It Depends…

There are no right answers in cybersecurity

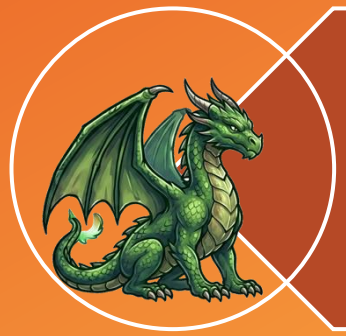
There are, however, plenty of wrong ones…

Security:
Your Client's #1 priority*

* Not counting customer satisfaction, profit, compliance, job security, public image...

What does security even mean??

What does security even mean??



Confidentiality

Integrity

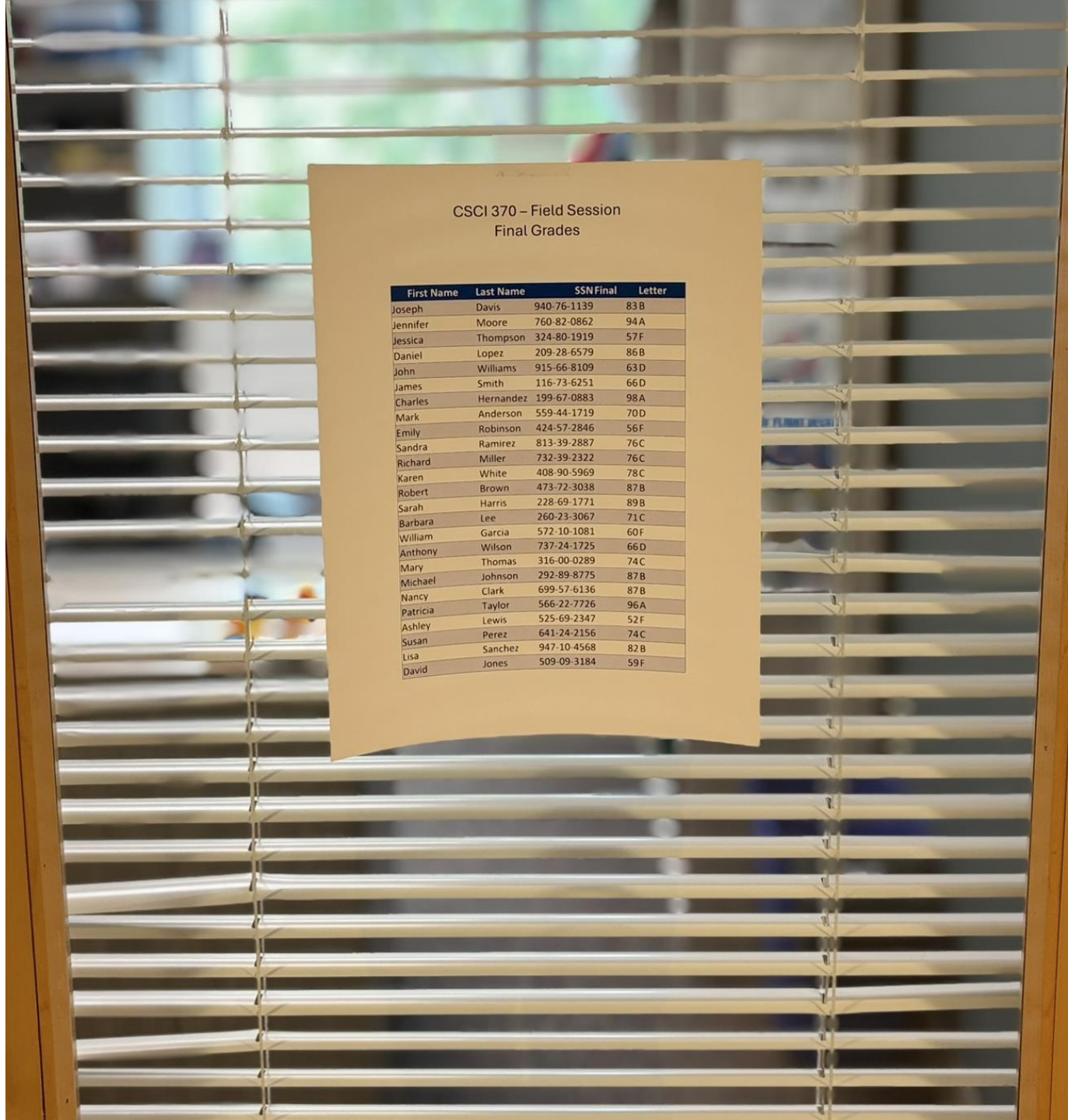
Availability

It Depends!

Confidentiality is easy!

It Depends!

Availability is easy!



Security: Finding the right balance.

The Risk Register

Finding that balance is too important to be left to chance. Just like we must expose our decisions about functionality and design, we need to be deliberate when evaluating risk

What is risk?

https://www.balbix.com/insights/cyber-risk-heat-map/

Likelihood

Impact

4	8	12	16
3	6	9	12
2	4	6	8
1	2	3	4

NIST 800 37

Low	< 4
Medium	< 8
Moderate	< 12
High	

Some Key Terms Cybersecurity World

Asset

- A system, resource, or capability of value to its owner that requires protection

Vulnerability

- A flaw or weakness in an asset's design, implementation or operation, and management that could be exploited by some threat.

Threat

- Any circumstance or event with the potential to adversely impact organizational
- Threat source: may be natural or man made.

Risk

- the impact of an exploit taking place

Control/Countermeasure

- actions taken/configurations to remediate vulnerabilities

Some Key Terms
Project Management World

Asset

- something that we are trying to protect

Risk

- A negative outcome that could happen

Trigger

- The thing that causes the risk to be realized

Priority

- likelihood * impact

Mitigation Strategy

- actions taken/configurations to remediate vulnerabilities

Owner

- Individual responsible for monitoring for the trigger and implementing the mitigation strategy.

Step 1: Set Organizational Risk Tolerance

The organization (your client), not your team team should determine the risk tolerance.

Risk = Likelihood * Impact		
20-25	Risk Taker	
15-20	Risk Tolerant	
10-15	Cautious	
5-10	Risk Averse	
0-5	Risk Intolerant	

Step 2: Identify Assets

Asset is something we are trying to protect.

Student Records
Research Findings
CS Faculty
PII
Electron Microscope

Step 3: Identify Vulnerabilities

Vulnerability is a weakness. Each asset has many vulnerabilities.

Student Records	Records are associated with individuals Stored on system with no password.
Research Findings	Can be erased Expensive to reproduce.
CS Faculty	Easy to bribe
PII	Inadequate safeguards in society around id theft.
Electron Microscope	Doesn't work if it gets wet Difficult to replace

Step 4: Identify Threats

Threat is the bad thing that happens if a vulnerability is exploited

Student Records stored with student names

- Disclosure is a violation of the Federal Education Privacy Act

CS Faculty are easy to bribe

- Students bring donuts to class and get a better grade than they earned.

Electron Microscope's don't work if they get wet

- Clear creek floods and destroys the microscope.

To identify threats, you need to identify threat sources. This may be done now, or maybe done before anything else.

Step 5: Compute the risk

For each threat, determine the likelihood and the impact

Asset	Vulnerability	Threat	Likelihood	Impact	Risk
Grades	Grades stored with student names	Disclosure is FERPA violation	3	4	12

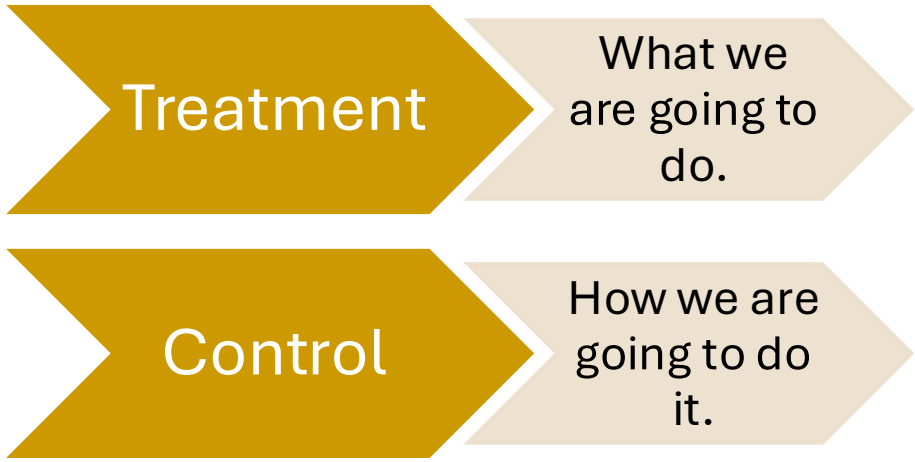
Likelihood and impact may not be associated with a single factor. Multiple vulneraries may influence the likelihood and/or impact.

Any Risk above the Organizational Tolerance should be dealt with

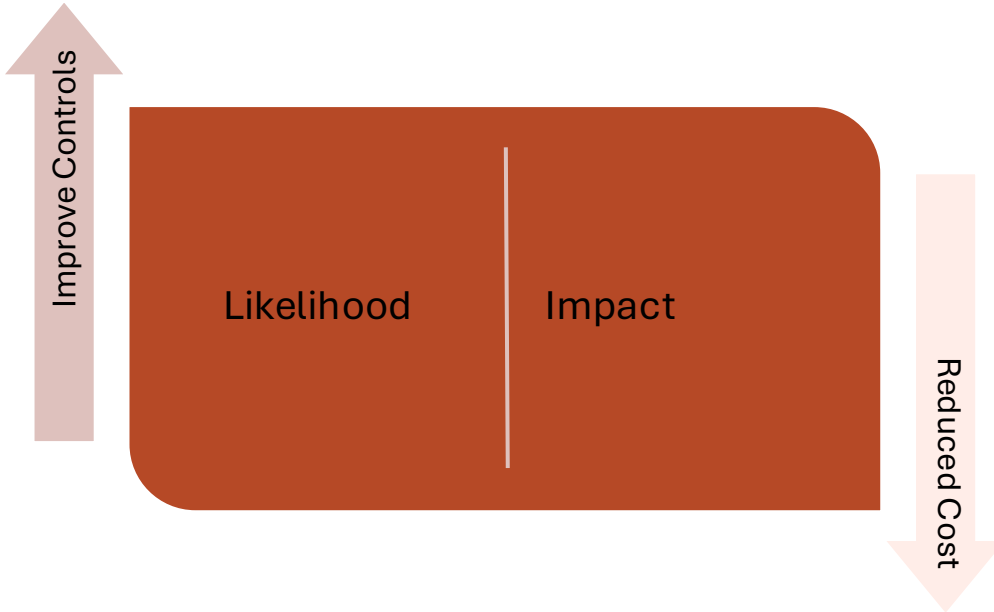
Asset	Vuln	Threat	Likelihood	Impact	Risk
Student Grades	Stored with name & SSN	Disclosure is FERPA viol	Likely (4)	Medium(3)	12
Research Findings	Encrypted to protect human subjects	Loose encryption key, it's gone	Occasional (2)	Catastrophic (4)	4
Organization Reputation	Customers get mad if PII leaked	Customers leave for other app.	Medium(3)	Serious (3)	9
Microscope	Doesn't work when wet	Clear Creek Flood	Medium(3)	Serious (3)	9
Students	People can't live under 100 tons of rock	Meteorite hits campus	Rare(1)	Doomsday(5)	5

Step 6: Risk Treatment

1. Risk Acceptance
2. Risk Avoidance
3. Risk Transfer
4. Reduce Impact
5. Reduce Likelihood



Controls



Reduce Likelihood

May involve addressing vulnerability or threat (or both).

- Formal code review to identify bugs.
- Review npm/pypi packages.
- Provide donuts in kitchen daily.
- Keep microscope on upper floors.

Reduce Impact

May involve addressing vulnerability or threat (or both).

- Local backups
- Remote backups
- Discard PII
- Offline checksums

Group Exercise: Camping Risks

Risks: What might happen and how serious is it?

Asset	Vuln	Threat	Likelihood	Impact	Risk	Treatment	Owner	Control
Student Grades	Stored with name & SSN	Disclosure is FERPA viol	Likely (4)	Medium(3)	12	Reduce Likelihood	Joe	Code review tools.
Research Findings	Encrypted to protect human subjects	Loose encryption key, it's gone	Occasional (2)	Catastrophic (4)	4	Reduce Likelihood	Sue	Keep organizational backups
Organization Reputation	Customers get mad if PII leaked	Customers leave for other app.	Medium(3)	Serious (3)	9	Reduce Impact	Mark	PR plan in place.
Microscope	Doesn't work when wet	Clear Creek Flood	Medium(3)	Serious (3)	9	Transfer	Kirsten	Buy insurance
Students	People can't live under 100 tons of rock	Meteorite hits campus	Rare(1)	Doomsday(5)	5	Accept		

Questions?