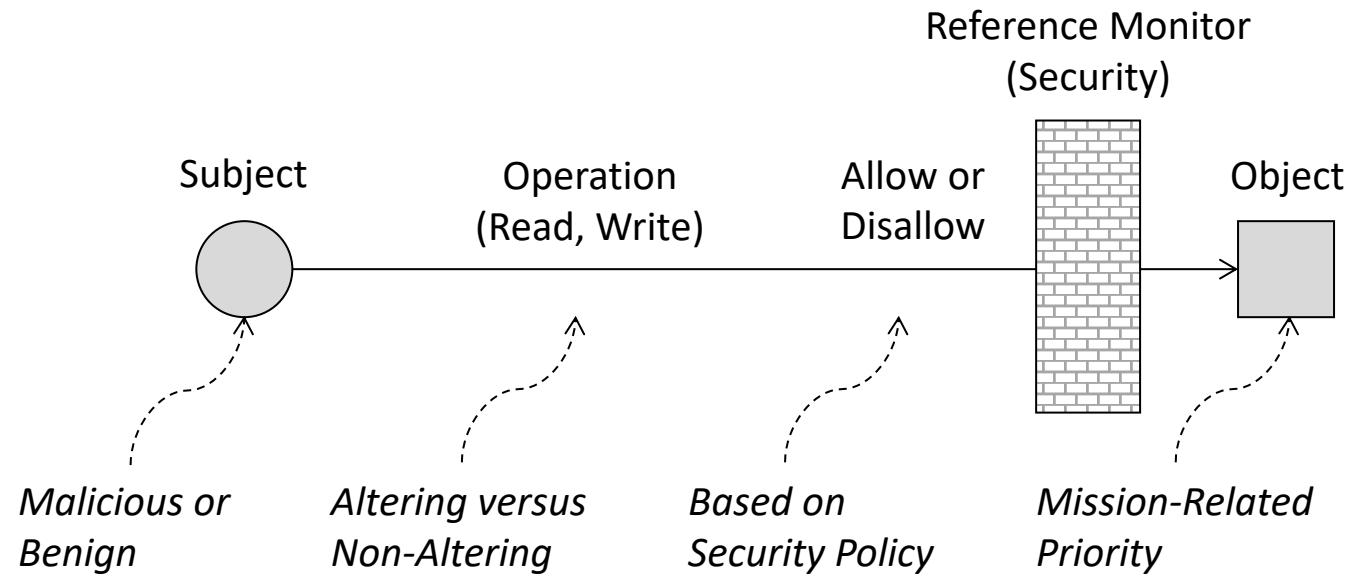
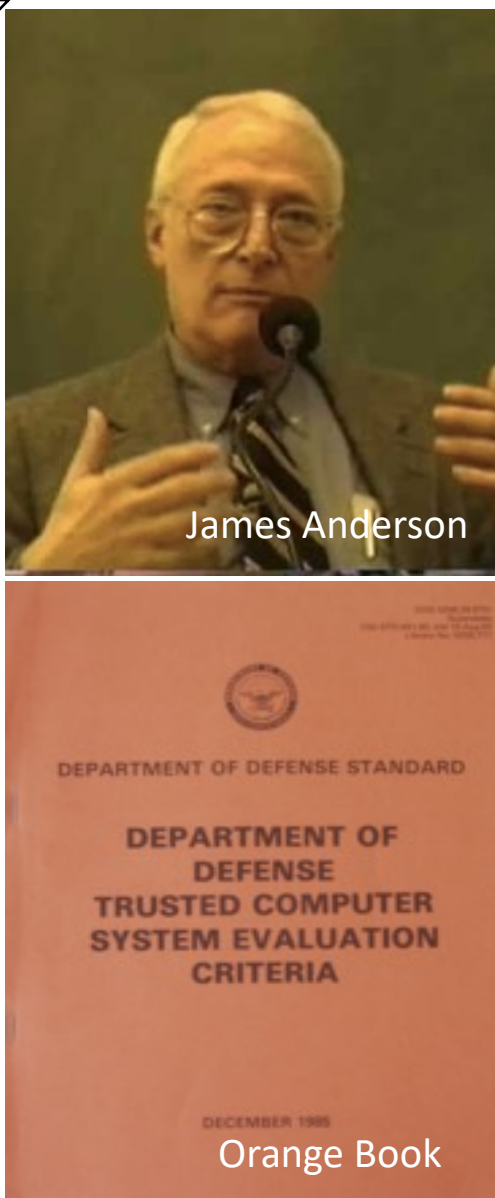
Week 4



**Week 4: Threat-Vulnerability Analysis**

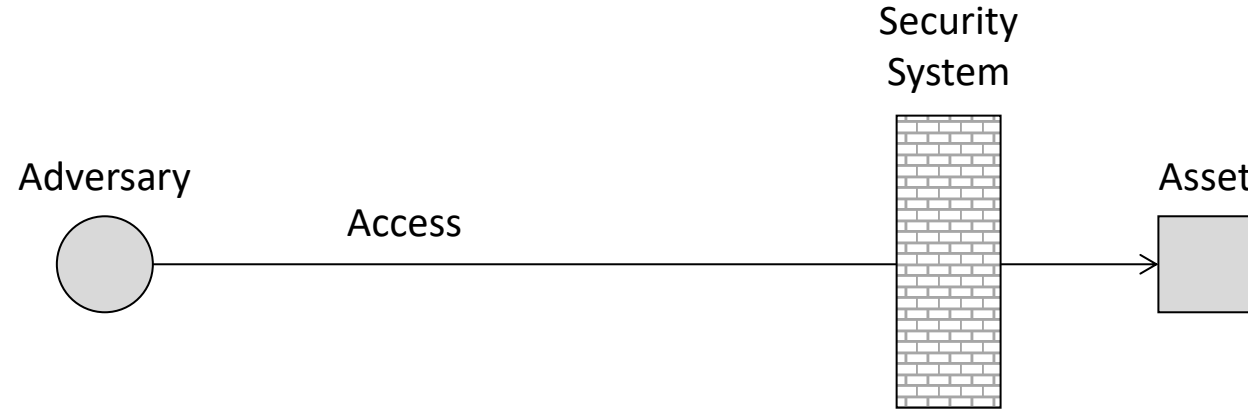
What are the Foundational Issues in Cyber Security?



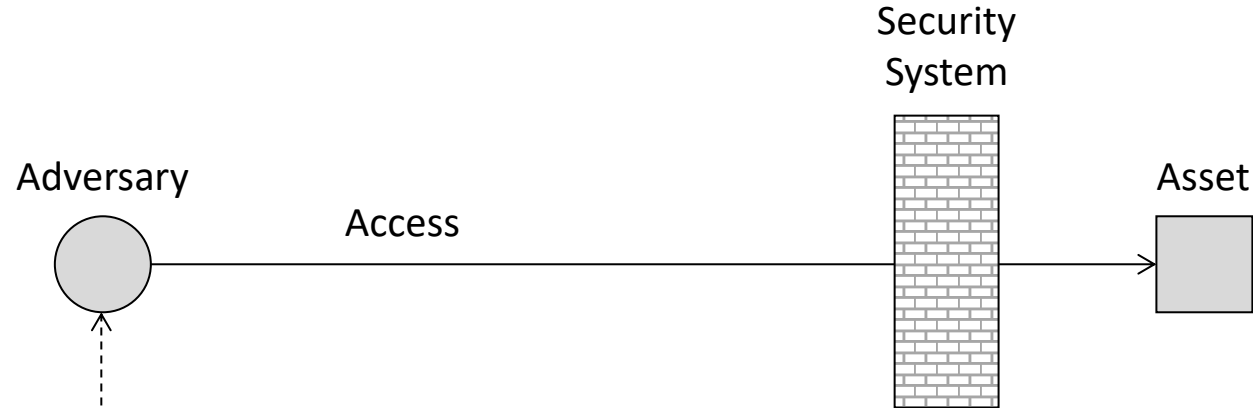


## Cyber Security: Subject-Object Reference Model





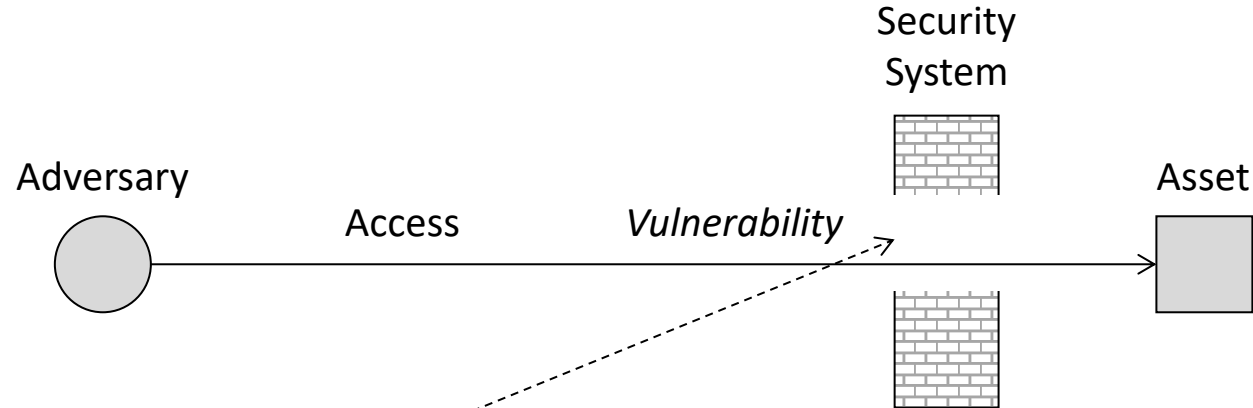
## Cyber Security: Basic Operational Framework



Incomplete  
List

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

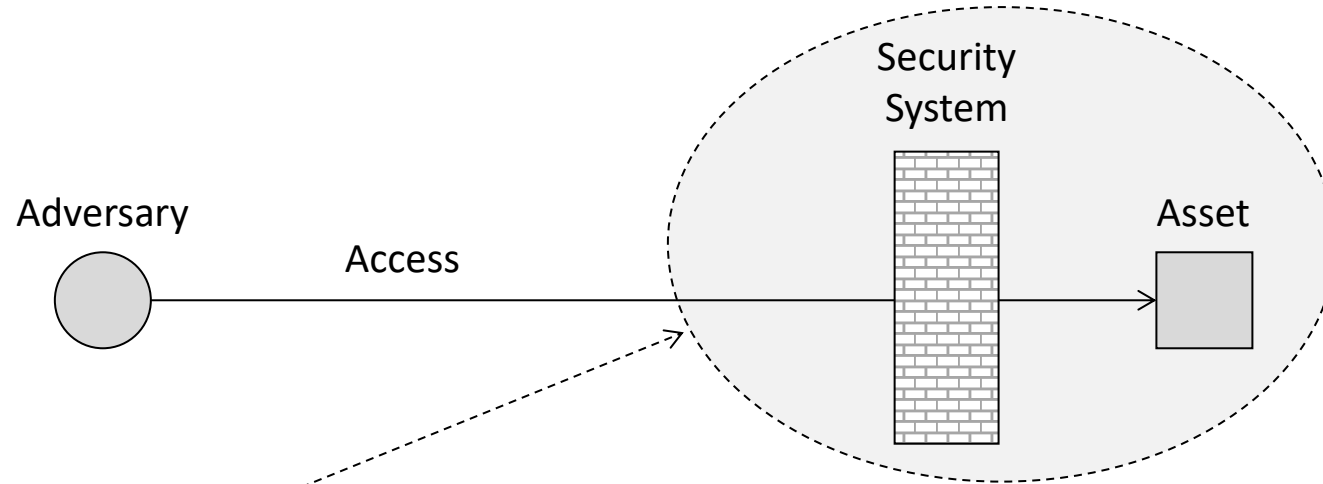
## Cyber Security: Adversary Types



Incomplete  
List

<i>Vulnerability Type</i>	<i>Root Cause</i>	<i>Defining Attributes</i>
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



<i>Threat Type</i>	<i>Motivation</i>	<i>Defining Attributes</i>
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

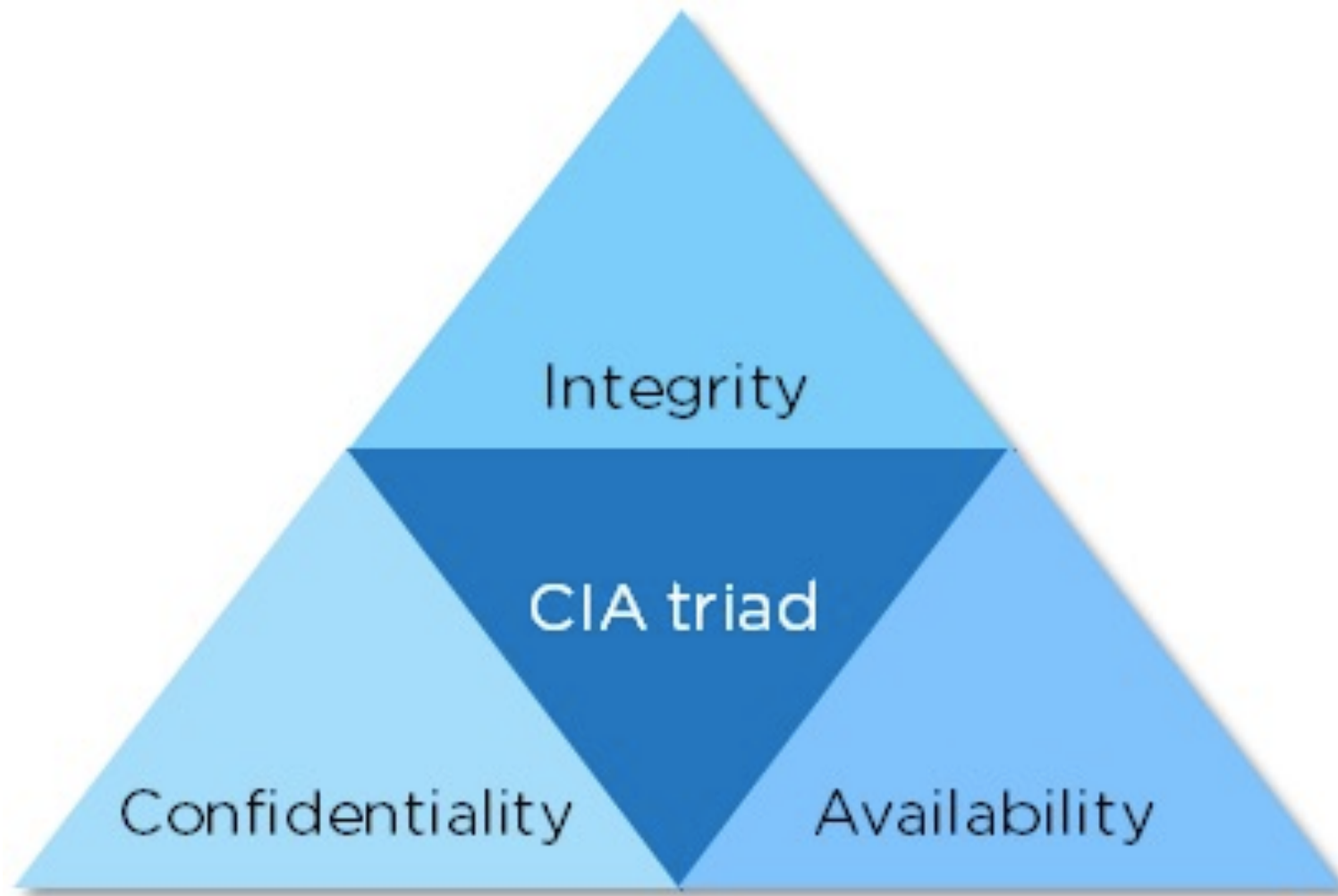
# Cyber Security: Threat Types



What Cyber Security Definitions Should I Memorize?



**Def: Assets – Resources required for organization to meet its mission.**



**Def: Threats – Malicious outcomes levied against assets.**





**Def: Confidentiality Threat – Information disclosed to unauthorized parties.**





**Def: Privacy Threat – *Personal information* disclosed to unauthorized parties.**





**Def: Integrity Threat – Asset maliciously altered (includes destroyed).**





Week 4

**Def: Availability Threat – Asset maliciously blocked from authorized use.**



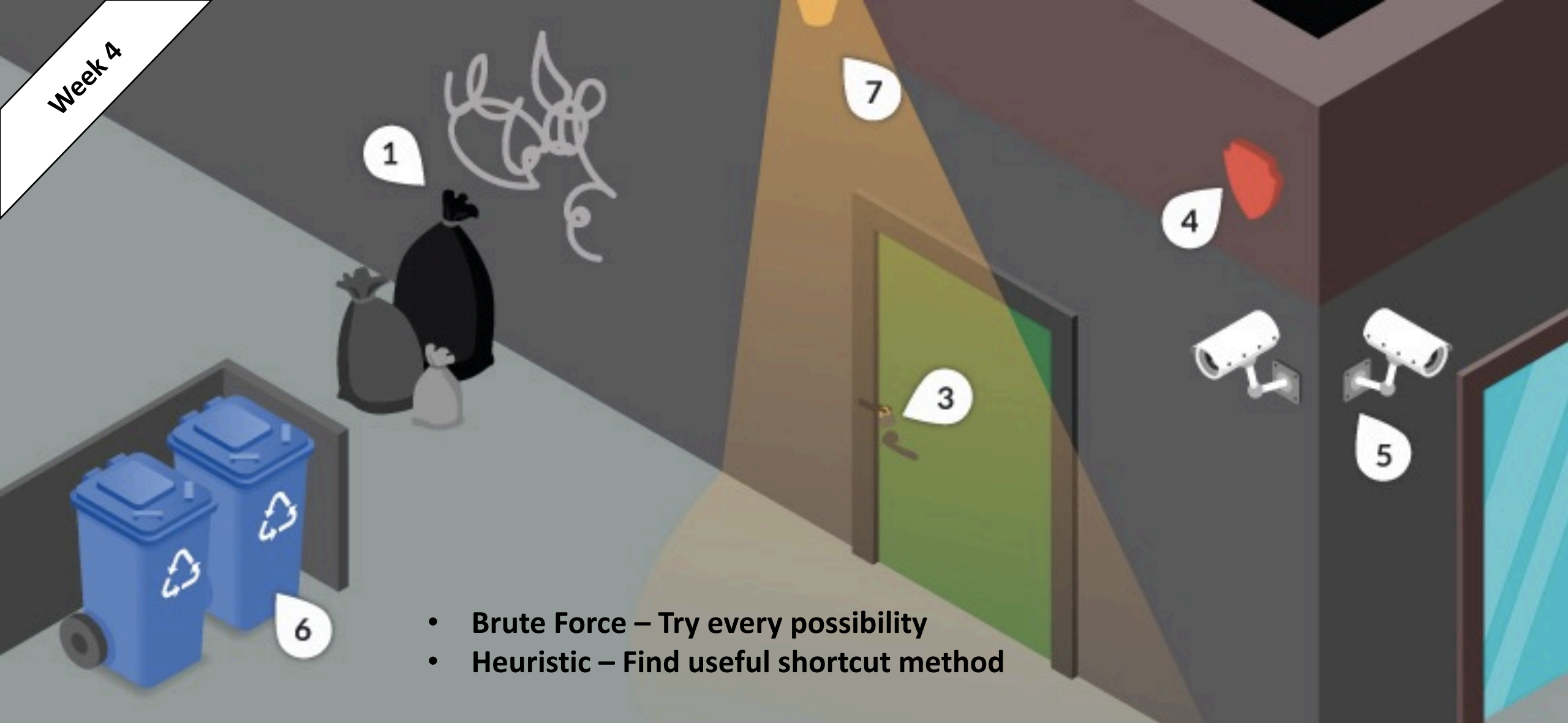


**Def: Theft/Fraud – Stealing service or product without paying.**





**Def: Vulnerability – System bug or attribute that can be maliciously exploited.**



- Brute Force – Try every possibility
- Heuristic – Find useful shortcut method

**Def: Attack – Sequence of steps to exploit a vulnerability.**

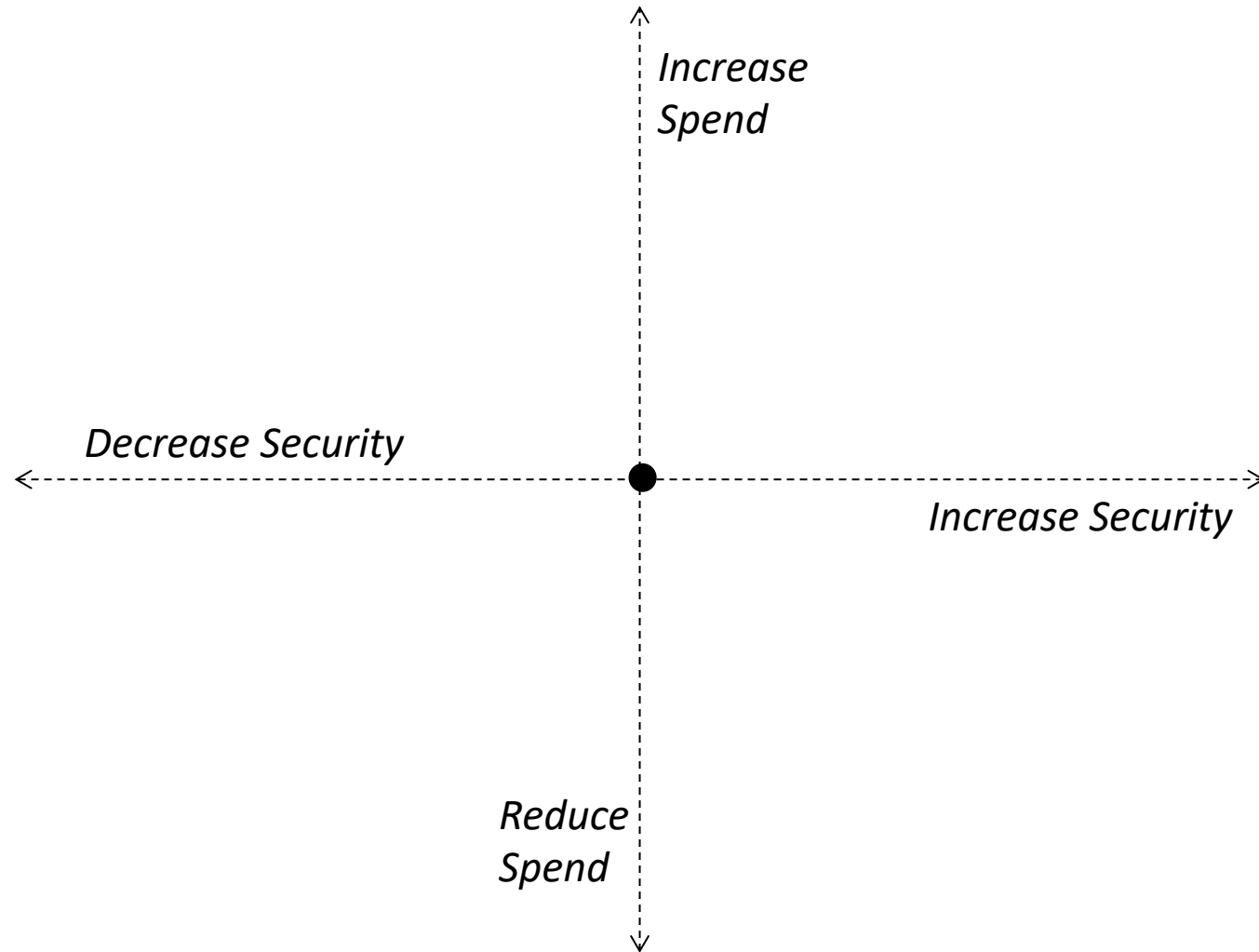


**Risk (R) equals  
Probability (P) of Threat  
times  
Consequence (C) of Threat**

$$R = P * C$$

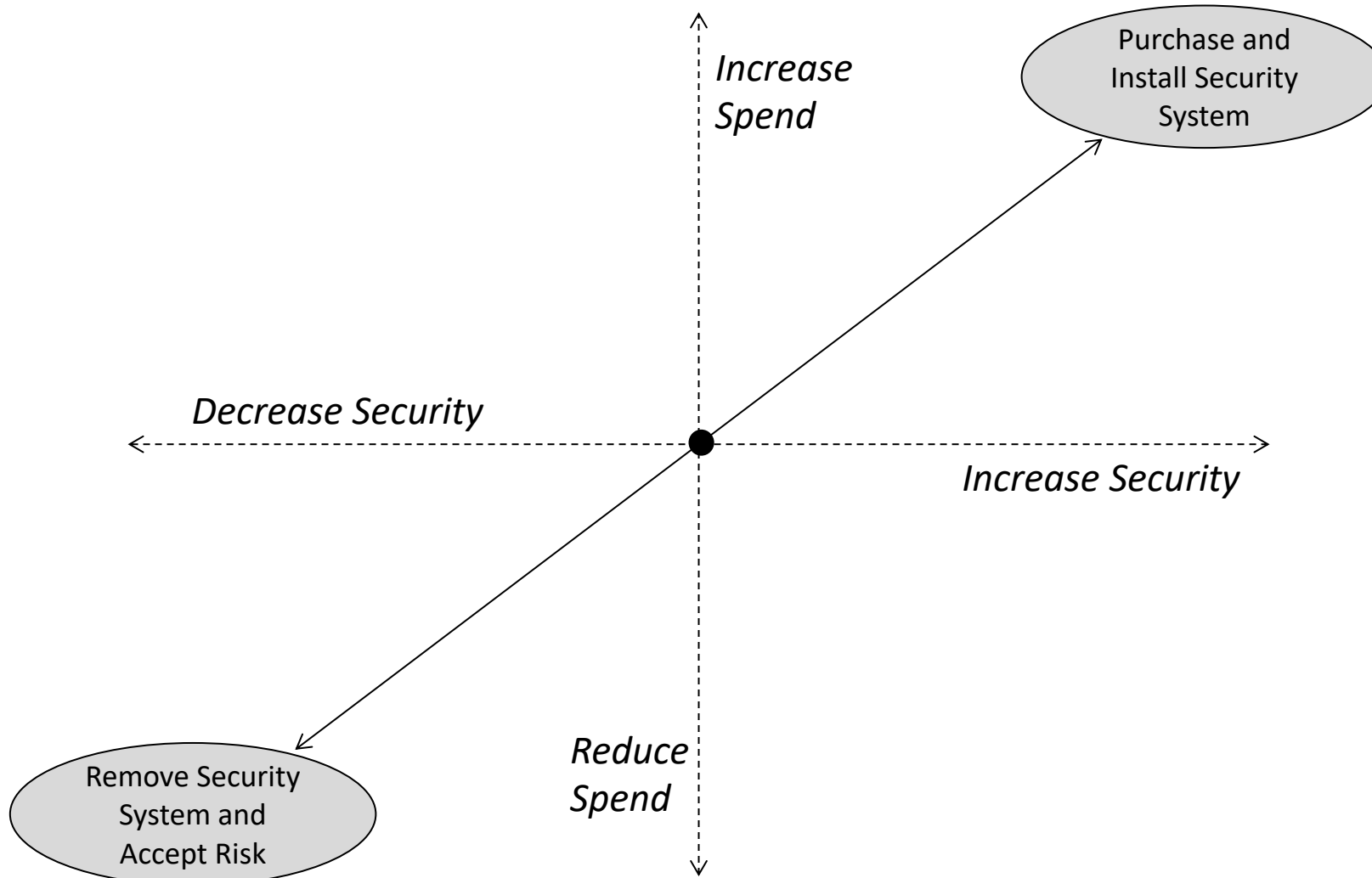
**Def: Risk – Probability “Times” Consequence**

**Week 4**



## Security Risk Assessment – Decision Framework

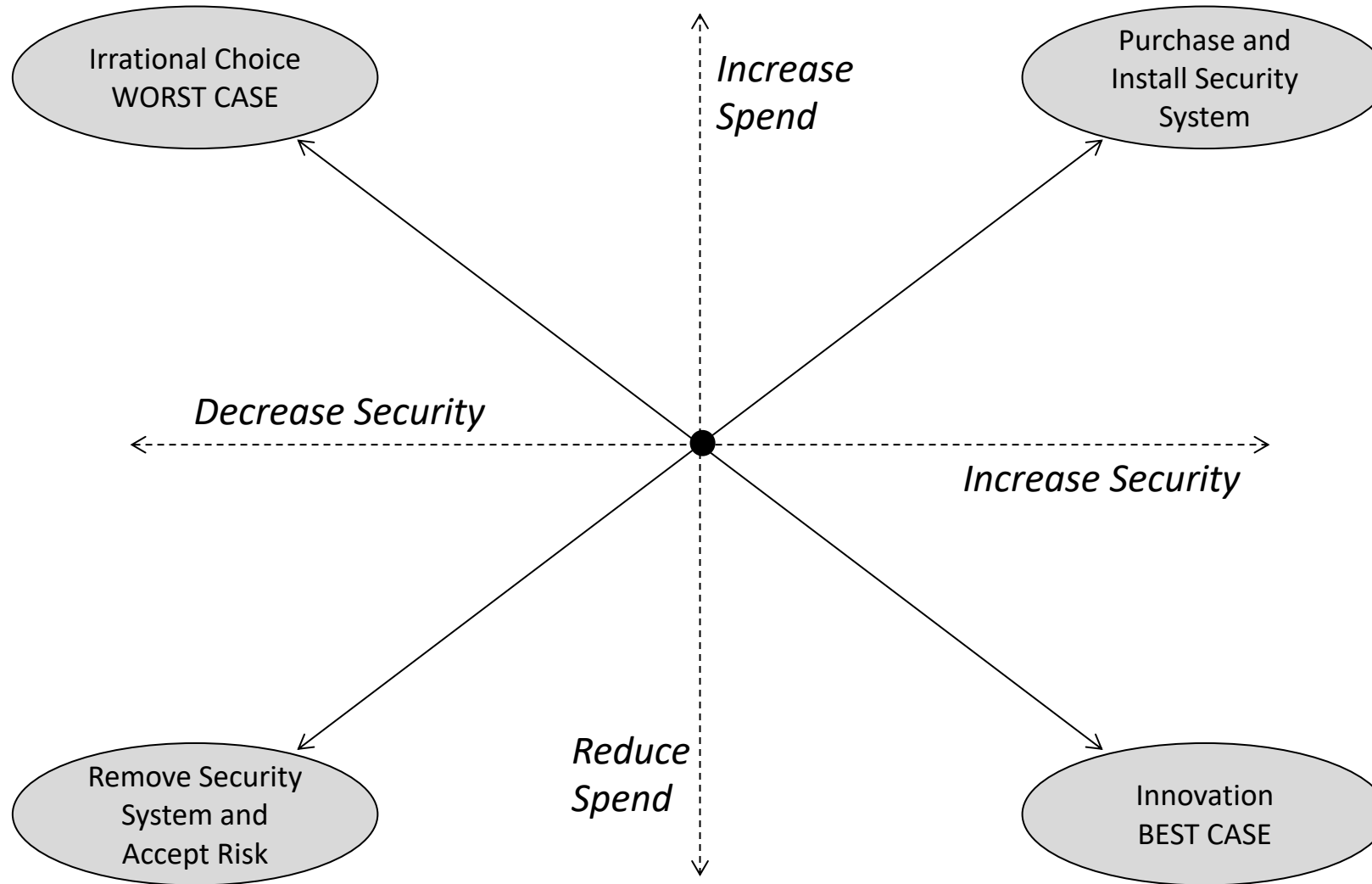
Week 4



## Security Risk Assessment – Decision Framework



**Week 4**



## Security Risk Assessment – Decision Framework

How Are Assets Prioritized?



Week 4

**Illustrating Tiered Prioritization of Assets**

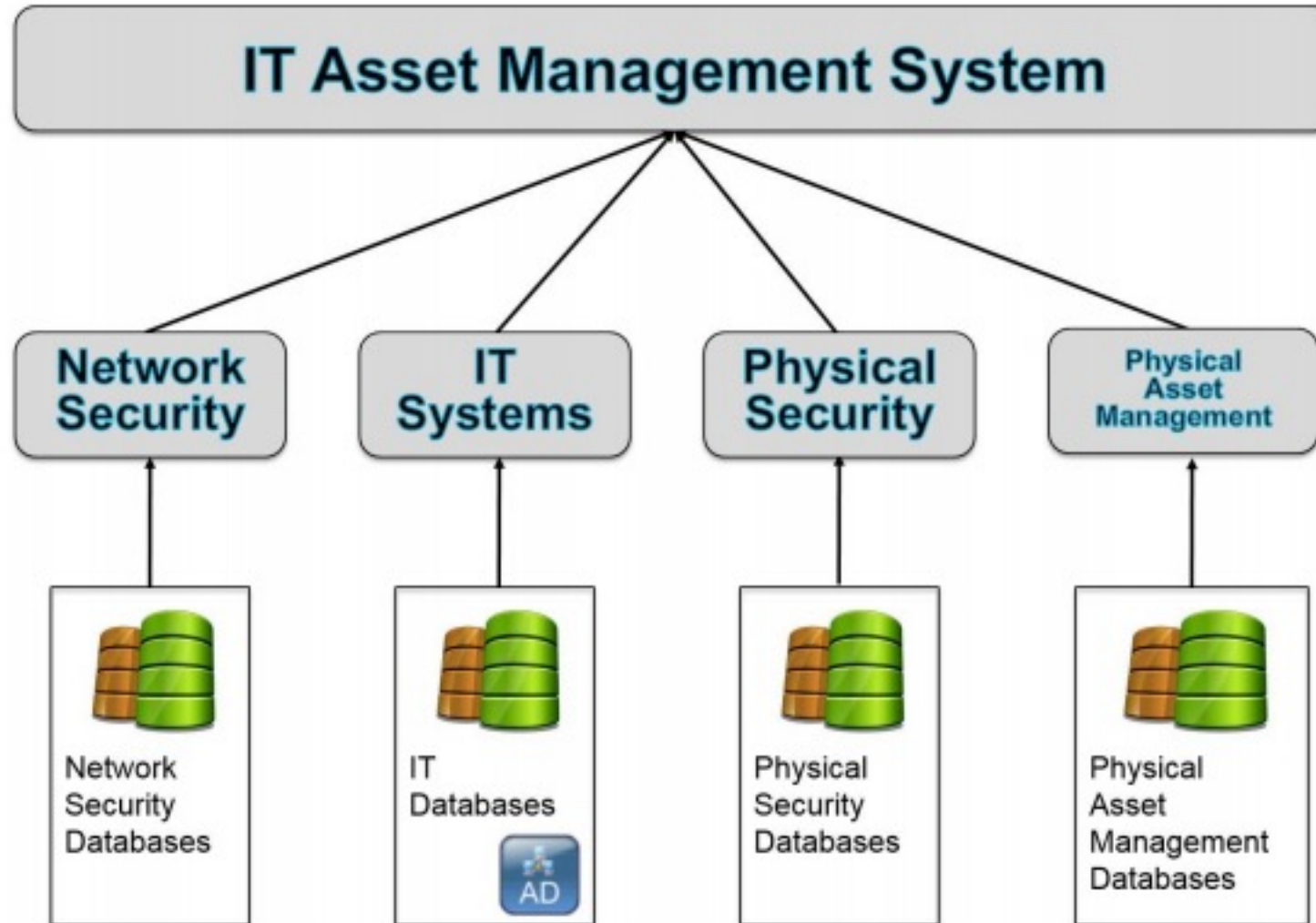
Week 4



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

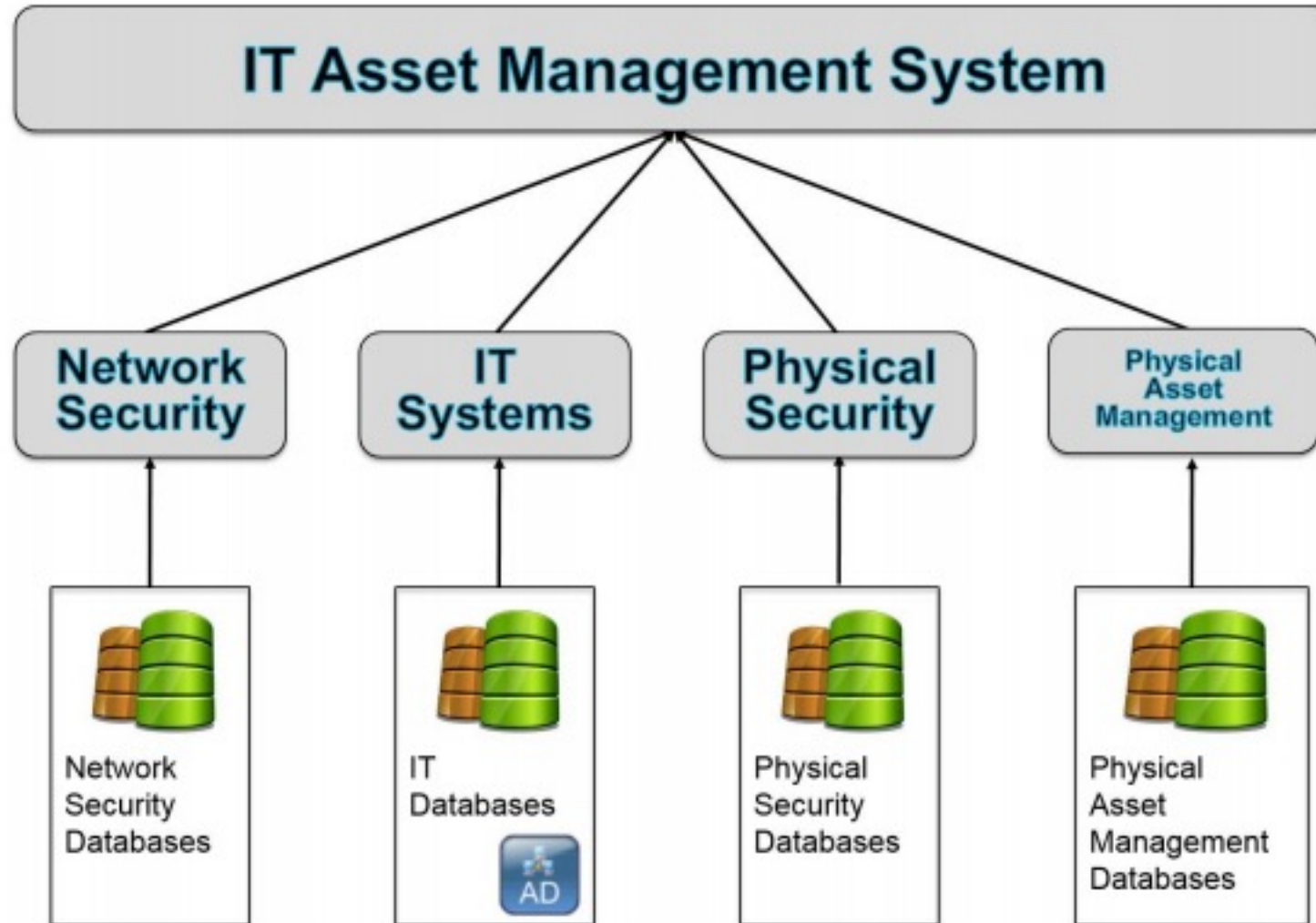
**Illustrating Tiered Prioritization of Assets**





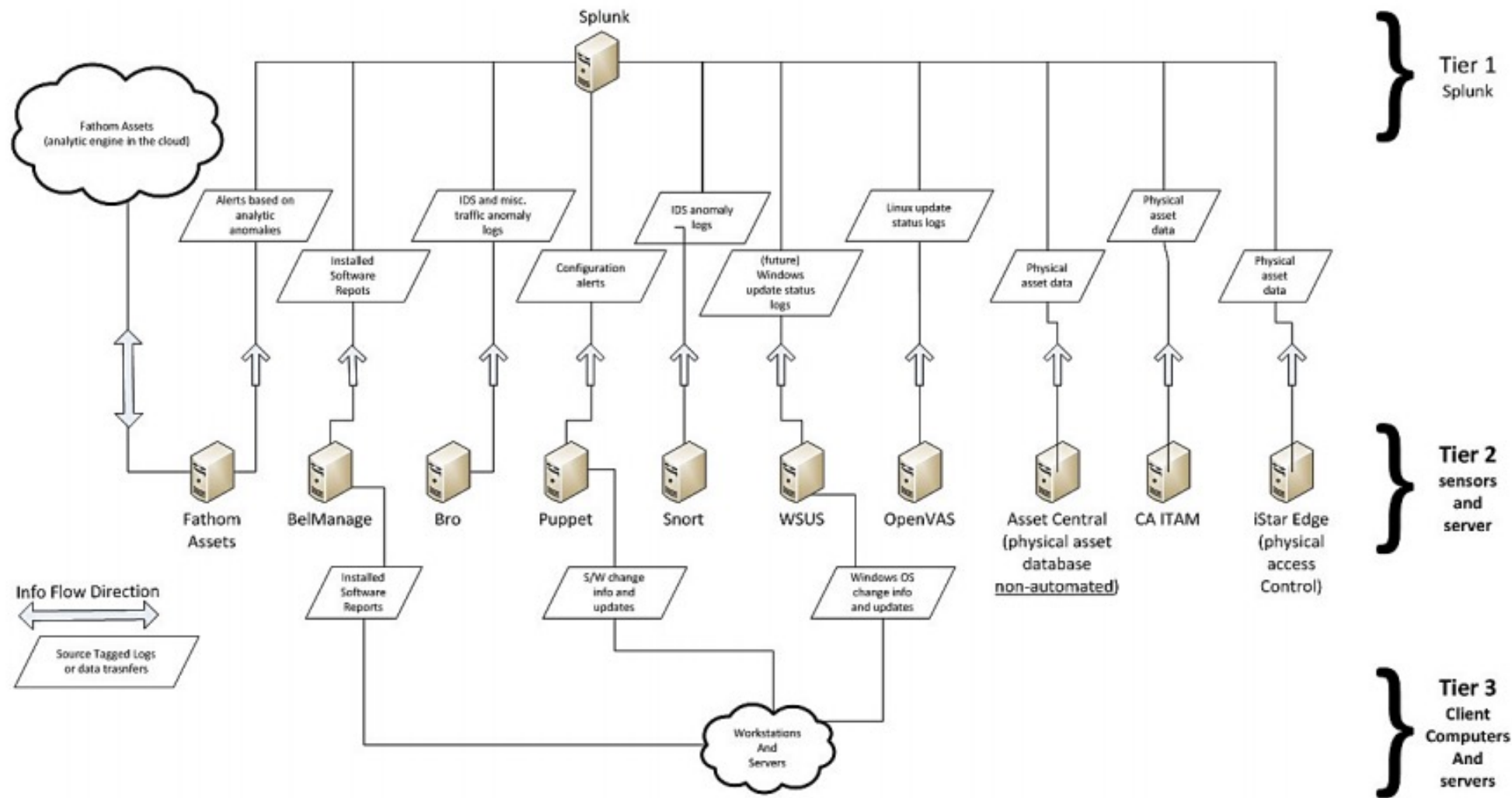
**NIST IT Asset Management System Model**





**NIST IT Asset Management System Model**

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



**NIST IT Asset Management (ITAM) Dataflow Reference Architecture**

Week 4

### Premise

Routers

Switches

Hosts

Vulnerability Data

...

Load Balancers

### Cloud

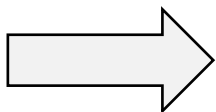
Workloads

Applications

...

Google, Microsoft,  
AWS, VMWare, Cisco

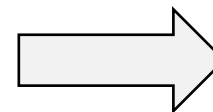
Collect  
Network Data



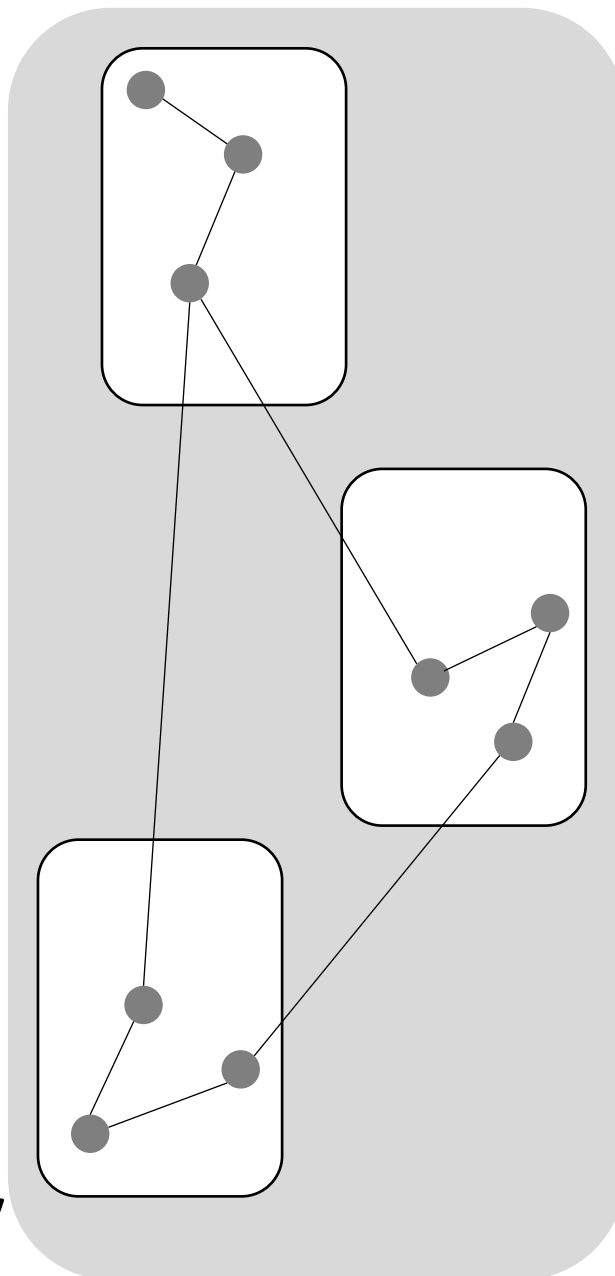
Process and  
Analyze

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**

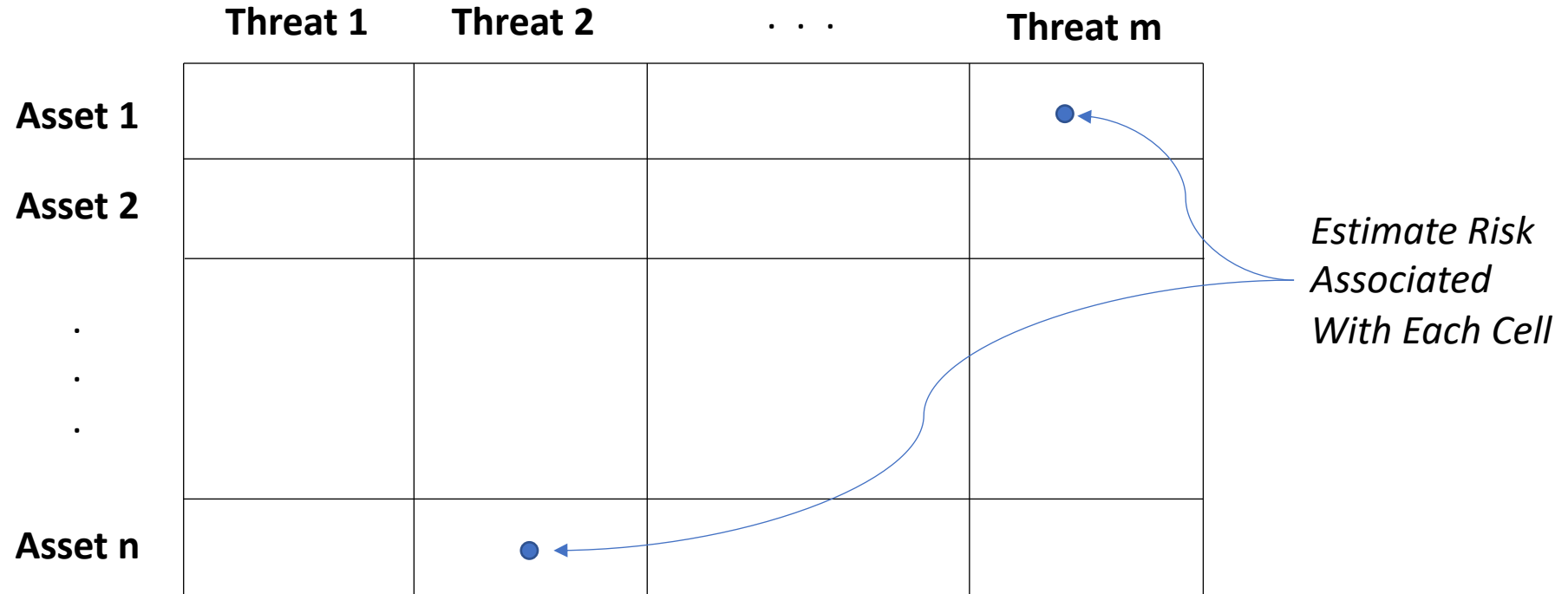
	Threat 1	Threat 2	. . .	Threat m	<i>List the threats (Probably CIA)</i>
Asset 1					
Asset 2					
.					
.					
.					
Asset n					
<i>List the assets (Based on mission)</i>					

**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

Developing a Threat-Asset Matrix



## Developing a Threat-Asset Matrix



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

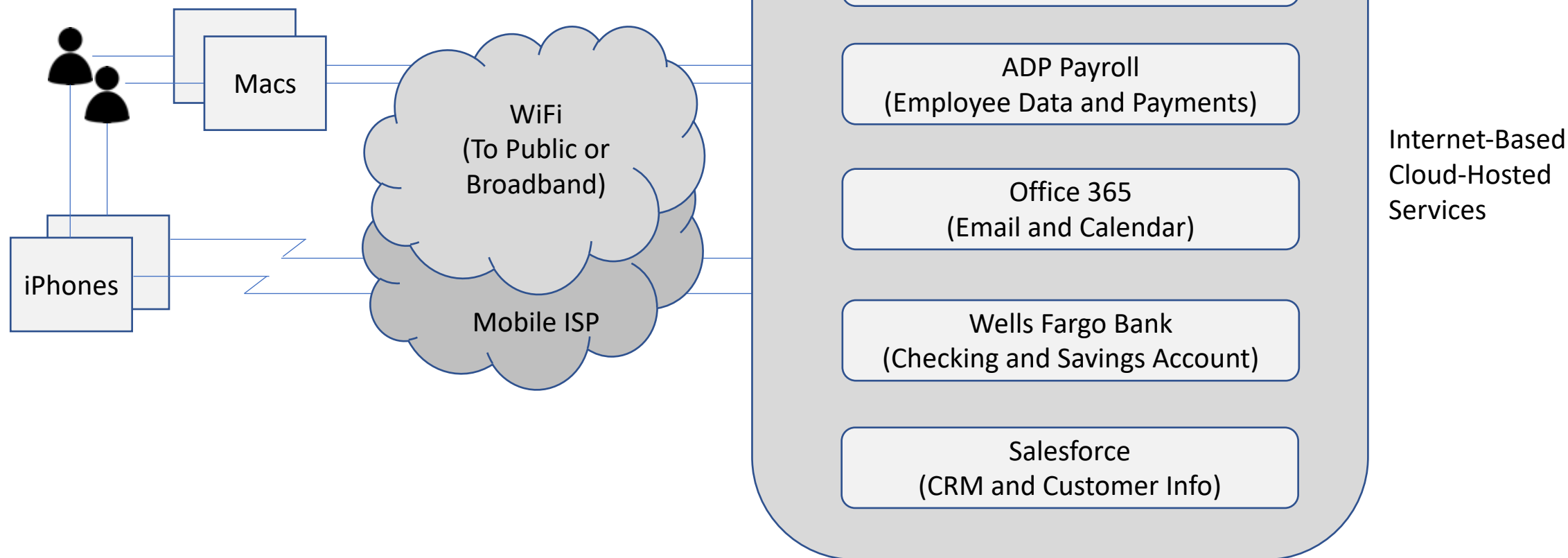
*Estimate probability P  
and consequence C on  
simple scale (3, 2, 1)*

## 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*

# Developing a Threat-Asset Matrix



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



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.)

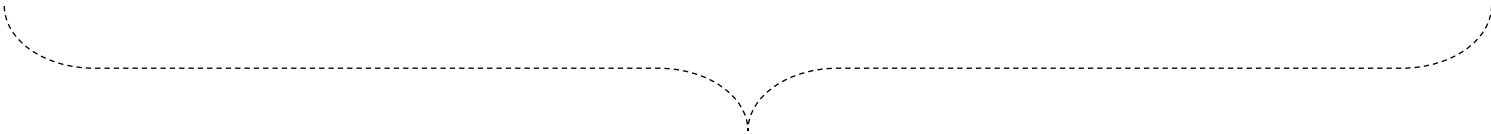
Salesforce (CRM, Customer Data, etc.)

*Eight major  
asset types*

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

- 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.)

**Confidentiality                      Integrity                      Availability                      Theft/Fraud**



*Four major  
threat types*

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

	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.**

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**

- 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.)

Confidentiality	Integrity	Availability	Theft/Fraud
6			

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



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**

- 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.)

Confidentiality	Integrity	Availability	Theft/Fraud
6			
2			

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

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**

- 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.)

Confidentiality	Integrity	Availability	Theft/Fraud
6			
2			
1			

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

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**

- 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.)

Confidentiality	Integrity	Availability	Theft/Fraud
6			
2			
1			
9			

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

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

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.)

Confidentiality	Integrity	Availability	Theft/Fraud
6			
2			
1			
9			
P = 1, C = 2, R = 2			
P = 2, C = 3, R = 6			
P = 1, C = 2, R = 2			
P = 2, C = 3, R = 6			

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



	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.

	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.

Business Asset	Estimated Risk
Box Cloud Storage (Production Software)	Total Risk = 36 – 1 <sup>st</sup> Highest Risk Asset
Salesforce (CRM, Customer Data, etc.)	Total Risk = 17 – 2 <sup>nd</sup> Highest Risk Asset
Developer MACs (Software, etc.)	Total Risk = 16 – 3 <sup>rd</sup> Highest Risk Asset
Office 365 (Email, Calendars, etc.)	Total Risk = 16 – 3 <sup>rd</sup> Highest Risk Asset
Rackspace Website (Papers, PDFs, etc.)	Total Risk = 11 – 4 <sup>th</sup> 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?



- 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**