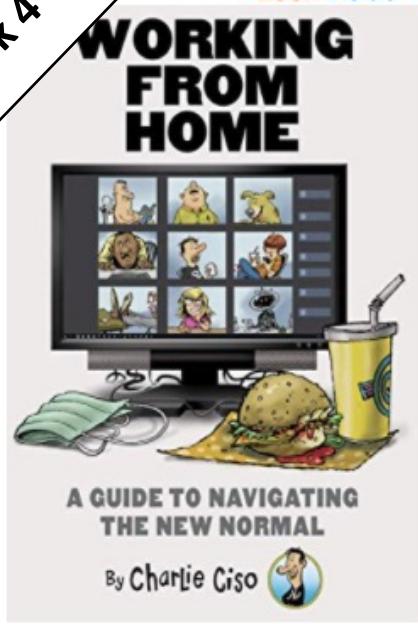




An Introduction to Cyber Security – CS 573

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

Week 4



Look inside ↓

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

Charlie Ciso

Our VP is three minutes late.
Should we all click to drop?



Let's show her the same respect we showed our college professors.



Dropping.
Later.

Click.
Click.

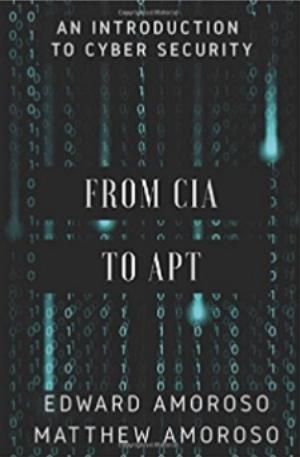
Powell/Amoroso



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

amazon Try Prime Books from cia to apt Shop Back to School Departments Browsing History Edward's Amazon.com Today's Deals Gift Cards & Registry Sell Help EN Hello, Edward Account & Lists Orders Try Prime Cart 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 Paperback – August 11, 2017
by Edward G. Amoroso (Author), Matthew E. Amoroso (Author)
Be the first to review this item
See all 2 formats and editions
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.

Look inside ↗

Flip to back
See all 2 images

Buy New \$25.00
Qty: 1
FREE Shipping.
In Stock.
Ships from and sold by Amazon.com.
Gift-wrap available.
 Yes, I want FREE Two-Day Shipping with Amazon Prime
Add to Cart
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 ▾

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

A PROPOSED BIDEN DOCTRINE FOR CYBER
EDWARD AMOROSO

This article first appeared on the TAG Cyber website in late November 2020 as the results of the 2020 election were becoming clear. The advice and guidance remain 100% relevant today in early 2021.

The first mistake the US federal government has made in cyber security since 2000 has been its misplaced belief in a global alliance or defense. The truth is, the lesson is that the best defense is a good offense. The problem is that preventing attacks is much harder than breaking into systems – hence the twisted emphasis.

It's time to leave cyber offense to US Cyber Command and to refocus 100% of our collective energies on improving our nation's defenses through distribution, virtualization, and simplification. This is best done locally, and it's time to stop thinking that we'll be the ones to be local and distributed. When it comes to cyber defense – we must think local.

The second mistake we have made in cyber has been our over-reliance on the effectiveness of information sharing. Certainly, good threat intelligence is important – and excellent commercial platforms exist. But this belief that a big-group-hug with our international allies will stop cyber threats is both immature and incorrect.

I worry that the Biden team, fully stocked with Obama veterans who will believe in friendly collaboration like religion will mistakenly emphasize cyber alliances as effective cyber defense. Unfortunately, this is like setting up a neighborhood watch to prevent thefts in everyone's roofs. It's much better to just fix the damn roofs.

The third and most serious mistake we have made as a nation in cyber involves our private requests (Obama) and public coping (Trump) that the Russians and Chinese should please stop attacking our infrastructure. Asking your adversary to stop hacking is like calling the clouds to stop raining. This approach does not work.

It amazes me that more experts in our field do not see the folly in this strategy. Imagine the misguided CEO wandering into the board room to explain that the new risk reduction plan is to plead with the bad guys to stop hacking. Any CEO taking this approach would be out of work quickly. And yet, we do this every day on a national level.

My advice instead to the incoming administration would be to create a new strategy – a Biden Doctrine for Cyber, if you will. Such a strategy would boldly establish the following goal: To implement a massively decentralized monitoring system that can detect and respond to a coordinated team that is so effective as to render advances obsolete. Here's how to do it:

First, we should immediately refine any new investment in overlay security programs such as Tritain 2. This centralized monitoring system was conceived twenty years ago and has been about as useful as

2021 SECURITY ANNUAL - 1ST QUARTER TAG CYBER

2021 TAG Cyber Security Quarterly Report

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

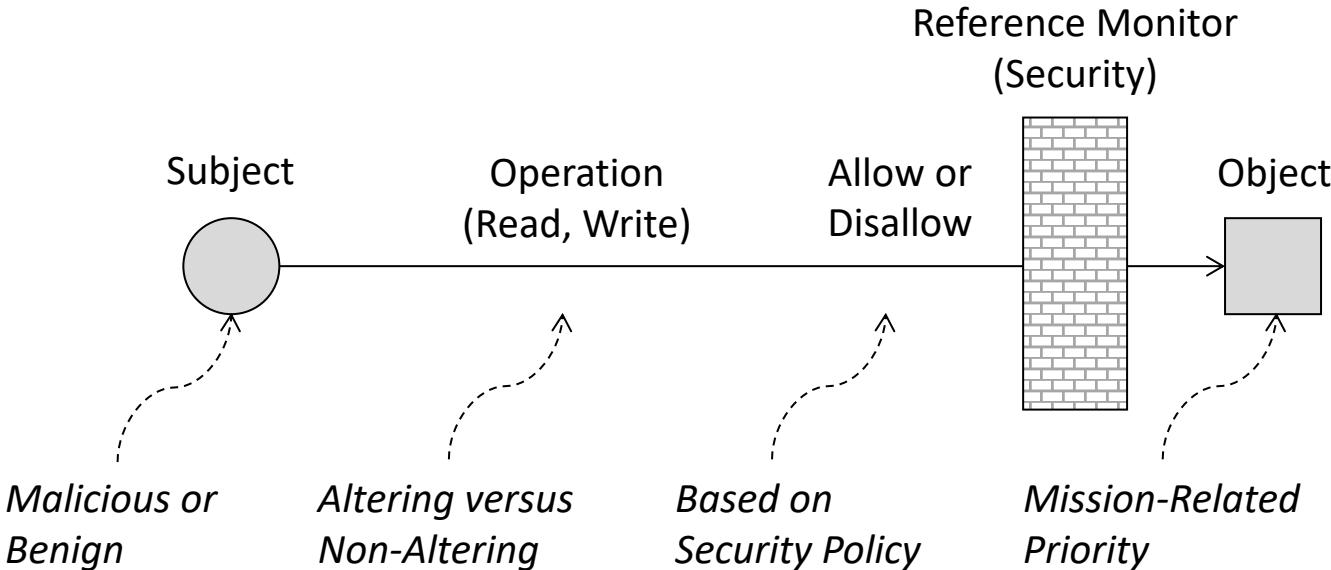
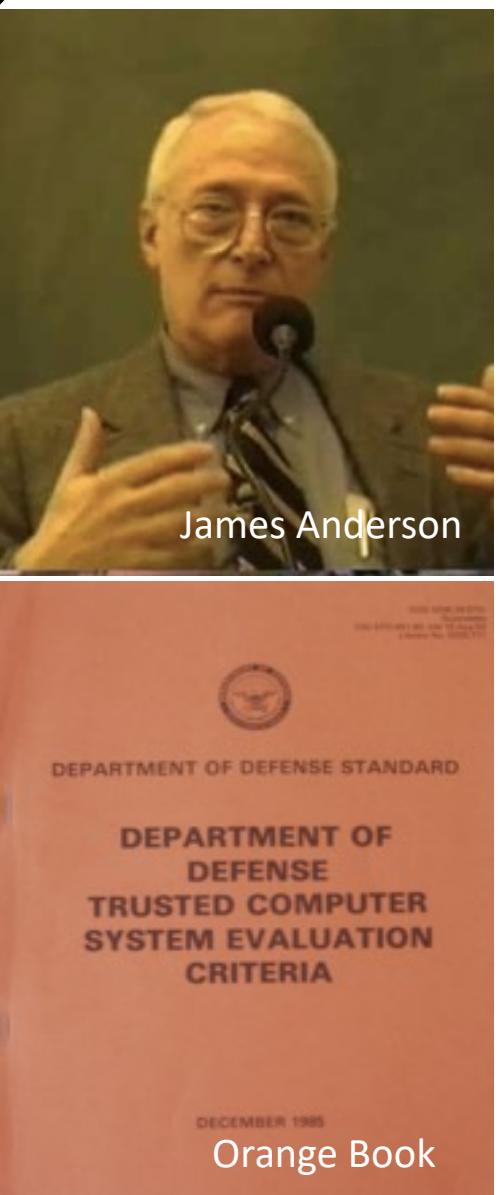
DOWNLOAD REPORT - 1ST QUARTER 2021

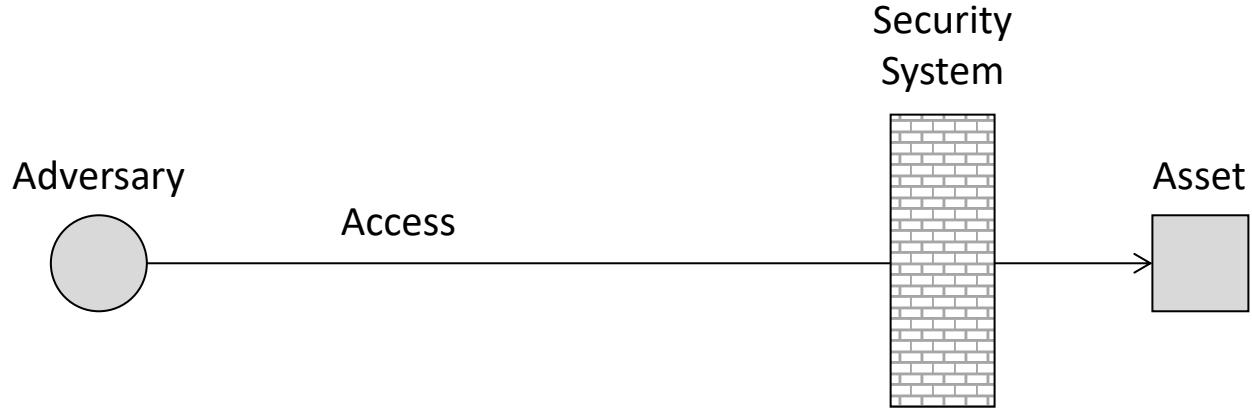
Required Additional Reading: <https://www.tag-cyber.com/advisory/quar>terly



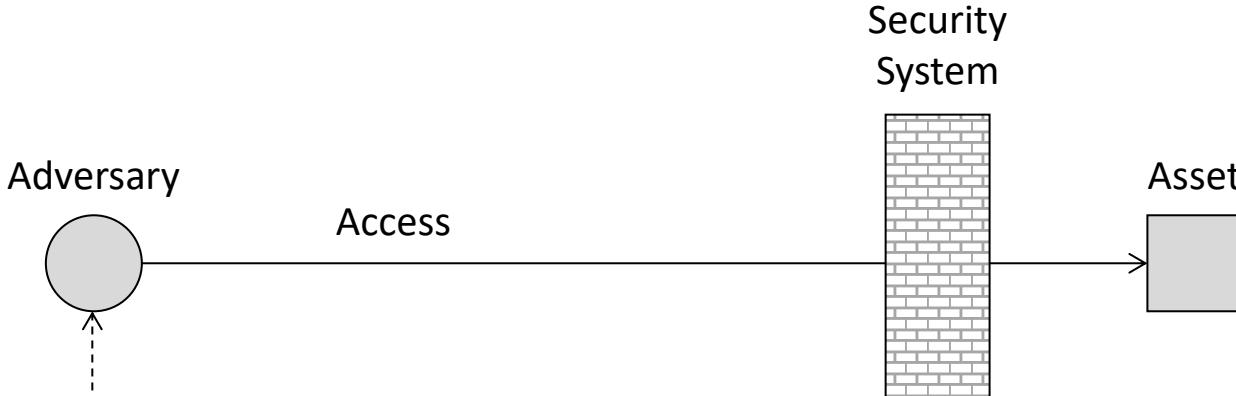
Week 4: Threat-Vulnerability Analysis

What are the Foundational Issues in Cyber Security?





Cyber Security: Basic Operational Framework



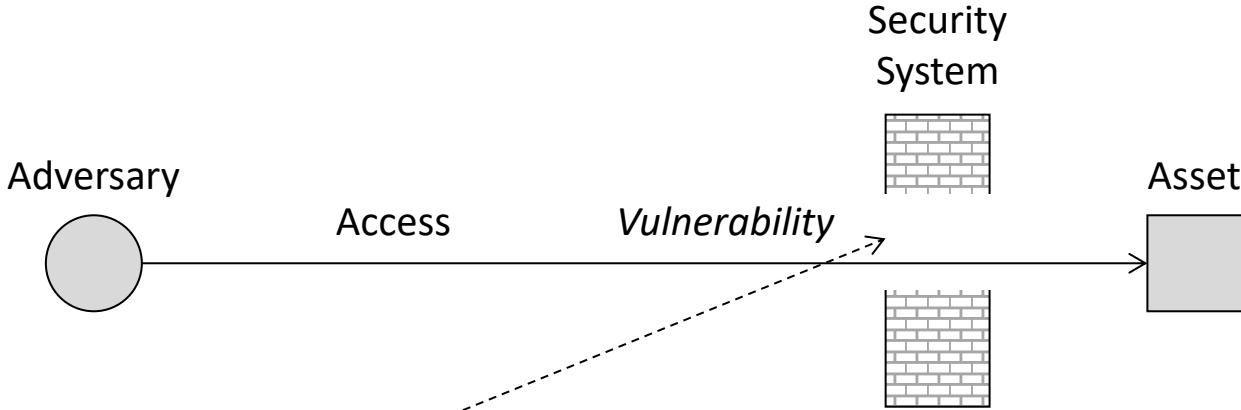
Incomplete
List

<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

Week 4





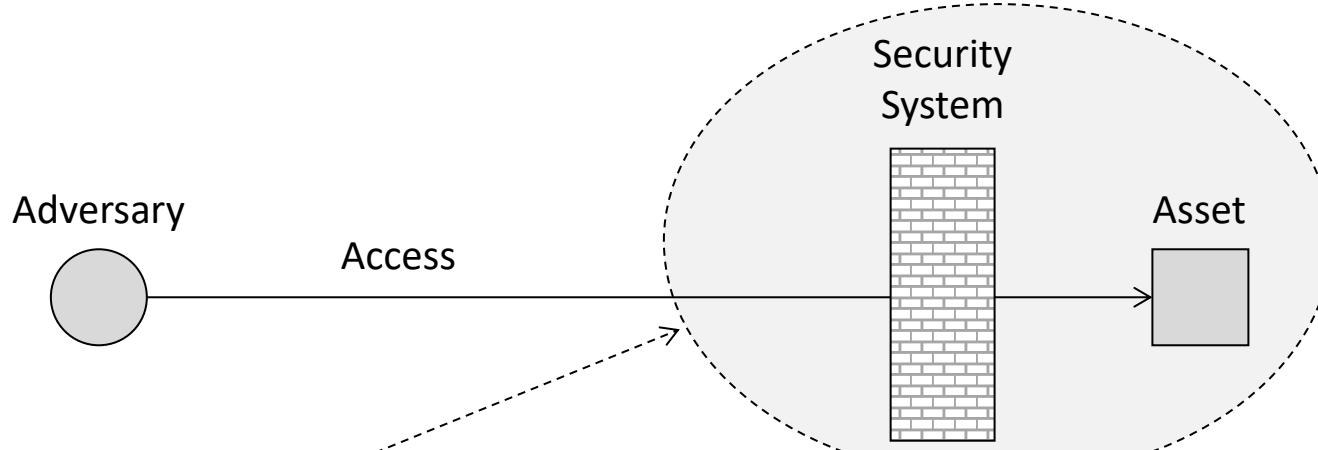
Incomplete
List

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

TOP 10 MOST EXPLOITED VULNERABILITIES FROM 2020

1. **CVE-2020-0796**: Windows SMBv3 Client/Server Remote Code Execution Vulnerability (codename: **SMBGhost**)
2. **CVE-2020-5902**: F5 Networks BIG-IP TMUI RCE vulnerability
3. **CVE-2020-1472**: Microsoft Netlogon Elevation of Privilege (codename: **Zerologon**)
4. **CVE-2020-0601**: Windows CryptoAPI Spoofing Vulnerability (codename: **CurveBall**)
5. **CVE-2020-14882**: Oracle WebLogic Server RCE
6. **CVE-2020-1938**: Apache Tomcat AJP File Read/Inclusion Vulnerability (codename: **GhostCat**)
7. **CVE-2020-3452**: Cisco ASA and Firepower Path Traversal Vulnerability
8. **CVE-2020-0688**: Microsoft Exchange Server Static Key Flaw Could Lead to Remote Code Execution
9. **CVE-2020-16898**: Windows TCP/IP Vulnerability (codename: **Bad Neighbor**)
10. **CVE-2020-1350**: Critical Windows DNS Server RCE (codename: **SIGRed**)



Complete List

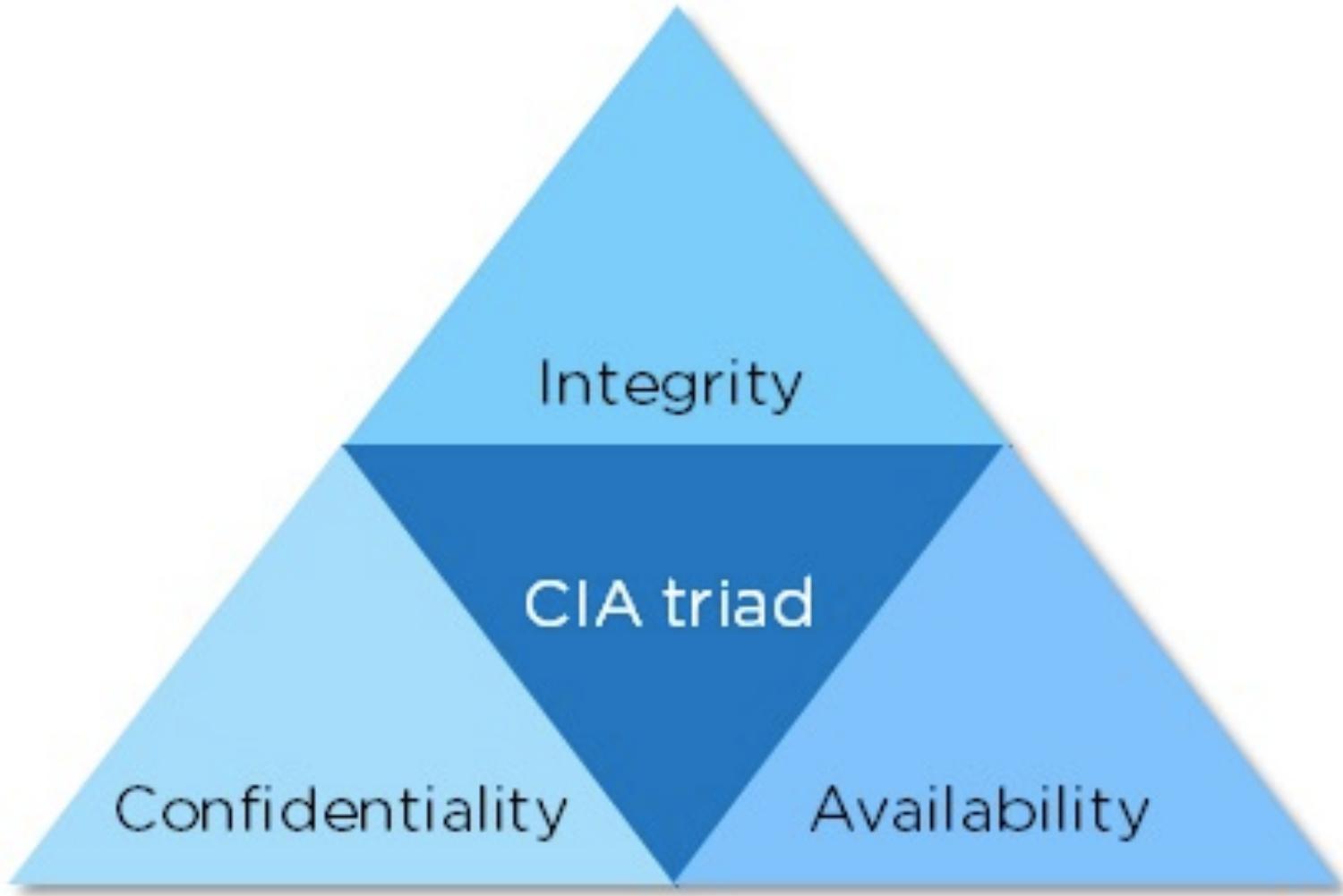
<i>Threat Type</i>	<i>Motivation</i>	<i>Defining Attributes</i>
Disclosure	Secrets	Personal and Business Information
Integrity	Degradation	Remote Operational Control/Change
Denial of Service	Disruption	Distributed Botnet Attacks Common
Theft/Fraud	Money/Goods	Ingenious and Clever Means for Theft

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.



TOP SECRET

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).



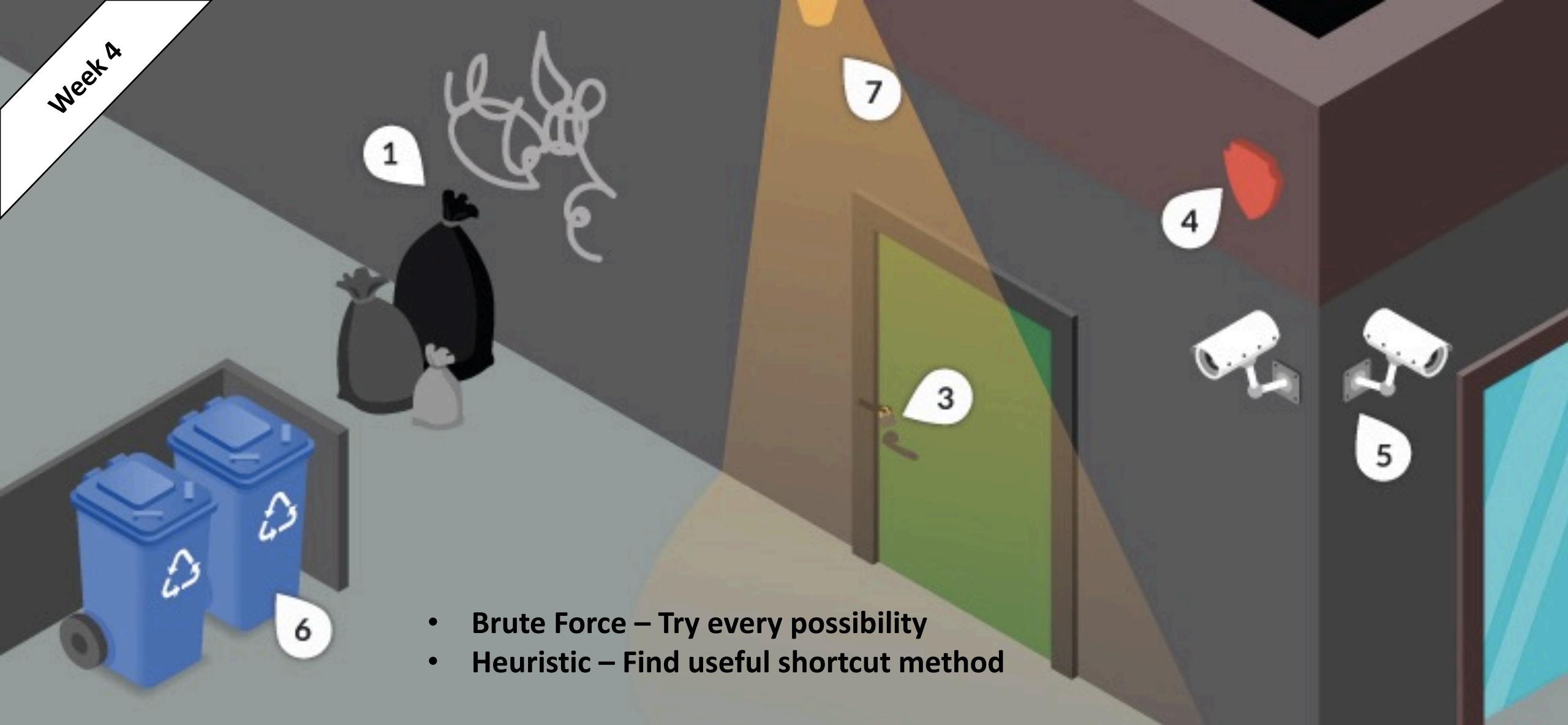
Def: Availability Threat – Asset maliciously blocked from authorized use.



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

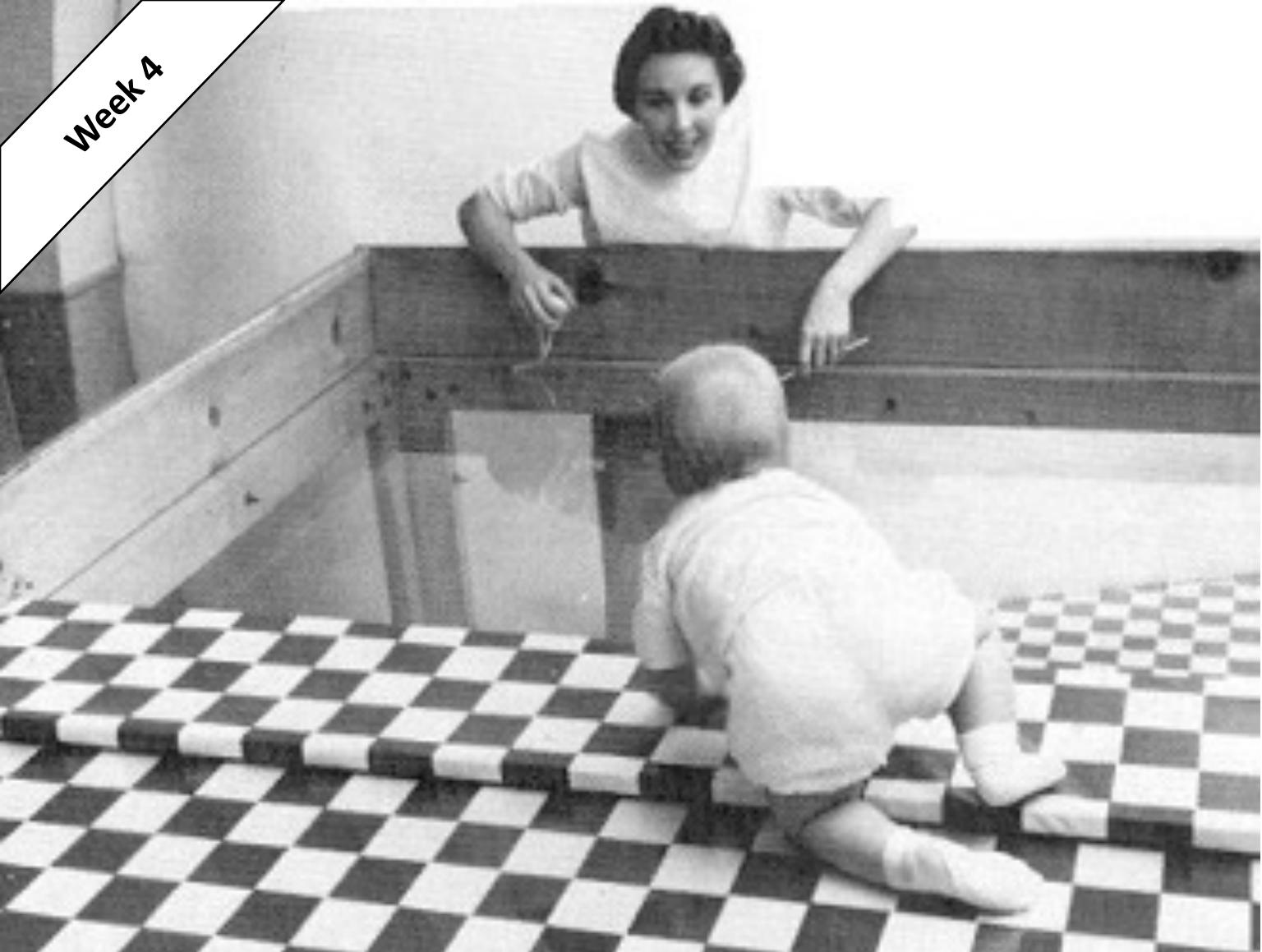


Def: Vulnerability – System bug or attribute that can be maliciously exploited.



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

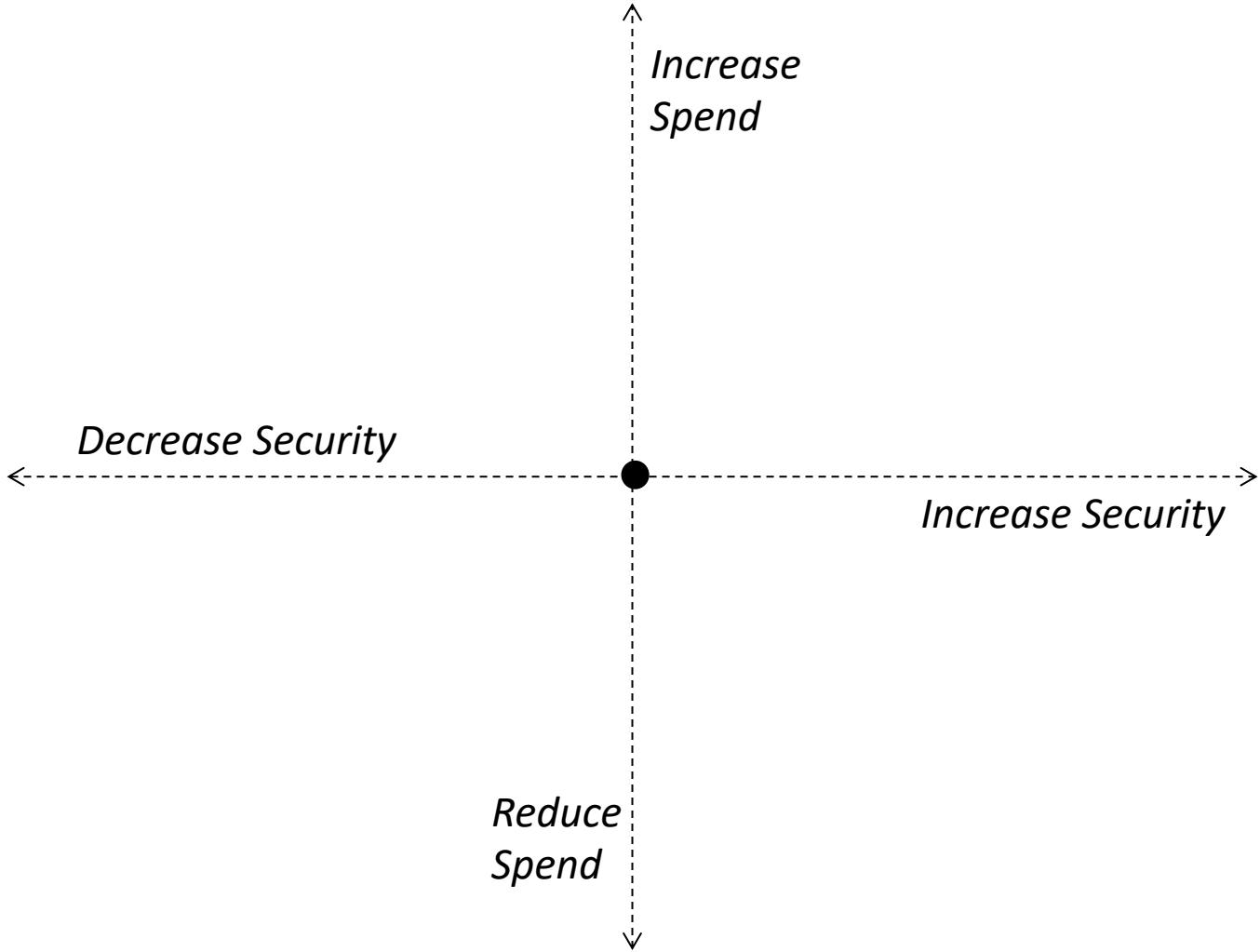
Def: Attack – Sequence of steps to exploit a vulnerability.



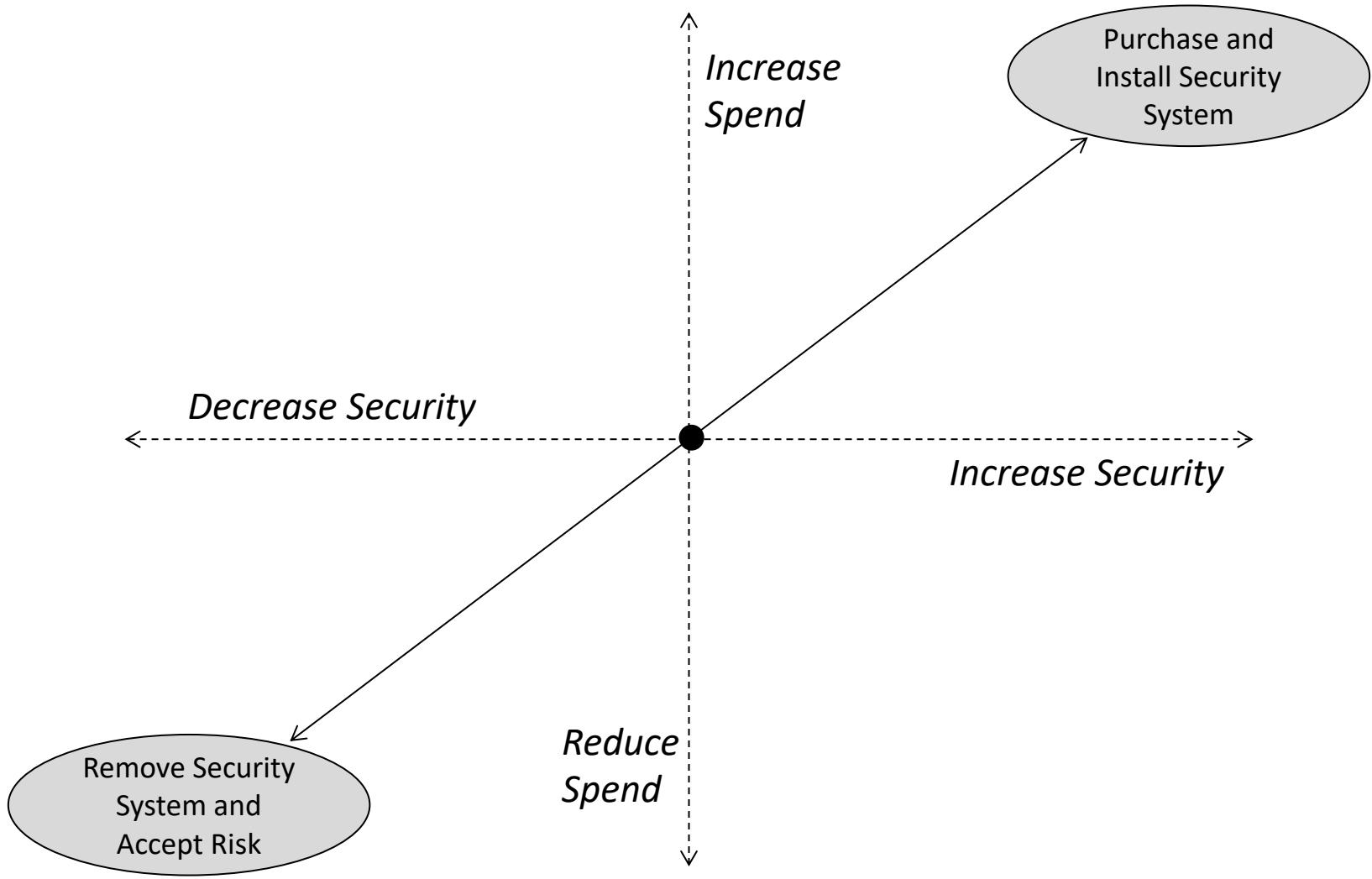
**Risk (R) equals
Probability (P) of Threat
times
Consequence (C) of Threat**

$$R = P * C$$

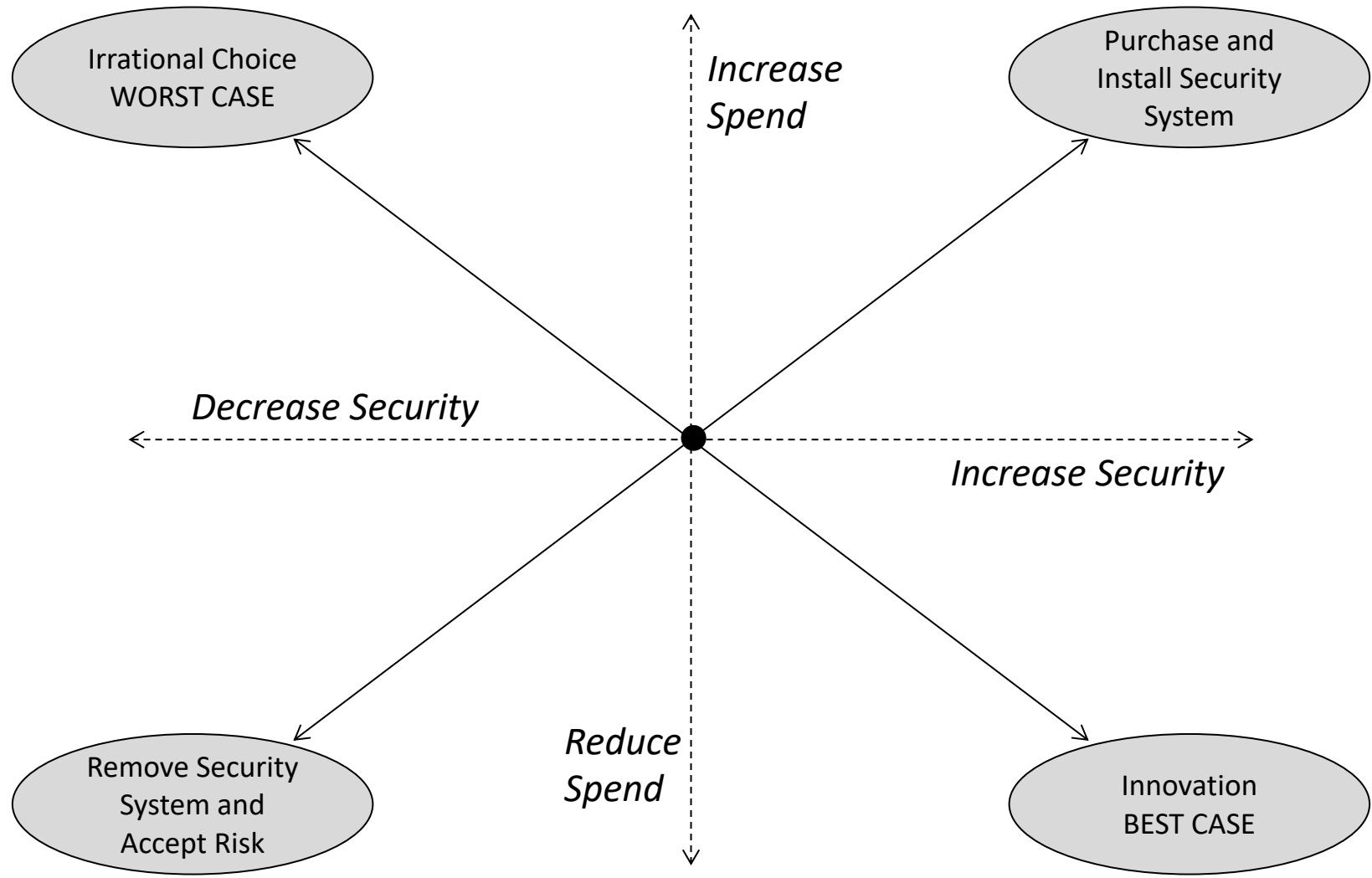
Def: Risk – Probability “Times” Consequence



Security Risk Assessment – Decision Framework



Security Risk Assessment – Decision Framework



Security Risk Assessment – Decision Framework



FAIR Model – Security Risk Assessment

How Are Assets Prioritized?

Week 4



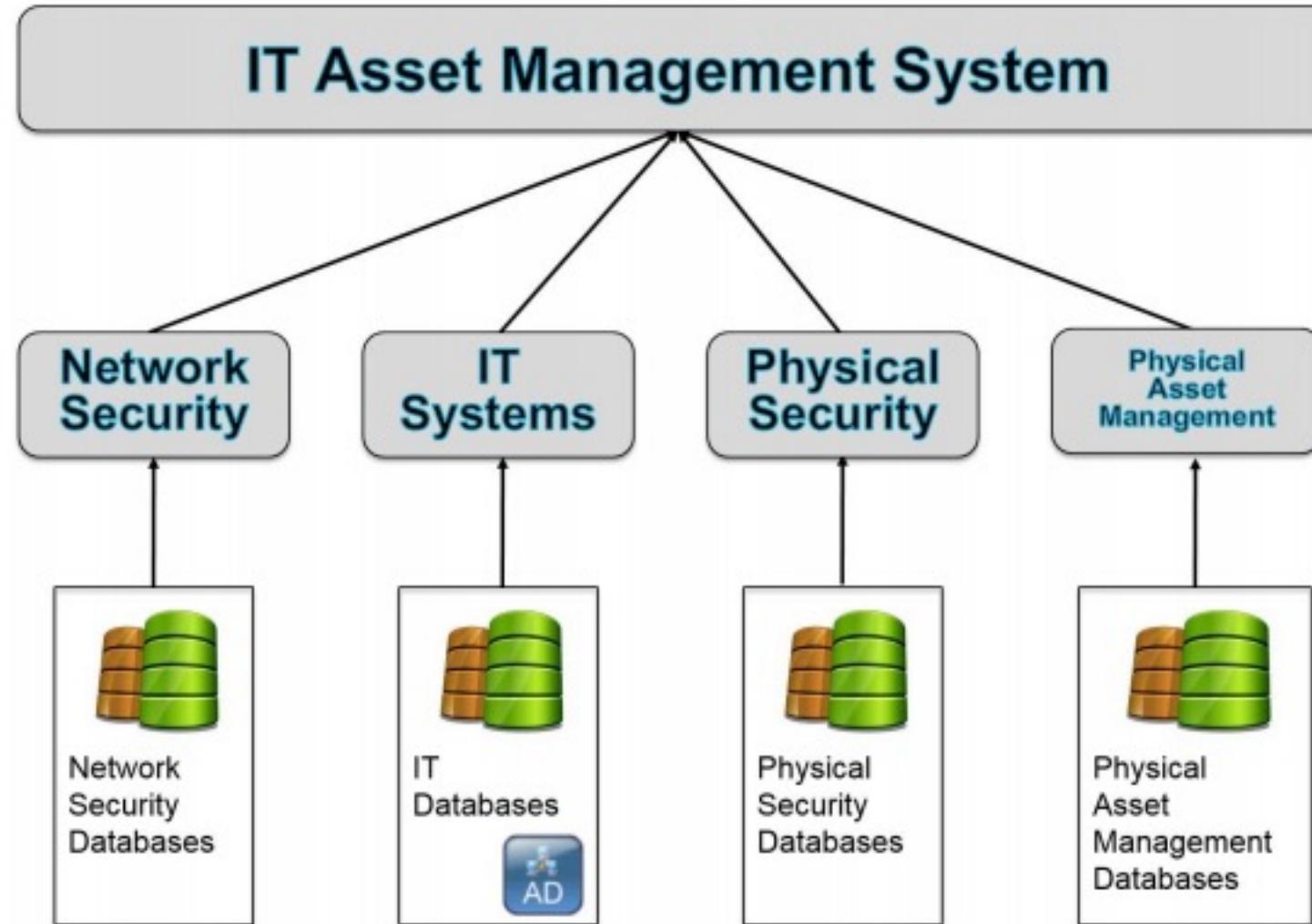
#abc7eyewitness

Illustrating Tiered Prioritization of Assets

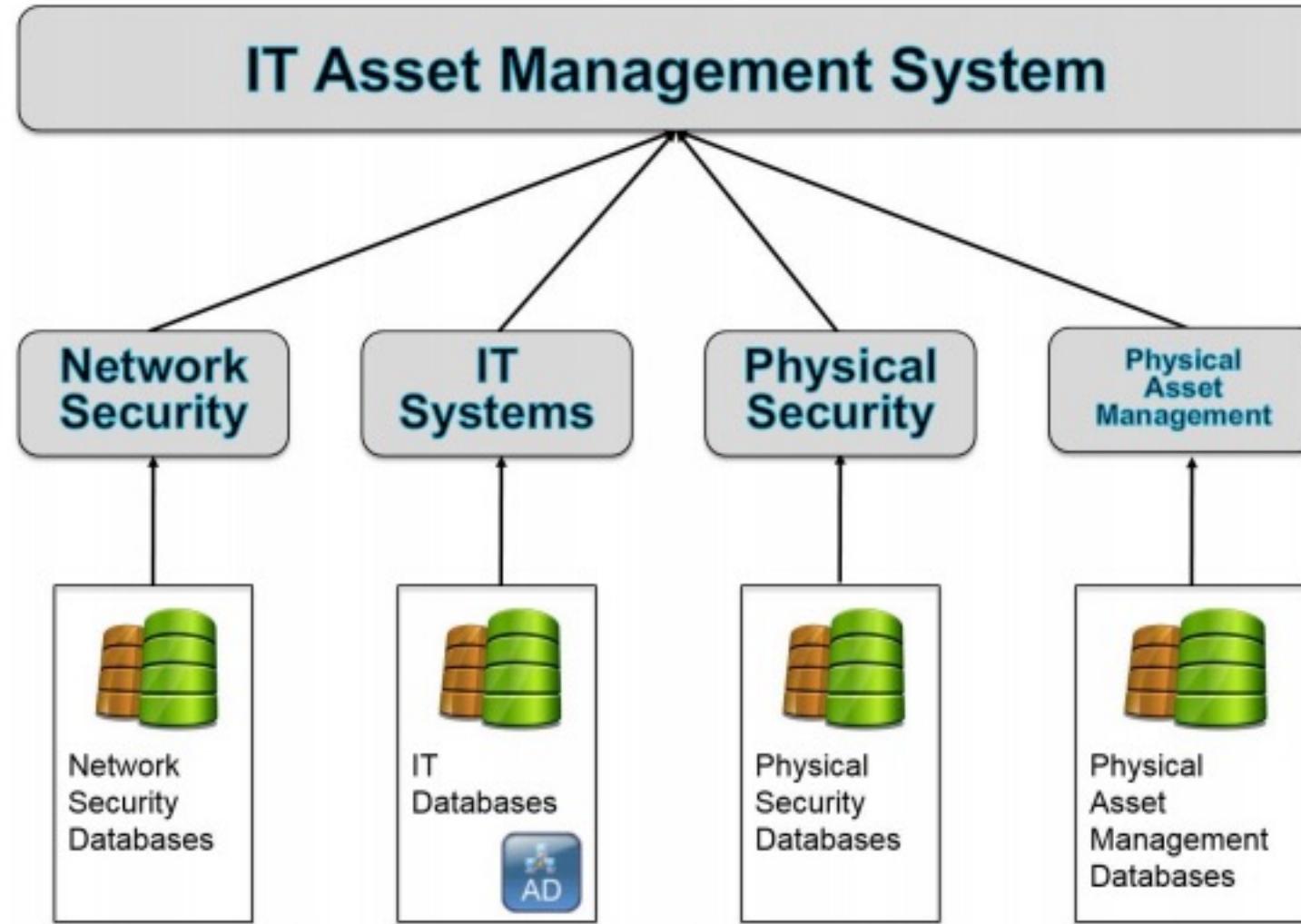


Illustrating Tiered Prioritization of Assets

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



NIST IT Asset Management System Model



NIST IT Asset Management System Model

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

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



Attack tree

From Wikipedia, the free encyclopedia



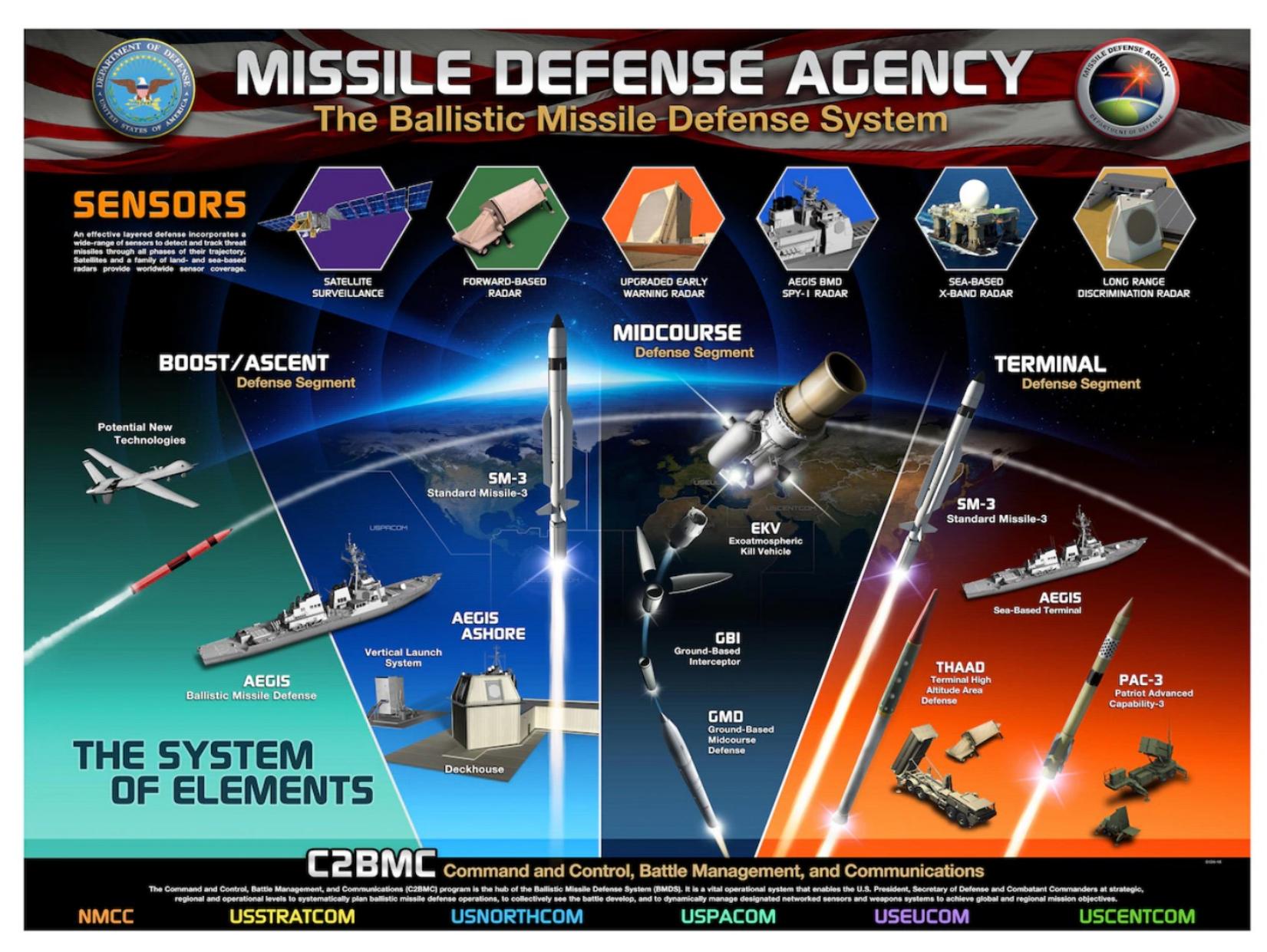
This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.

Find sources: "Attack tree" – news · newspapers · books · scholar · JSTOR (April 2012) (Learn how and when to remove this template message)

Attack trees are conceptual diagrams showing how an asset, or target, might be attacked. Attack trees have been used in a variety of applications. In the field of information technology, they have been used to describe [threats on computer systems](#) and possible [attacks](#) to realize those threats. However, their use is not restricted to the analysis of conventional information systems. They are widely used in the fields of defense and aerospace for the analysis of threats against tamper resistant electronics systems (e.g., avionics on military aircraft).^[1] Attack trees are increasingly being applied to computer control systems (especially relating to the electric [power grid](#)).^[2] Attack trees have also been used to understand threats to physical systems.

Some of the earliest descriptions of attack trees are found in papers and articles by [Bruce Schneier](#),^[3] when he was [CTO of Counterpane Internet Security](#). Schneier was clearly involved in the development of attack tree concepts and was instrumental in publicizing them. However, the attributions in some of the early publicly available papers on attack trees^[4] also suggest the involvement of the [National Security Agency](#) in the initial development.

Attack trees are very similar, if not identical, to *threat trees*. Threat trees were discussed in 1994 by Edward Amoroso.^[5]



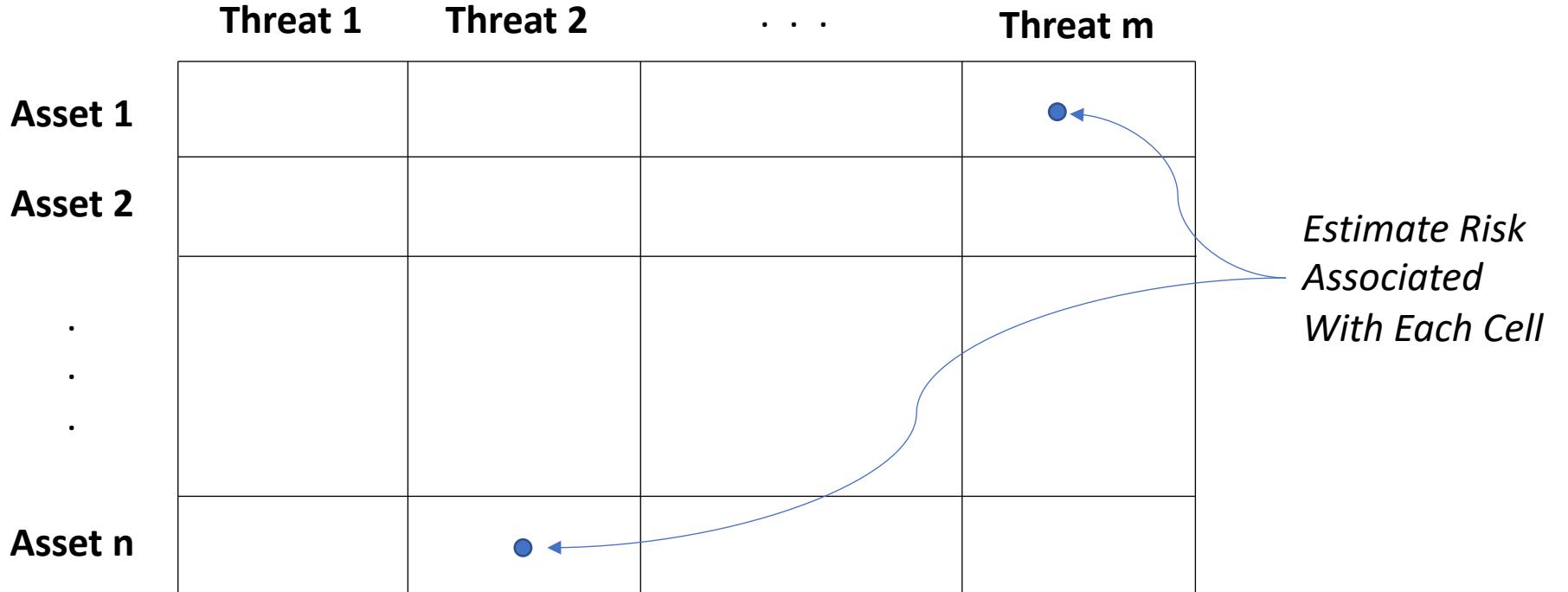
	Threat 1	Threat 2	...	Threat m	<i>List the threats (Probably CIA)</i>
Asset 1					
Asset 2					
.					
.					
.					
Asset n					
<i>List the assets (Based on mission)</i>					

Developing a Threat-Asset Matrix

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

*Create $(m \times n)$ 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

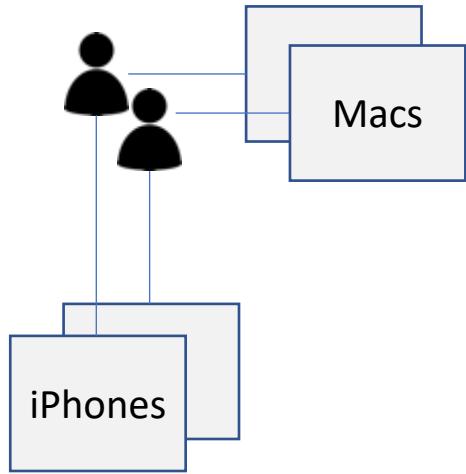
	Confidentiality	Integrity	Availability
Hardware	P = 3, 2, 1 C = 3, 2, 1 R = P * C	P = 3, 2, 1 C = 3, 2, 1 R = P * C	P = 3, 2, 1 C = 3, 2, 1 R = P * C
Software	P = 3, 2, 1 C = 3, 2, 1 R = P * C	P = 3, 2, 1 C = 3, 2, 1 R = P * C	P = 3, 2, 1 C = 3, 2, 1 R = P * C
Information	P = 3, 2, 1 C = 3, 2, 1 R =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

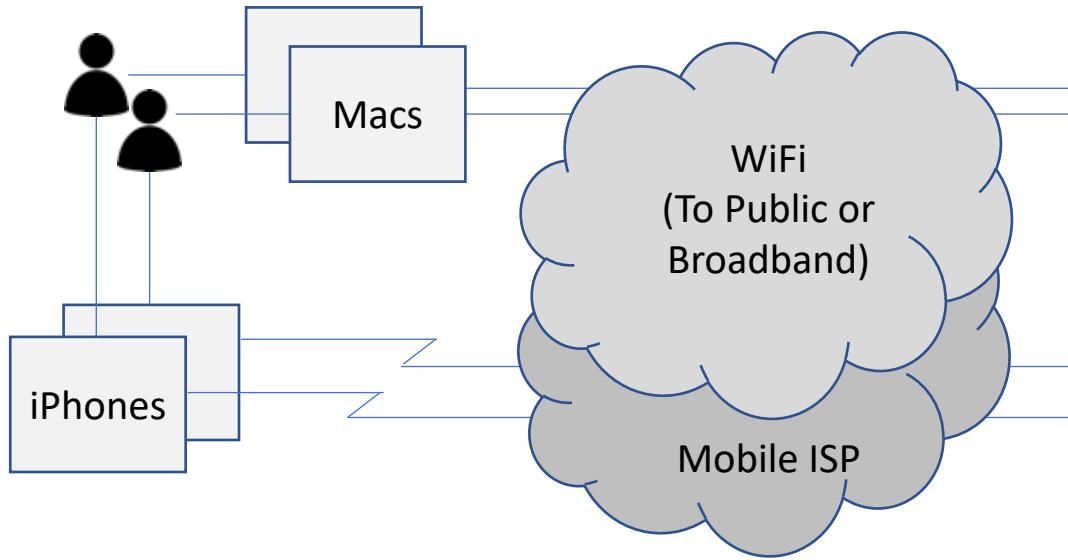
Developing a Threat-Asset Matrix

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

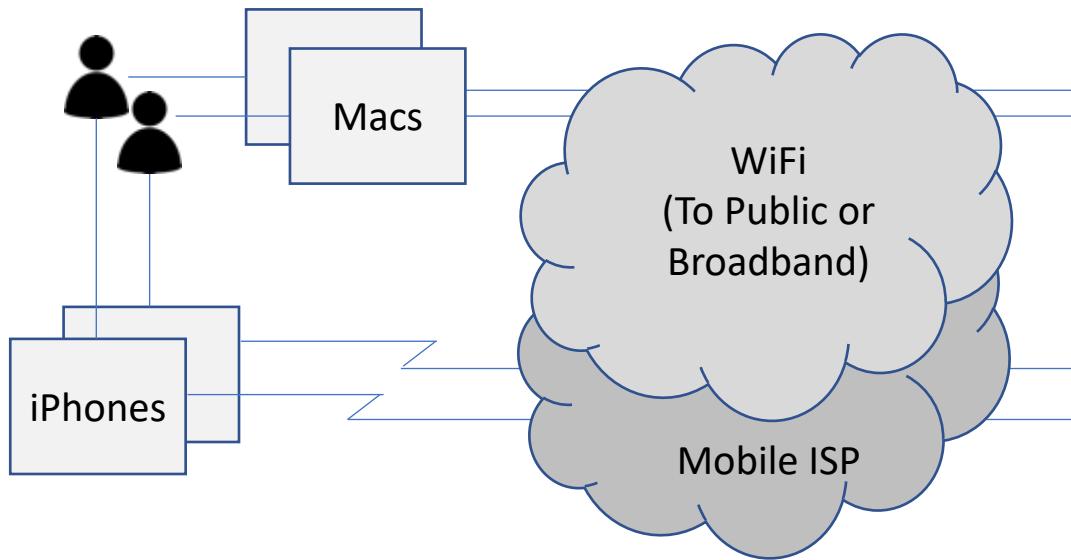
Week 4



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

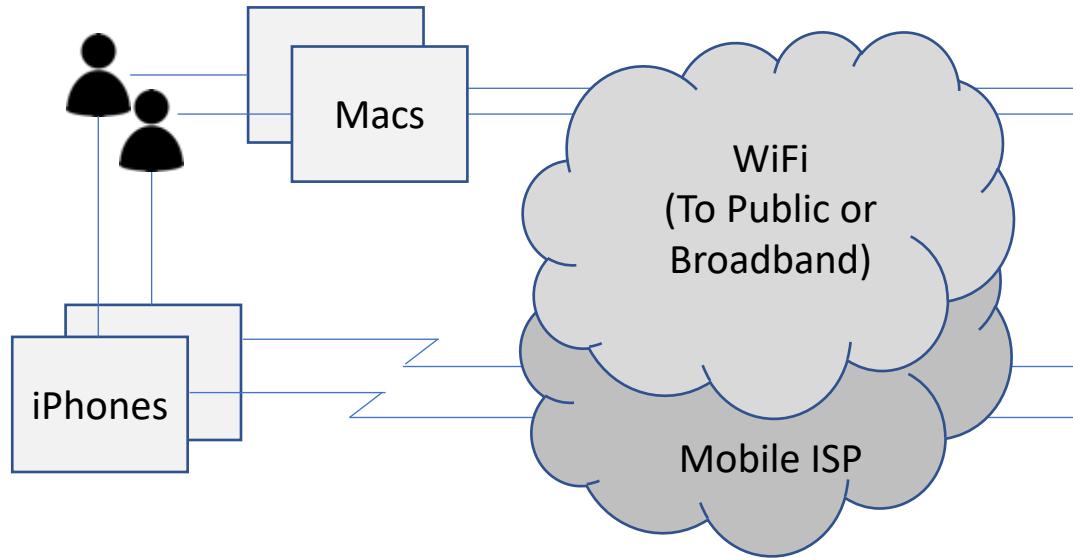


Case Study: Manage and Secure Assets for ACME Software-R-Us Inc.



Internet-Based
Cloud-Hosted
Services

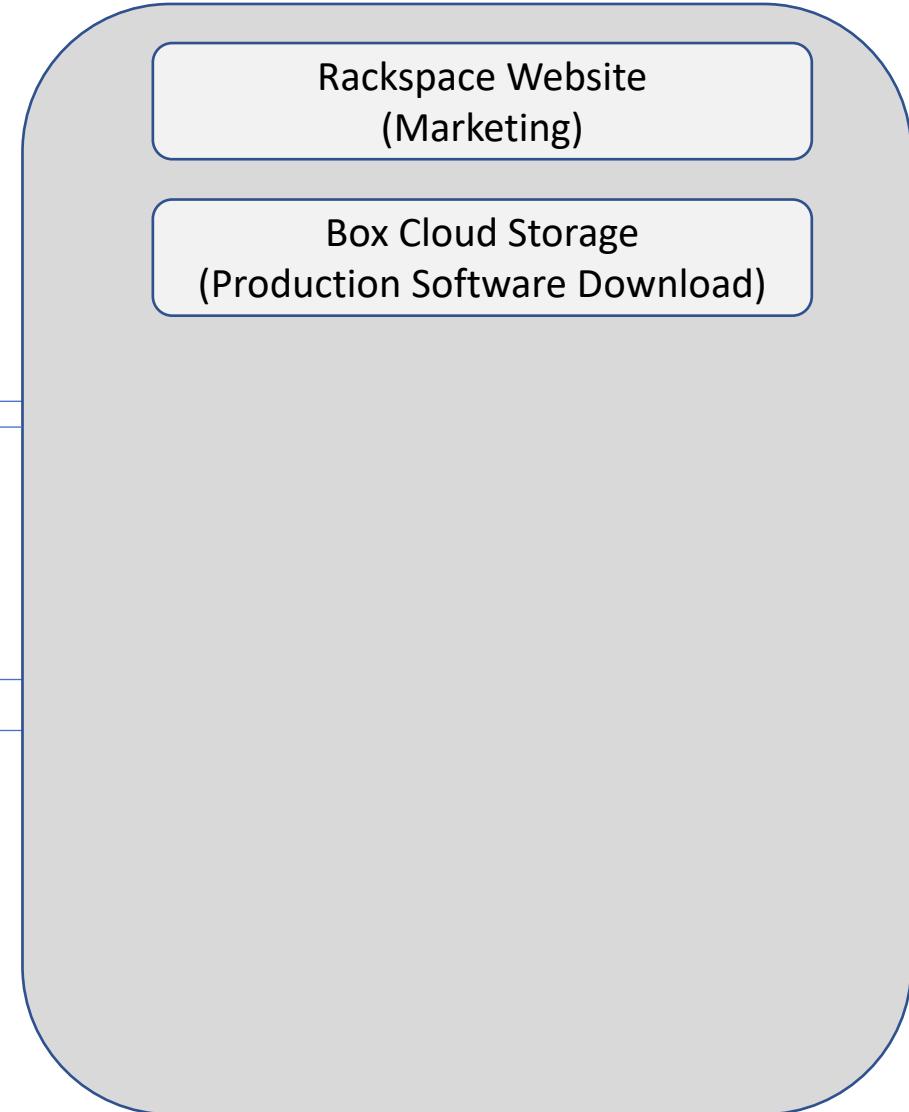
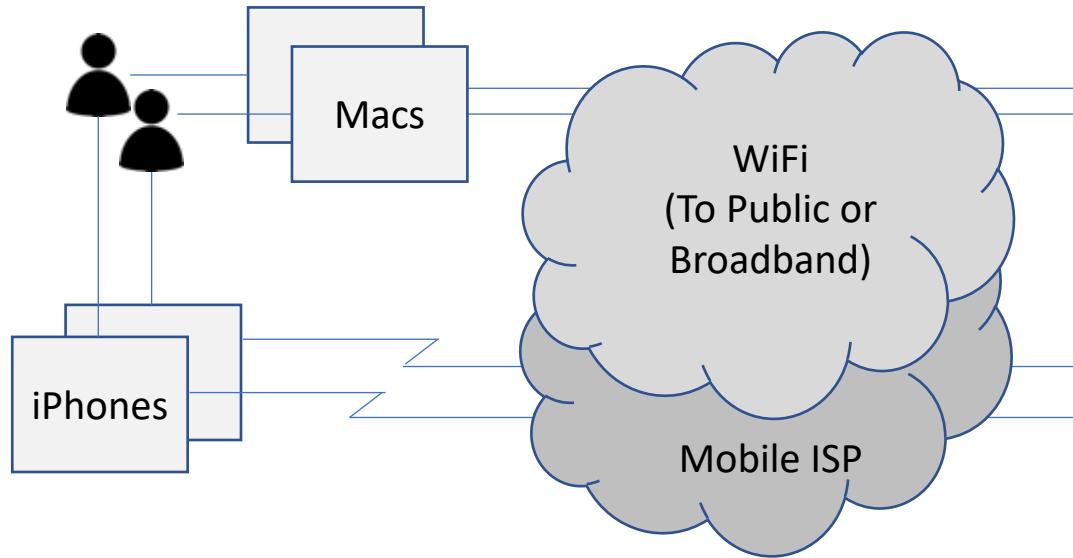
Case Study: Manage and Secure Assets for ACME Software-R-Us Inc.



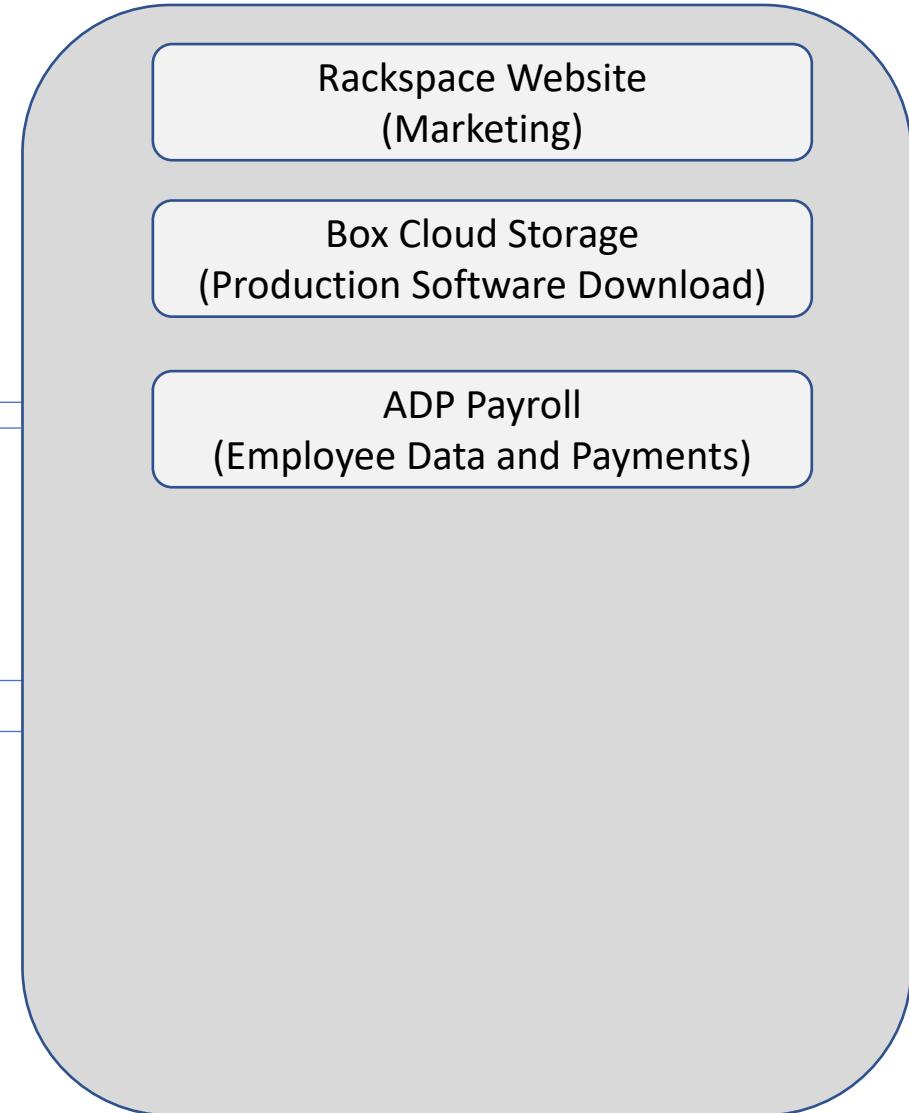
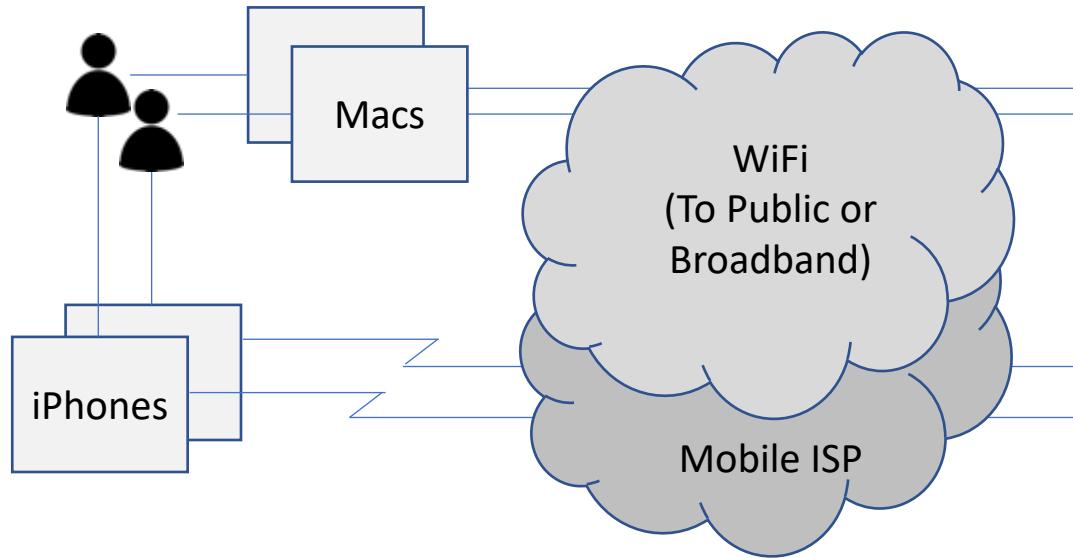
Rackspace Website
(Marketing)

Internet-Based
Cloud-Hosted
Services

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

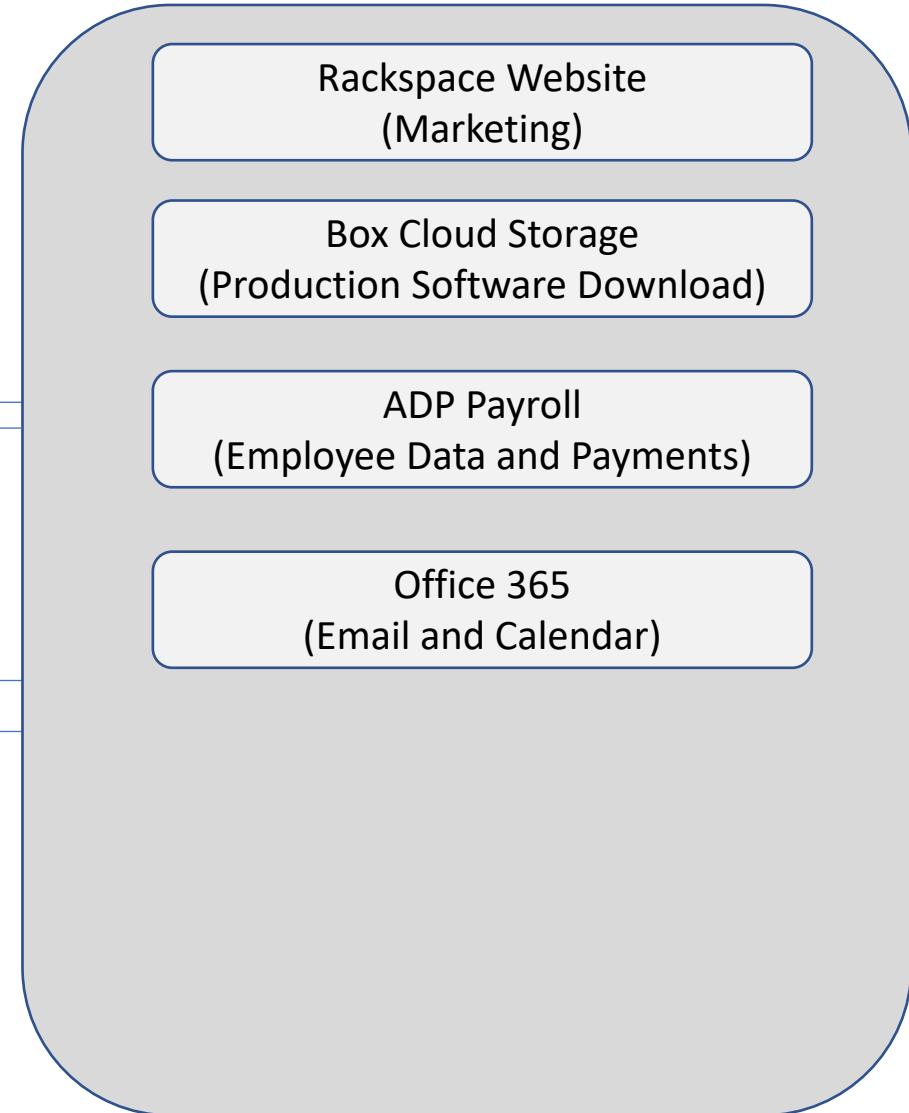
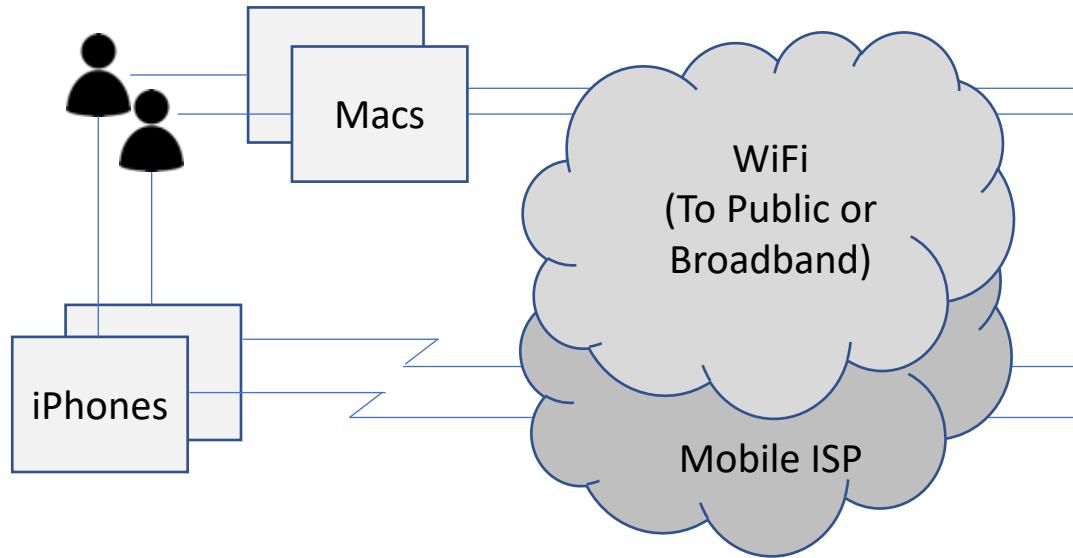


Case Study: Manage and Secure Assets for ACME Software-R-Us Inc.

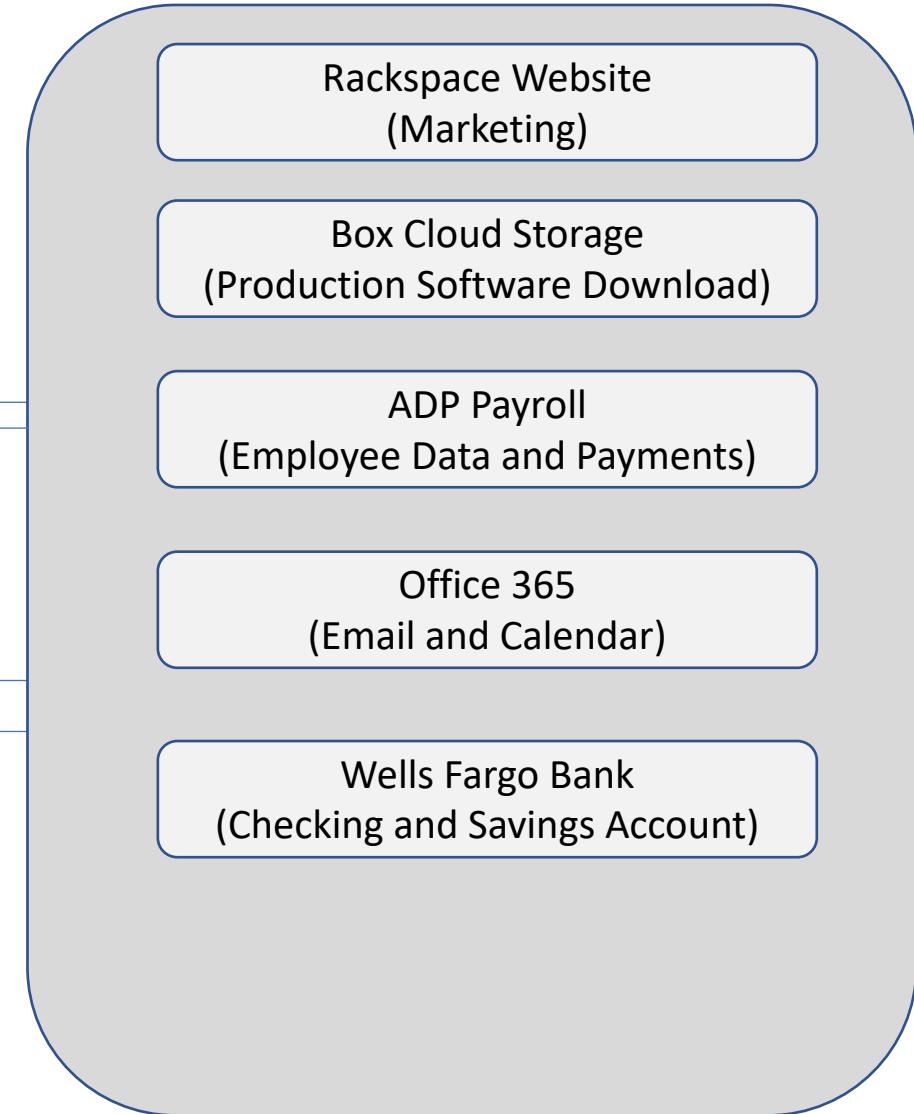
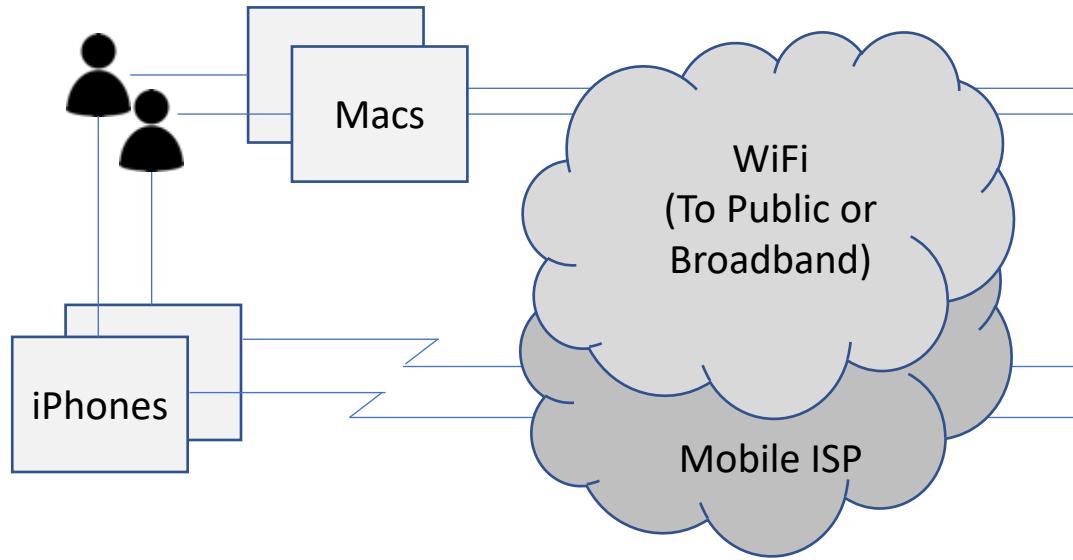


Internet-Based
Cloud-Hosted
Services

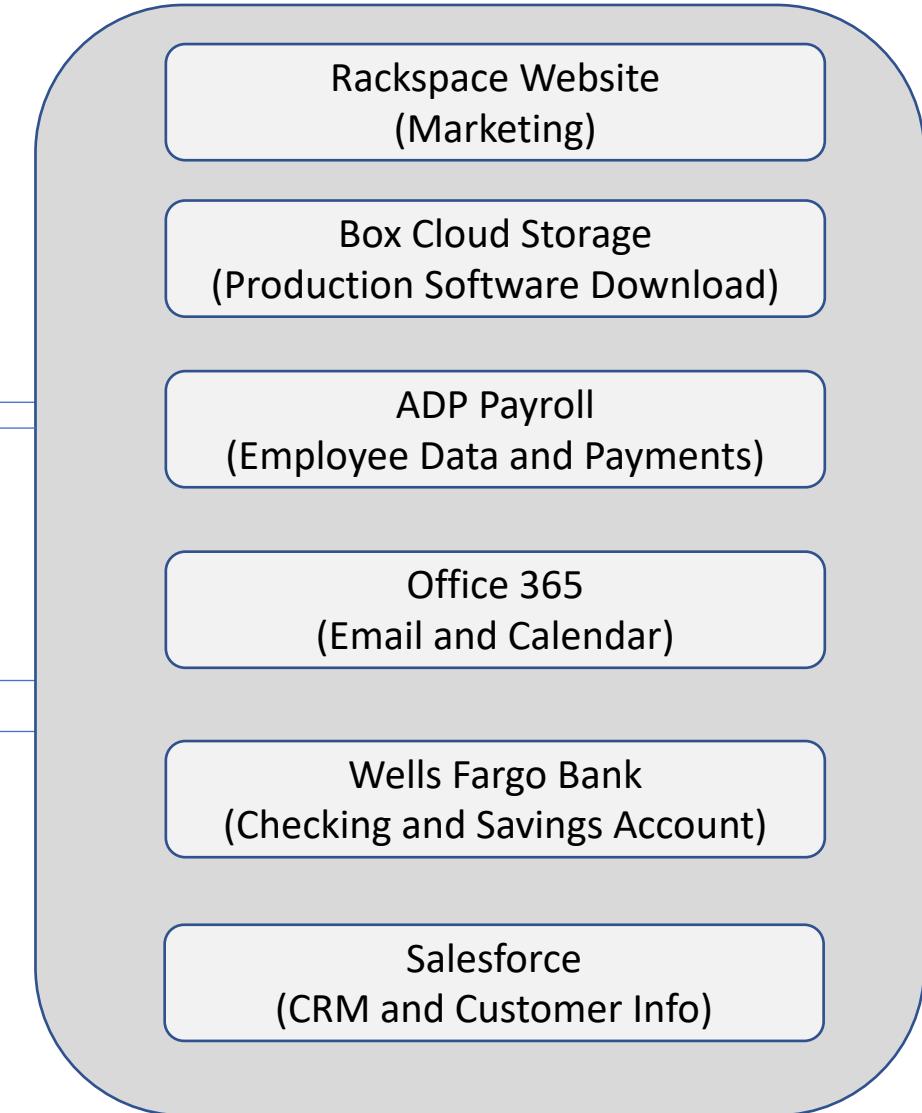
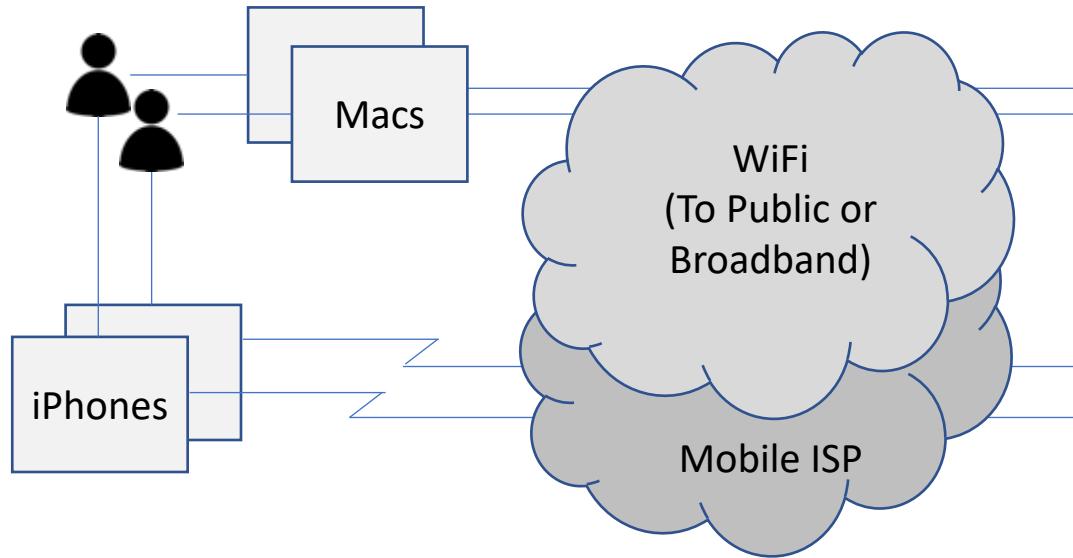
Case Study: Manage and Secure Assets for ACME Software-R-Us Inc.



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



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



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

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

Developer MACs (Software, etc.)

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

Developer MACs (Software, etc.)

Developer iPhones (Email, Photos, etc.)

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

Developer MACs (Software, etc.)

Developer iPhones (Email, Photos, etc.)

Rackspace Website (Papers, PDFs, etc.)

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)

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.)

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.)

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)

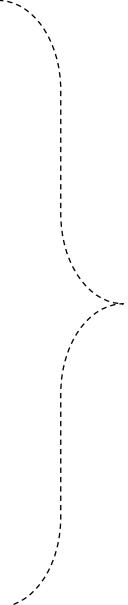
ADP Payroll (Employee PII, etc.)

Office 365 (Email, Calendars, etc.)

Wells Fargo Bank (Checking Acct, etc.)

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.)



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: $P = 2, C = 3, R = 6$

	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.

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.

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.

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.

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.

	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 st Highest Risk Asset
Salesforce (CRM, Customer Data, etc.)	Total Risk = 17 – 2 nd Highest Risk Asset
Developer MACs (Software, etc.)	Total Risk = 16 – 3 rd Highest Risk Asset
Office 365 (Email, Calendars, etc.)	Total Risk = 16 – 3 rd Highest Risk Asset
Rackspace Website (Papers, PDFs, etc.)	Total Risk = 11 – 4 th 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 Your 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 March 7th