Week 4

2021 TAG CYBER SECURITY ANNUAL

ME TO BREAK UP THE RSA CONFERENCE

The RSA Conference has devolved into a routine event for mid-lifers with booth-after-booth-after-booth of the same-old, same-old.

should then create five new program committees with no member over twenty-nine and at least two-thirds women. These five new committees should then caucus over beers outside Whisler's to reinvent five crazy-interesting conferences with themes that are meaningful and edgy. They should push the envelope.

Then the PCs should reinvent how these five new S-curves are physically held. It could be something cool like those crowdsourced, simulcast, conference-BNB things. Maybe it could involve using the headquarters of security companies from around the world. Instead of having physical booths at Moscone, vendors could host concurrent RSAC three-day parties for anyone who chooses to come to their venue. Or whatever. It would be fun.

Look – I know this would be a jolt, but if RSAC continues on its present path, then here is my prediction: Within three years, the RSA Conference will book less than 20K paid attendees, and it will start to lose its grip on the vendor community. Perhaps worse, the current show is really turning into a BoomerCon. Just like Spot the Fed at DEFCON, RSAC could initiate a Spot the Non-Boomer contest. It would be quite a challenge.

By the way, Black Hat is the new RSA Conference. Just look at this sponsorship page for a conference that started as anti-establishment. Rich Powell and I developed a cartoon to lampoon this inevitable transition. You see, Black Hat is riding up the middle of its S-Curve. It is still somewhat edgy, and still somewhat relevant. In a few years, I'll probably be whining that they please stop kicking their conference can down the road.

Oh – and there's this: RSAC 2020 attendance looked to our TAG Cyber team to be about 50% down. This had nothing to do with the conference and everything to do with the virus. But it is precisely such random events that can trigger a downfall. Some security vendor or enterprise team might notice, for example, that the earth continues to rotate despite not having been at RSAC. This leads to a decision next year to maybe … well, you get the idea.

I believe that breaking up RSAC into five new conferences is good business for the owners and healthy for our industry. Even the venerable AT&T, where I spent most of my adult life, thrived mightily post-divestiture despite decades of fighting the courts. If RSAC ownership wants to protect its investment, then they will listen to my advice. If they don't – well, at least RSAC 2025 will be easier to navigate, because no one will be there.

I hope they listen.

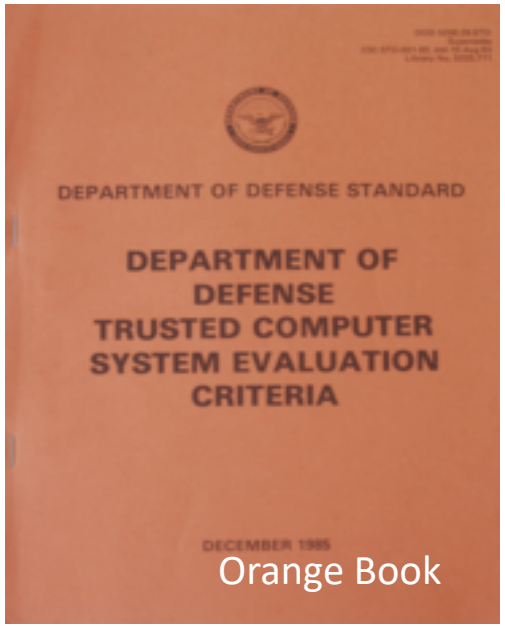
2021 SECURITY ANNUAL 49 TAG CYBER

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

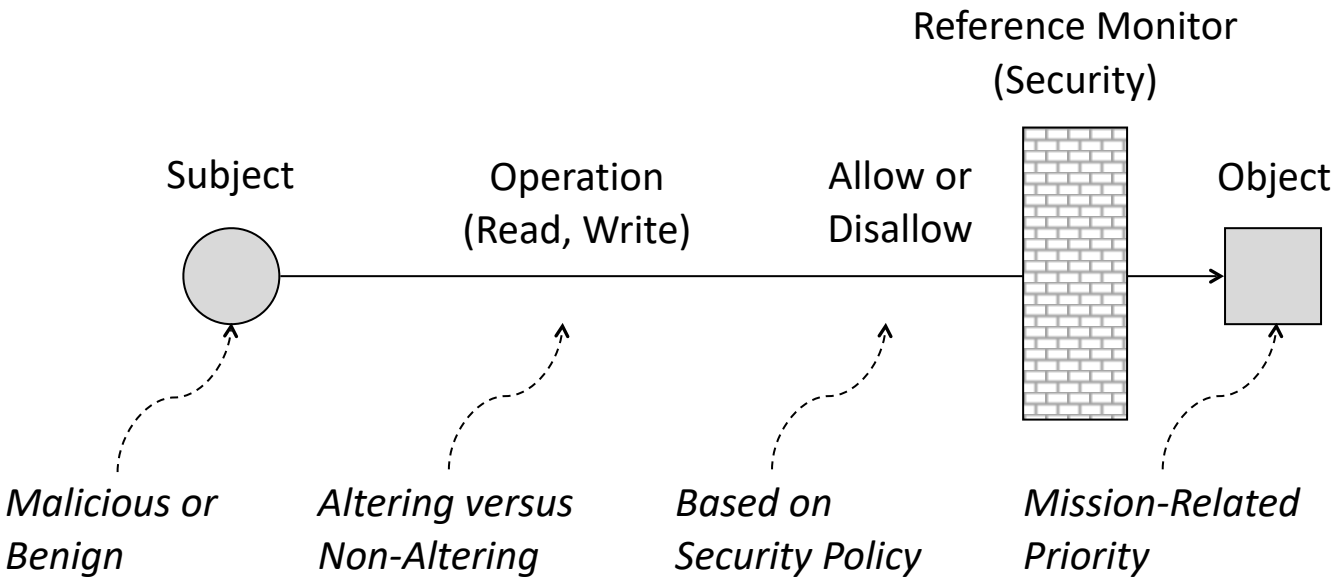
Week 4: Threat-Vulnerability Analysis

Week 4


James Anderson

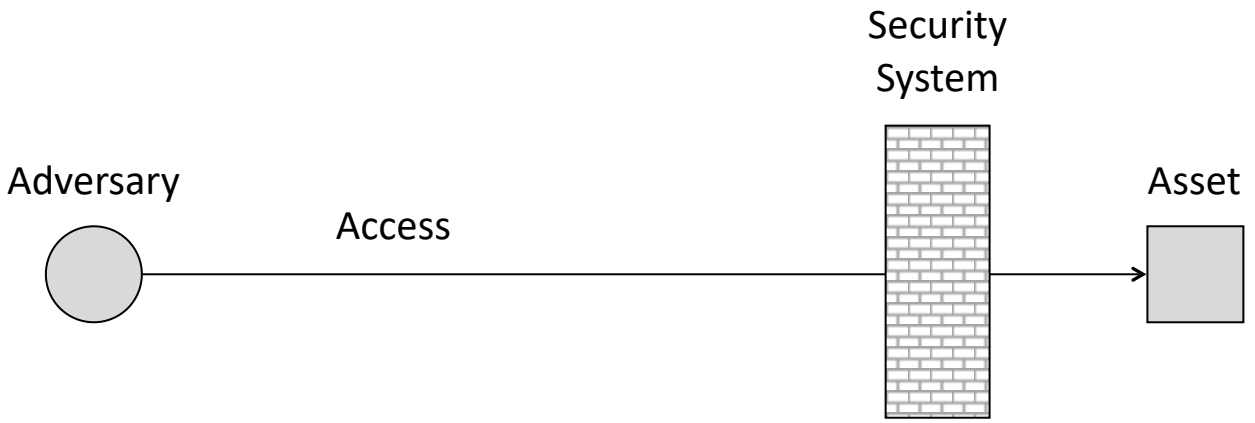


Orange Book



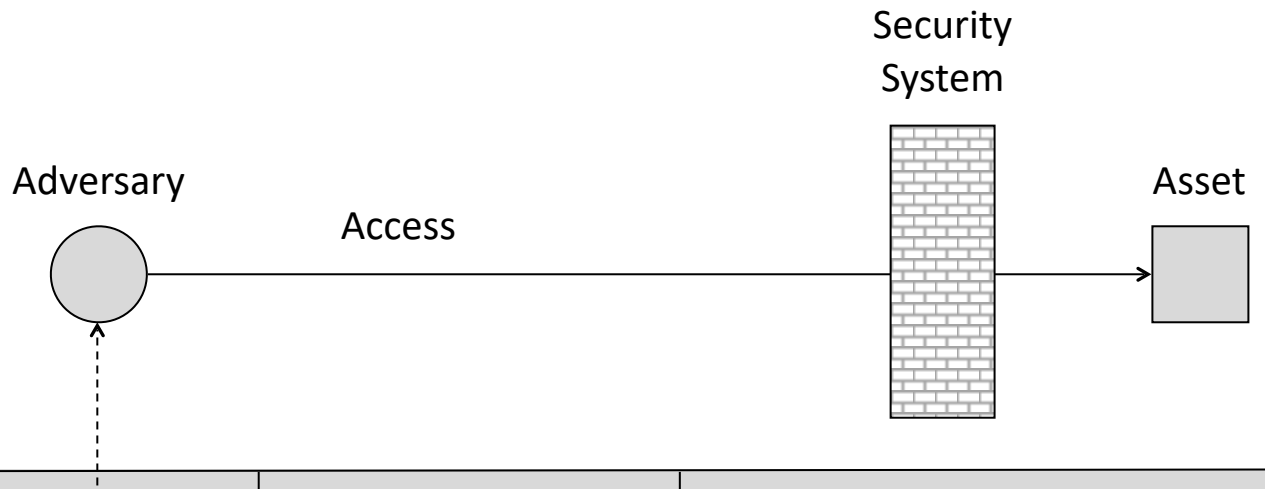
Cyber Security: Subject-Object Reference Model

Week 4



Cyber Security: Basic Operational Framework

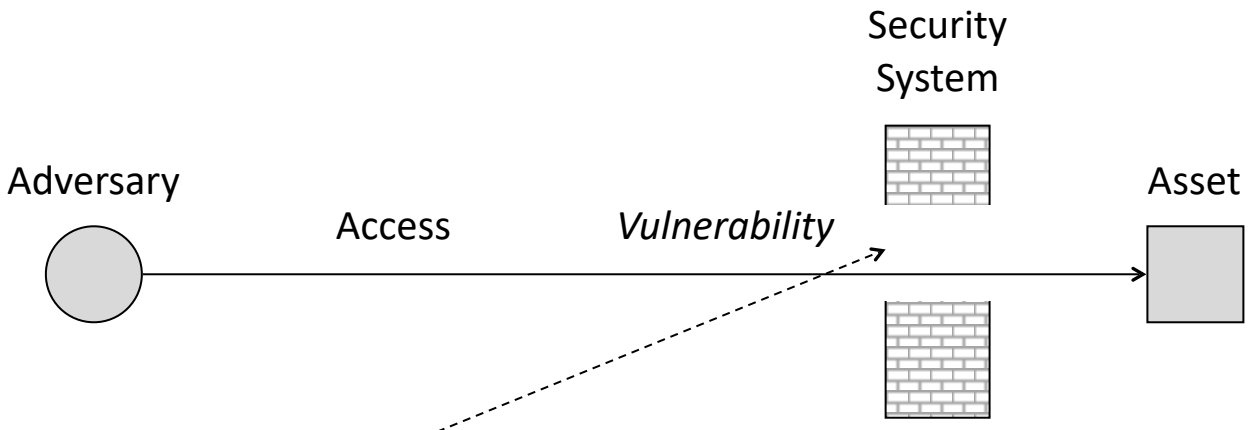
Week 4



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

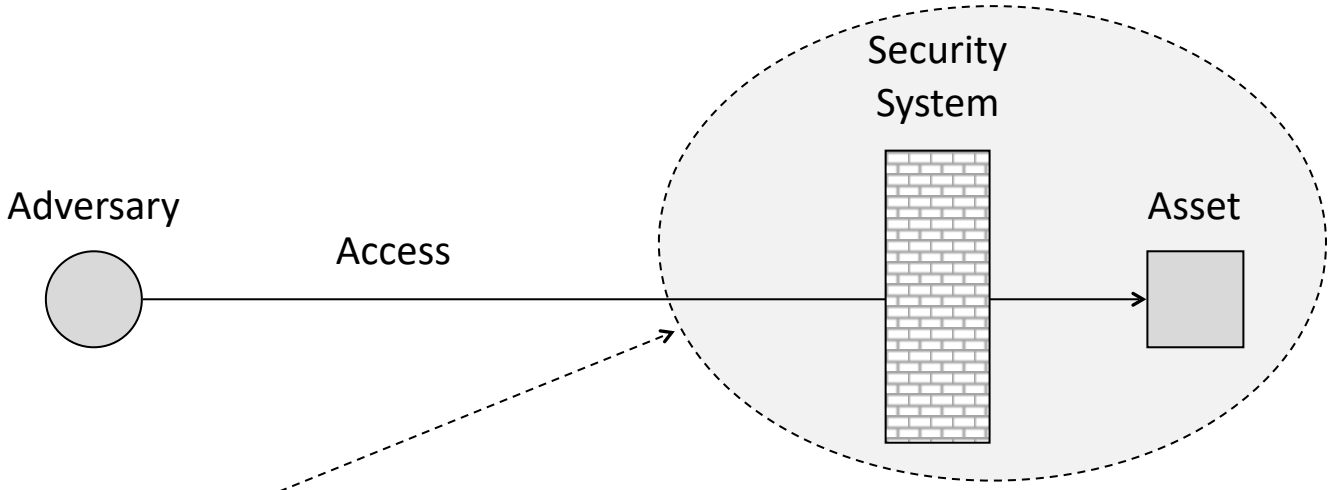
Week 4



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



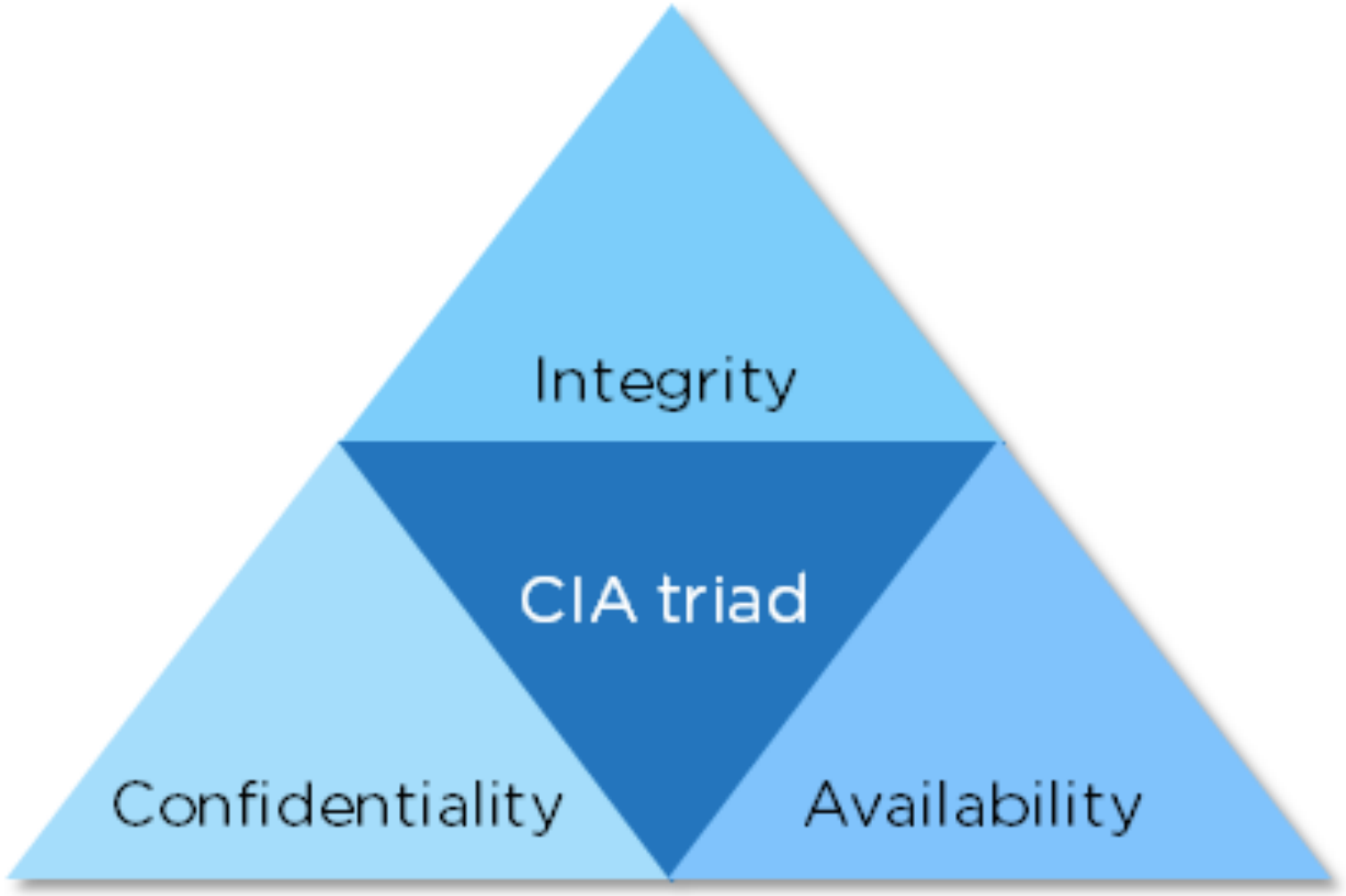
Threat Type	*Motivation*	*Defining Attributes*
Disclosure	Secrets	Personal and Business Information
Integrity	Degradation	Remote Operational Control/Change
Denial of Service	Disruption	Distributed Botnet Attacks Common
Theft/Fraud	Money/Goods	Ingenious and Clever Means for Theft

Cyber Security: Threat Types

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

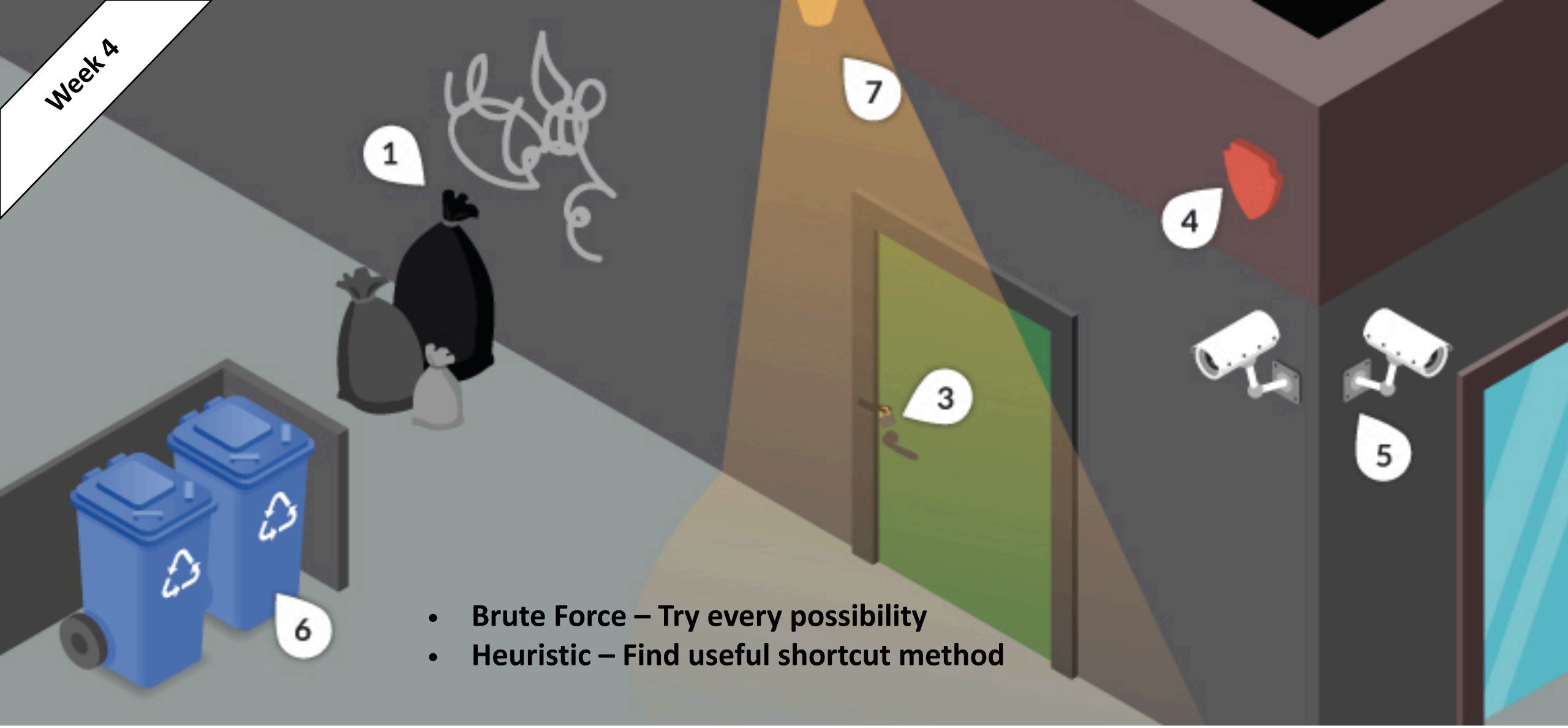
Def: <u>Availability Threat</u> – Asset maliciously blocked from authorized use.

Week 4

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

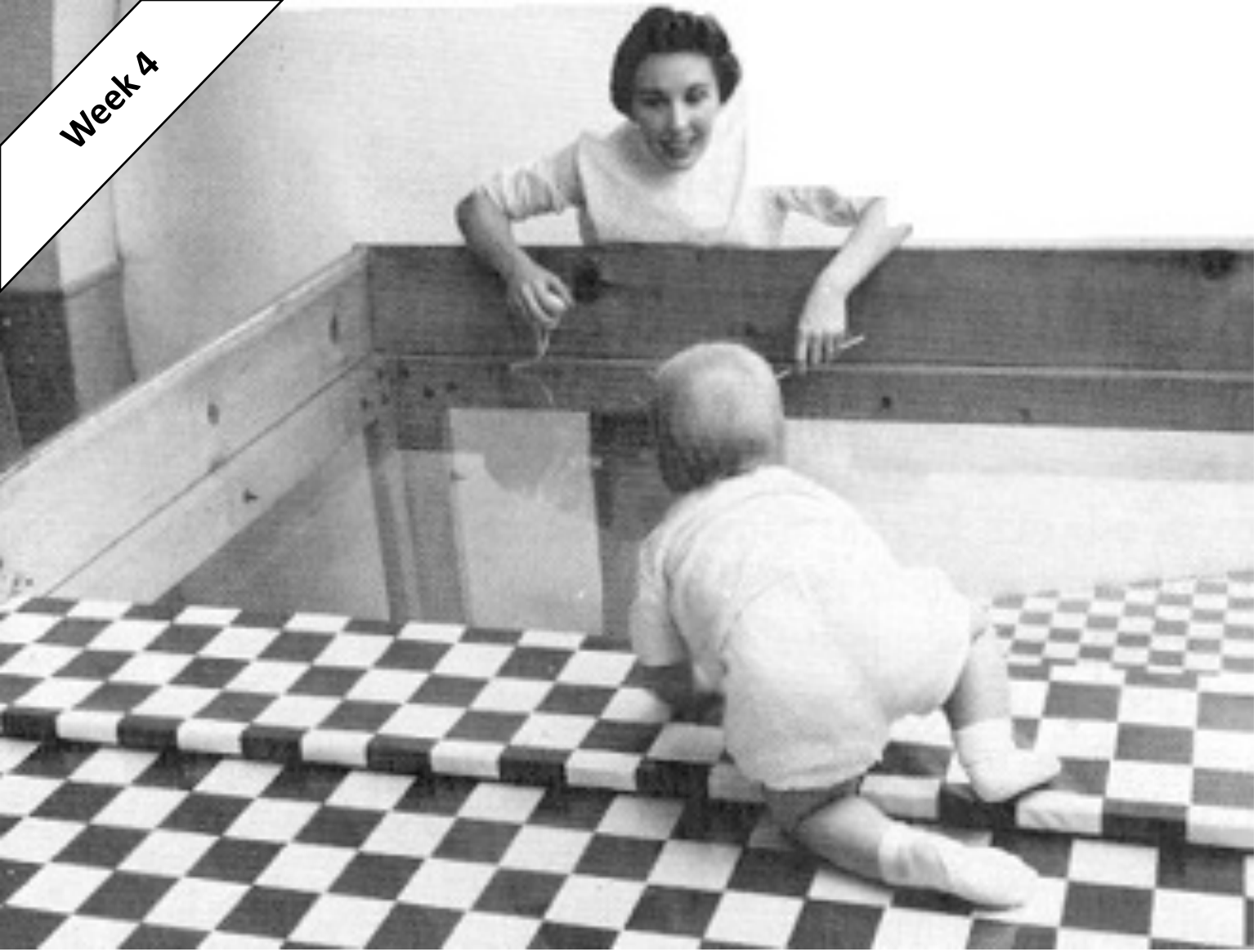
Week 4

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

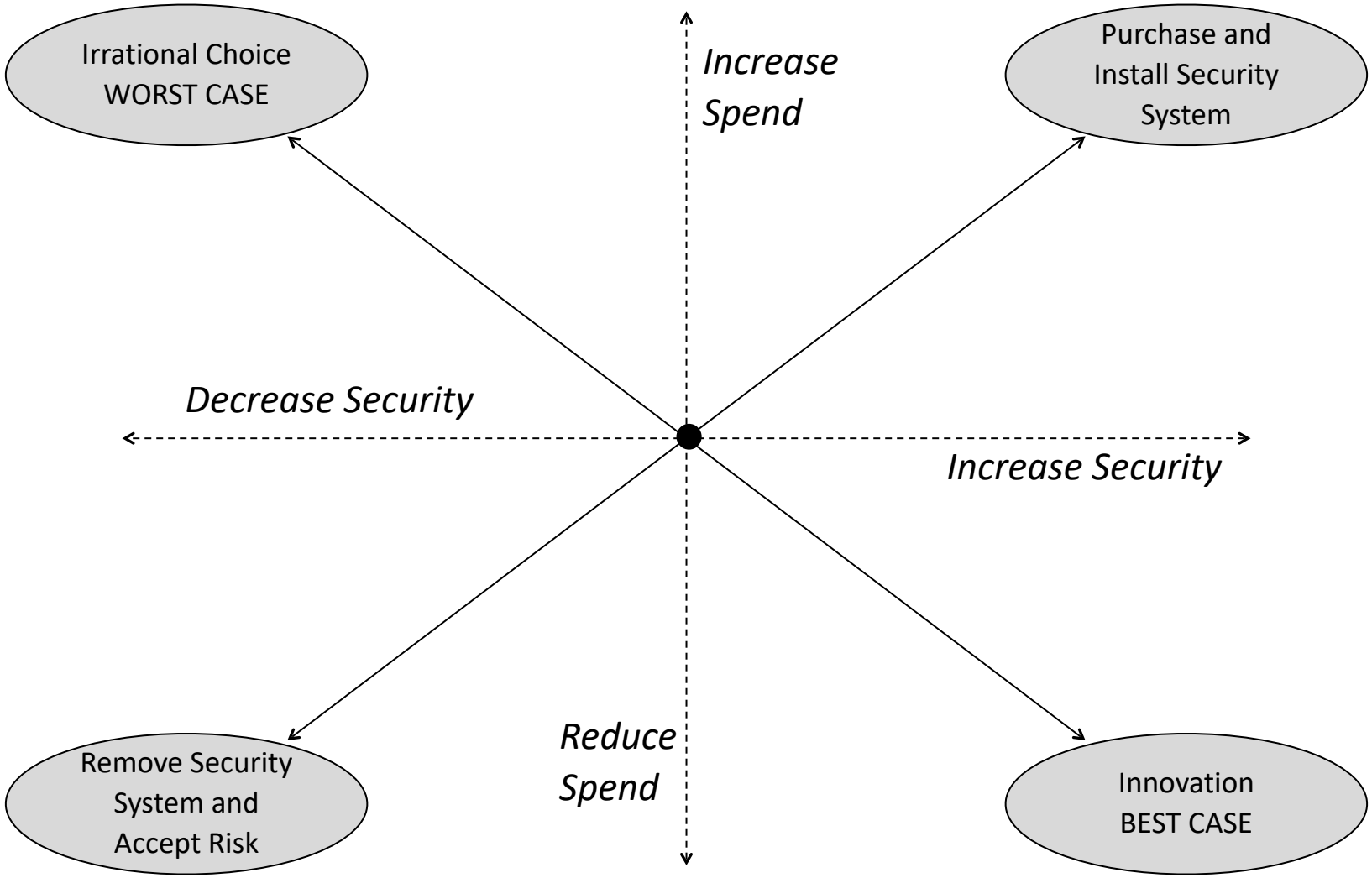


Risk (R) equals
Probability (P) of Threat
times
Consequence (C) of Threat

R = P * C

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

Week 4



Security Risk Assessment – Decision Framework

Week 4

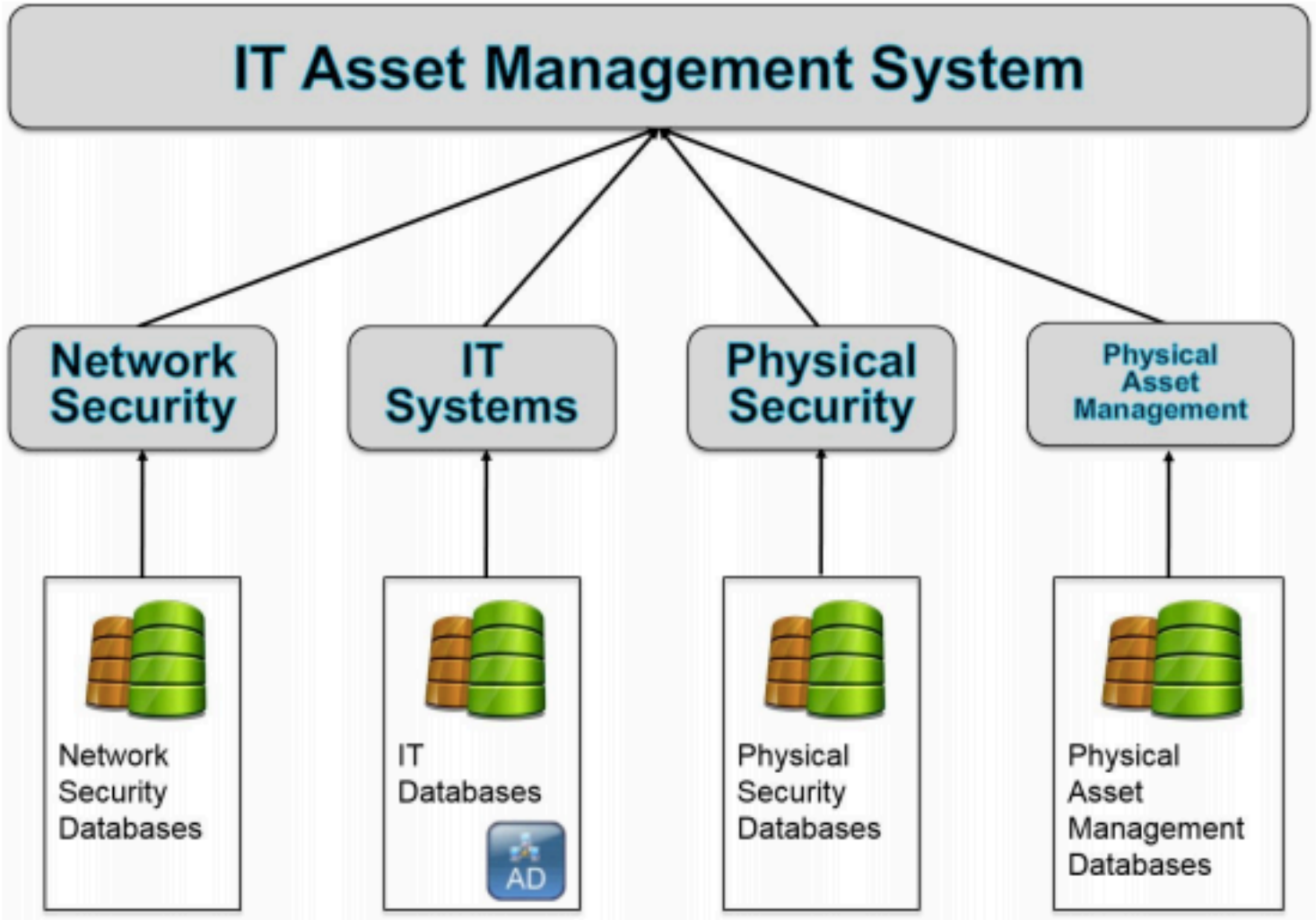
Illustrating Tiered Prioritization of Assets

Week 4

Illustrating Tiered Prioritization of Assets

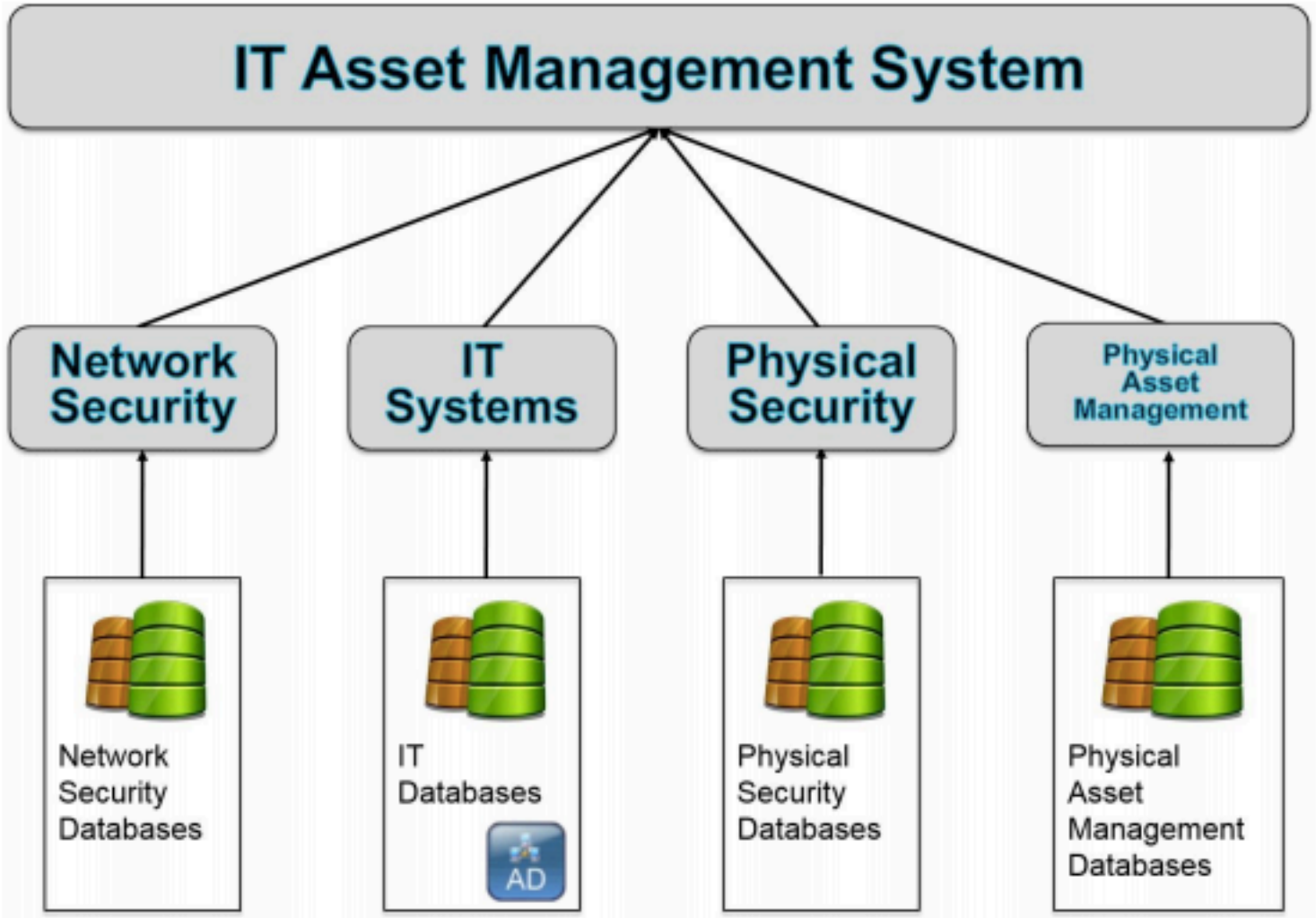
- ☑ Replaceability
- ☑ Convenience
- ☑ Sensitivity
- ☑ Emotion
- ☑ Dependence
- ☑ Liability
- ☑ Stewardship
- ☑ Finance
- ☑ Preference

Week 4



NIST IT Asset Management System Model

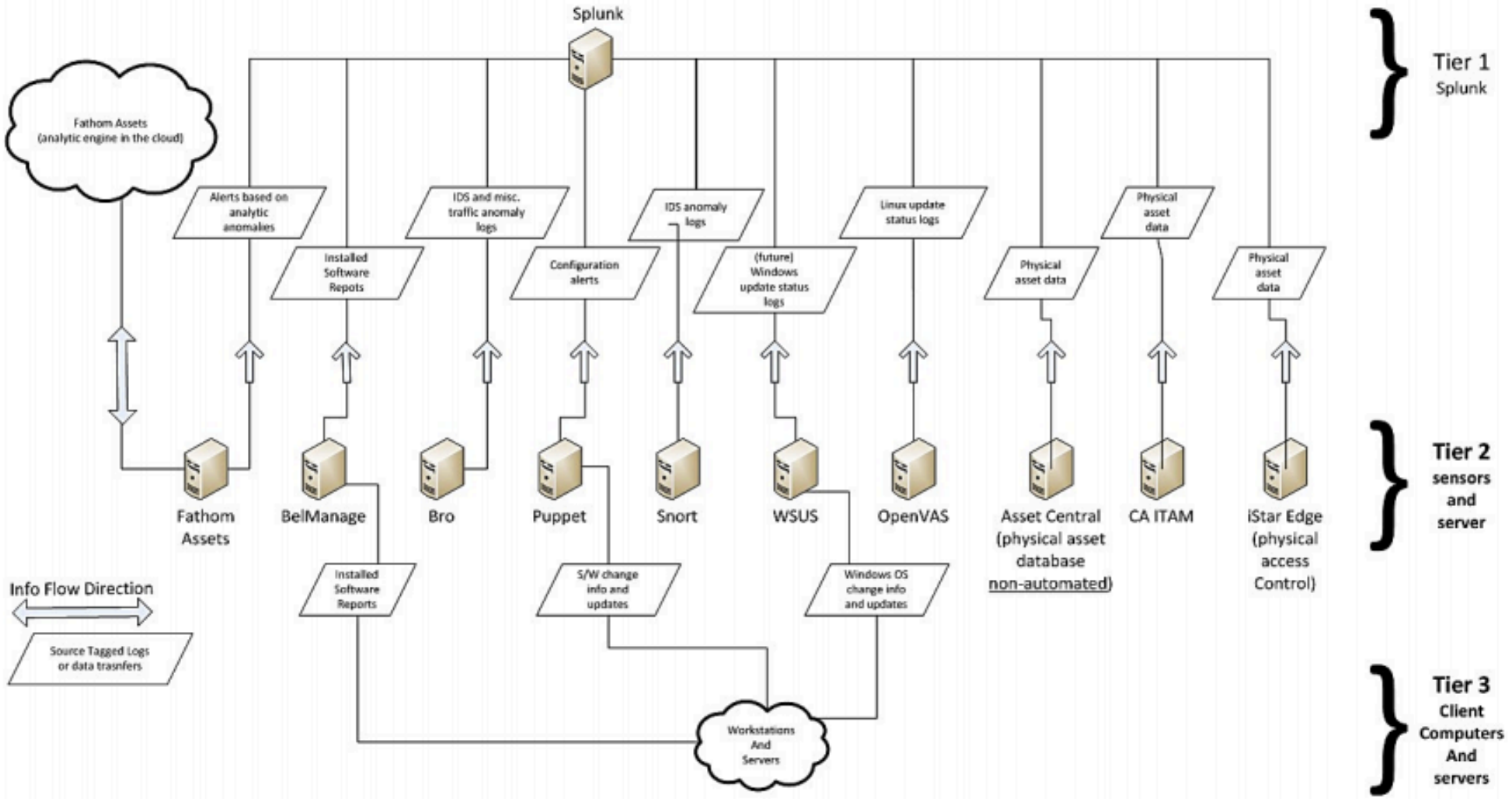
Week 4



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

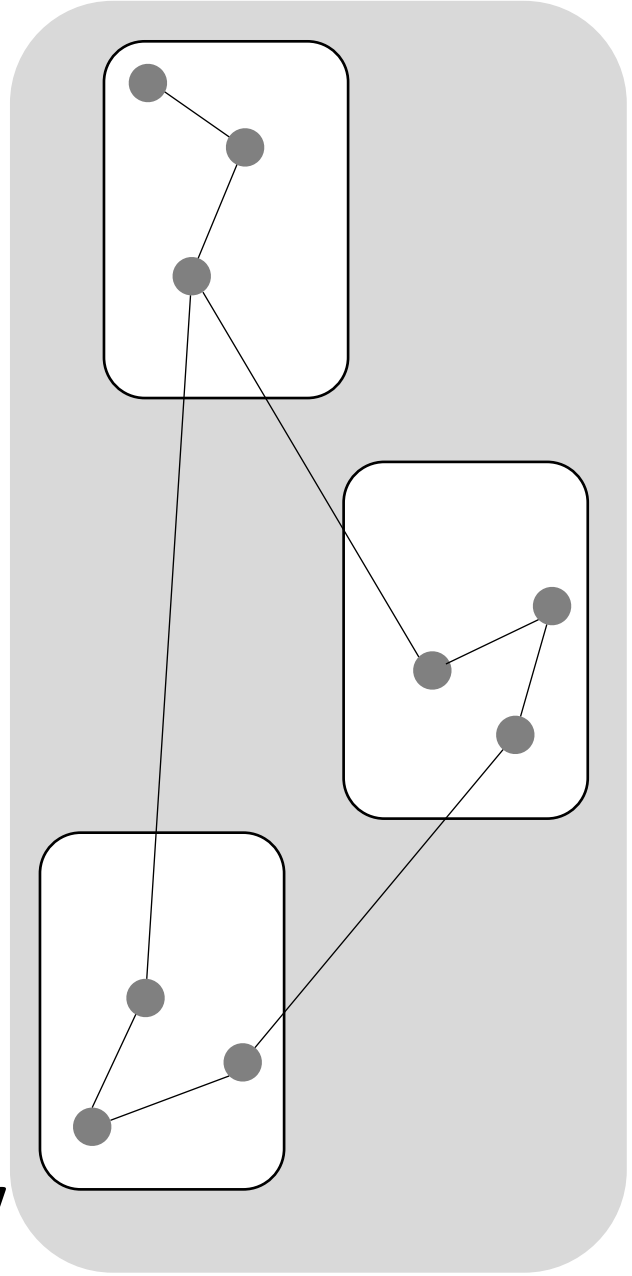
Cloud

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

Collect Network Data → Process and Analyze → Generate Connection Model

Asset Discovery Platform (Network Data)

Network Device Connectivity Map



Typical Automated Asset Discovery

Week 4

Developing a Threat-Asset Matrix

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

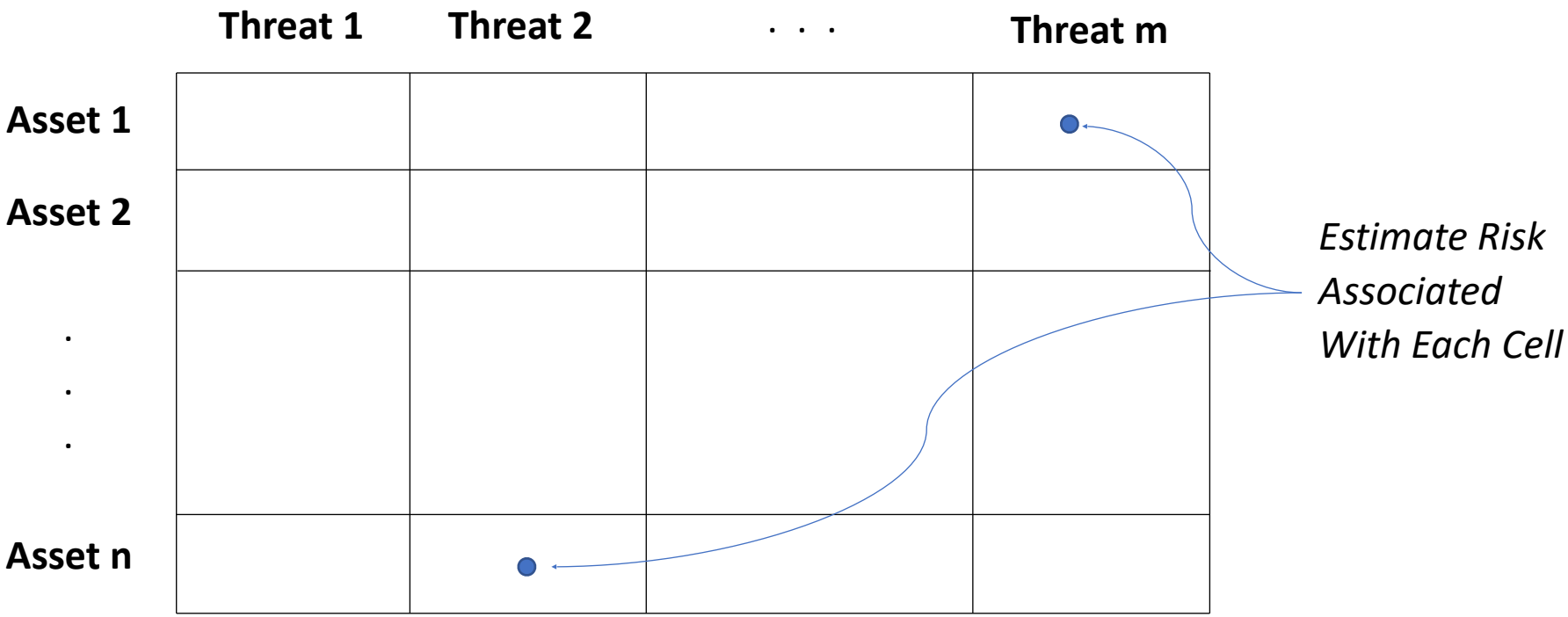
Week 4

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)

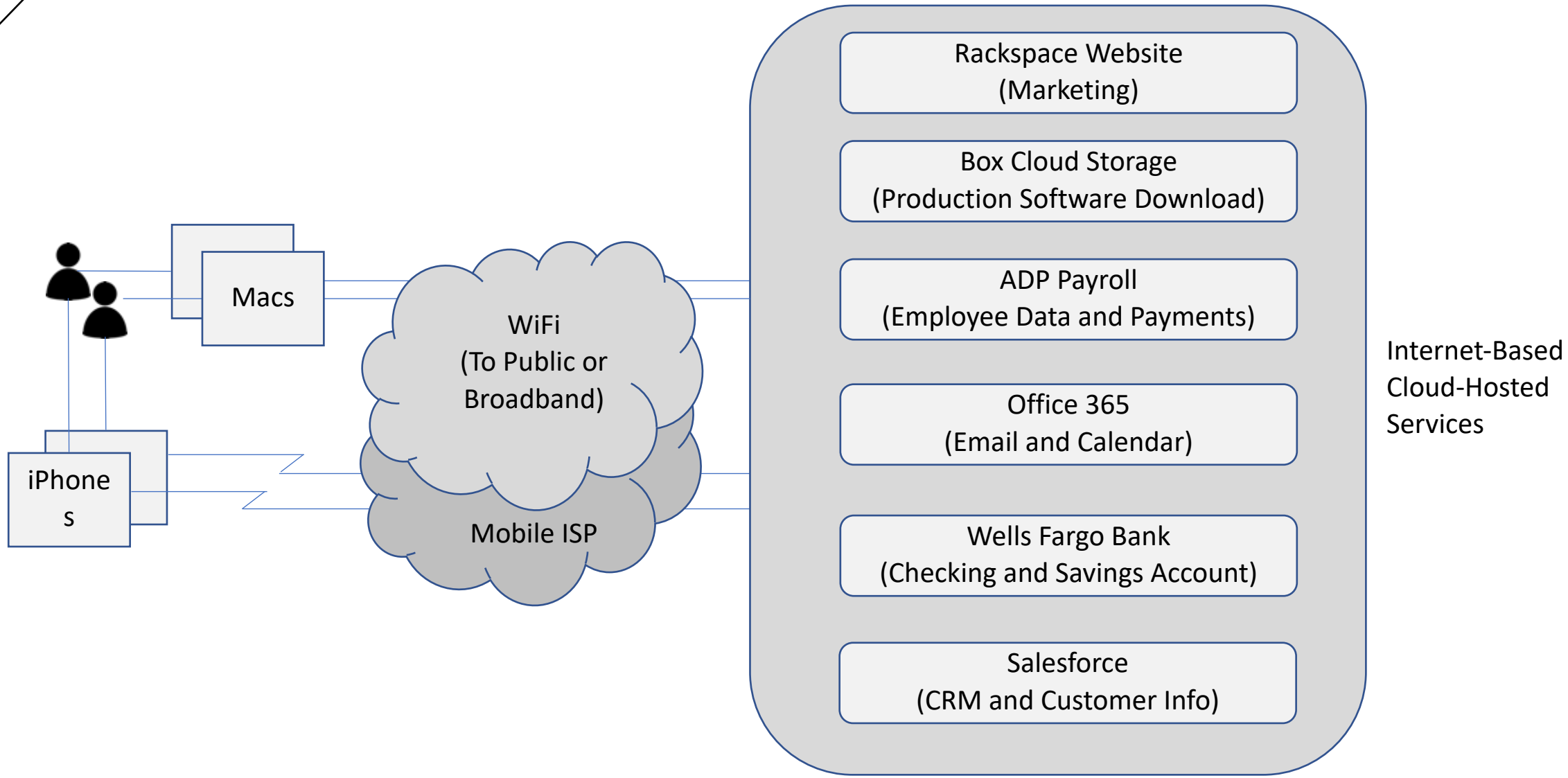
Week 4

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.