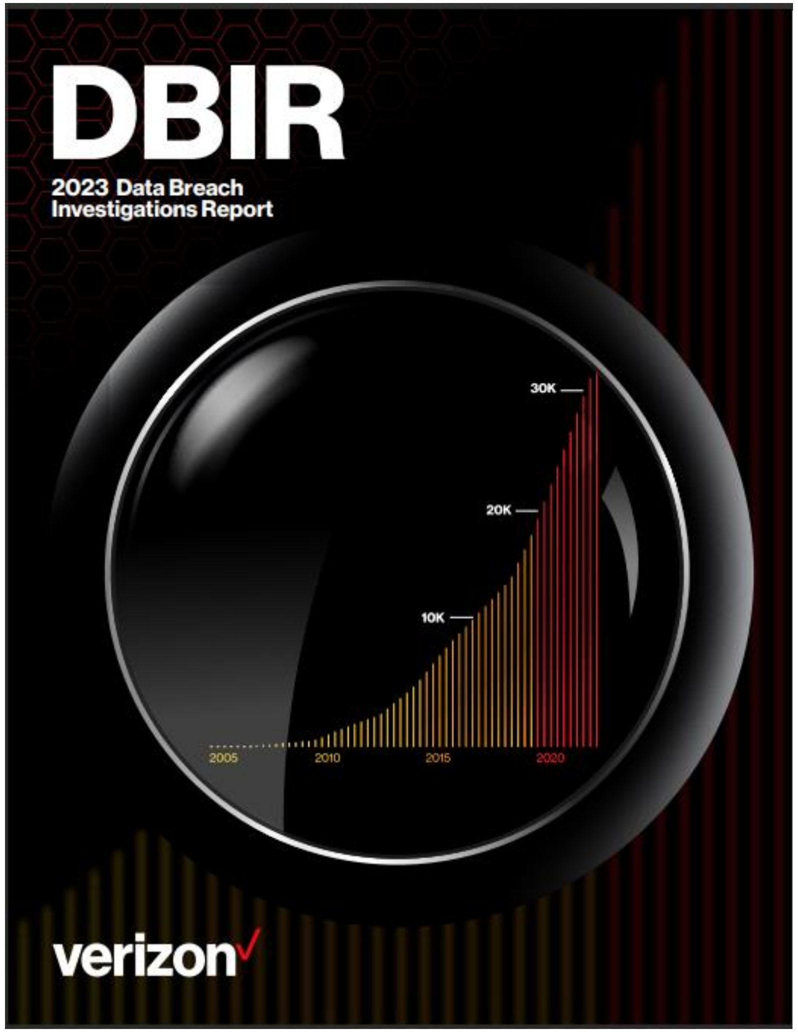
Information Systems Integration MIS 4596

Class 2

Agenda

- Threat Environment
- Cybersecurity Risk
- Threat Modeling
- Next Week’s Quiz

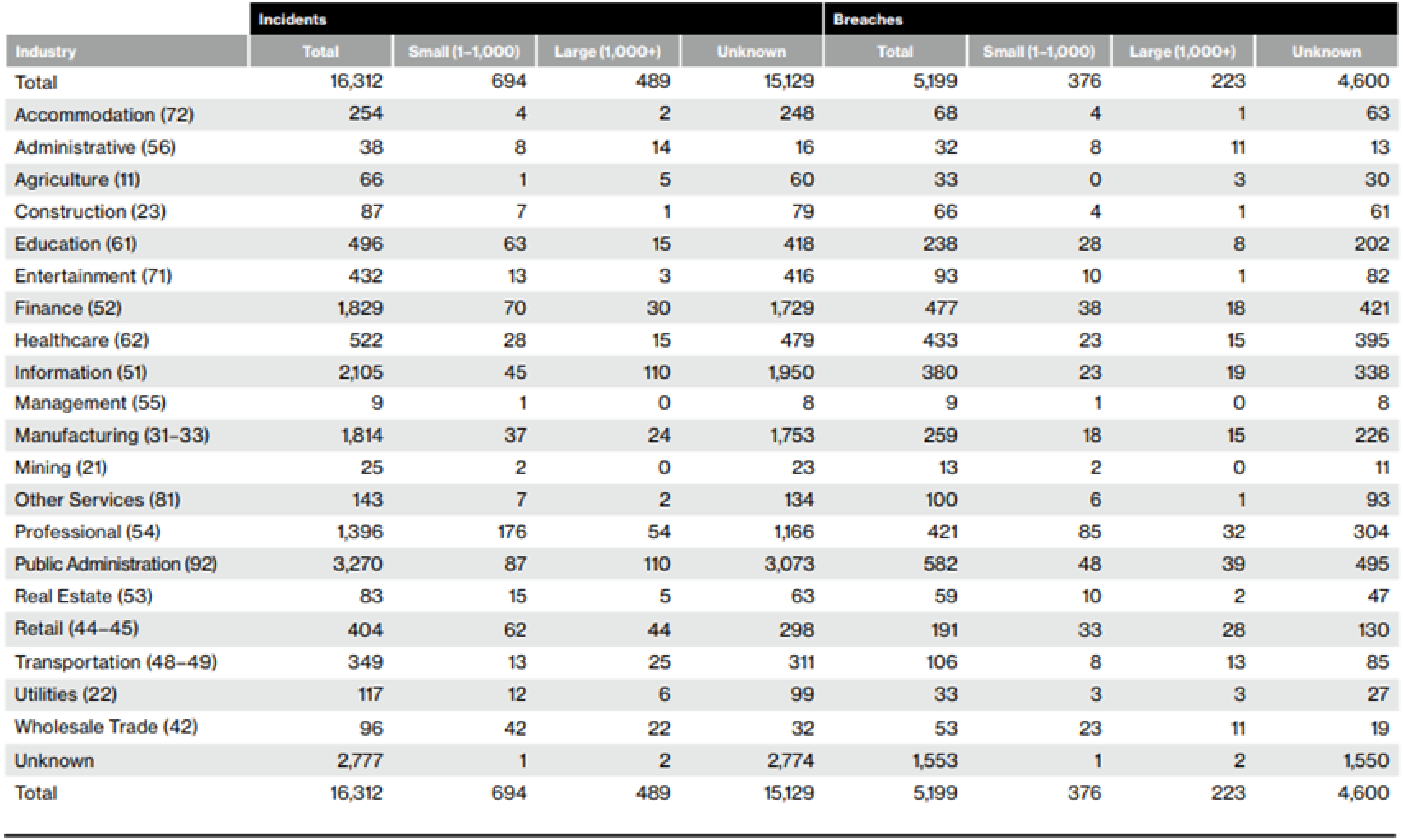
Threat Environment



DBIR

2023 Data Breach Investigations Report

verizon



	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	16,312	694	489	15,129	5,199	376	223	4,600
Accommodation (72)	254	4	2	248	68	4	1	63
Administrative (56)	38	8	14	16	32	8	11	13
Agriculture (11)	66	1	5	60	33	0	3	30
Construction (23)	87	7	1	79	66	4	1	61
Education (61)	496	63	15	418	238	28	8	202
Entertainment (71)	432	13	3	416	93	10	1	82
Finance (52)	1,829	70	30	1,729	477	38	18	421
Healthcare (62)	522	28	15	479	433	23	15	395
Information (51)	2,105	45	110	1,950	380	23	19	338
Management (55)	9	1	0	8	9	1	0	8
Manufacturing (31–33)	1,814	37	24	1,753	259	18	15	226
Mining (21)	25	2	0	23	13	2	0	11
Other Services (81)	143	7	2	134	100	6	1	93
Professional (54)	1,396	176	54	1,166	421	85	32	304
Public Administration (92)	3,270	87	110	3,073	582	48	39	495
Real Estate (53)	83	15	5	63	59	10	2	47
Retail (44–45)	404	62	44	298	191	33	28	130
Transportation (48–49)	349	13	25	311	106	8	13	85
Utilities (22)	117	12	6	99	33	3	3	27
Wholesale Trade (42)	96	42	22	32	53	23	11	19
Unknown	2,777	1	2	2,774	1,553	1	2	1,550
Total	16,312	694	489	15,129	5,199	376	223	4,600

Table 2. Number of security incidents and breaches by victim industry and organization size

The 2023 DBIR examined 16,312 incidents, of which 5,199 were confirmed data breaches

Threat Environment

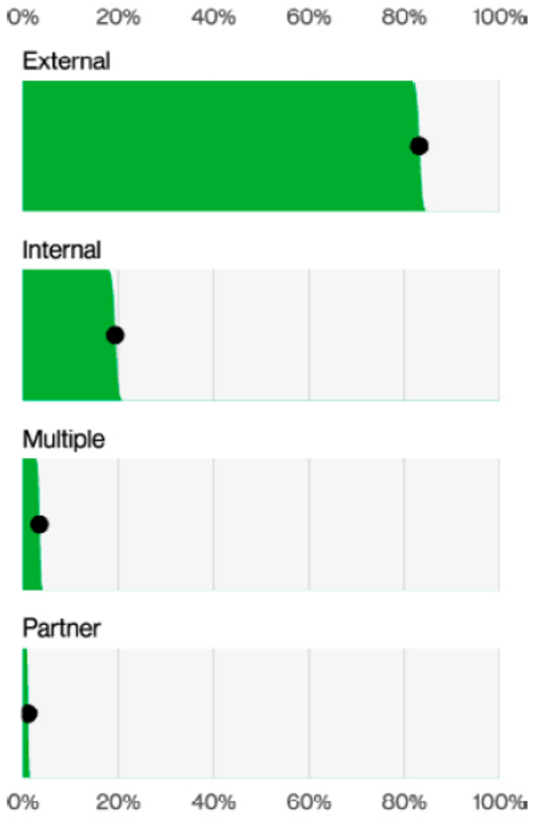


Figure 11. Threat actors in breaches (n=5,177)

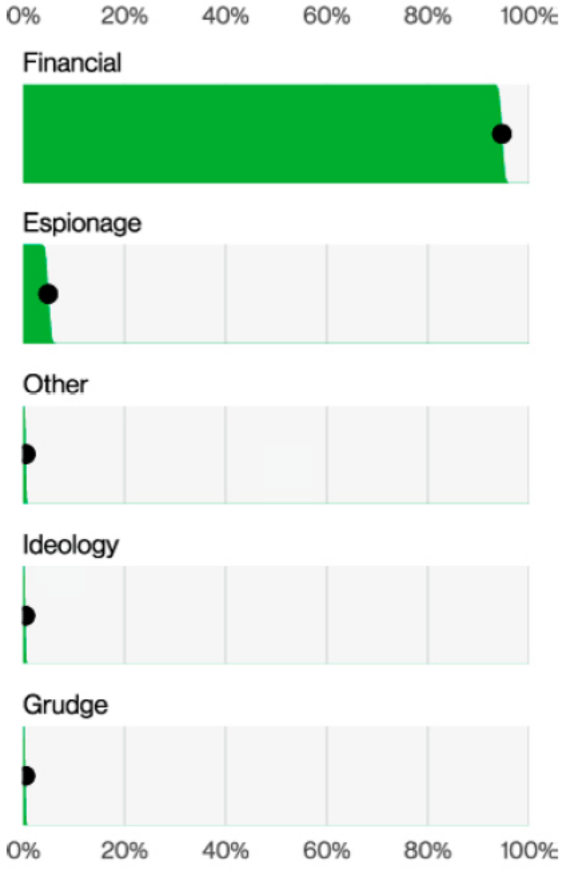


Figure 12. Threat actor Motives in breaches (n=2,328)

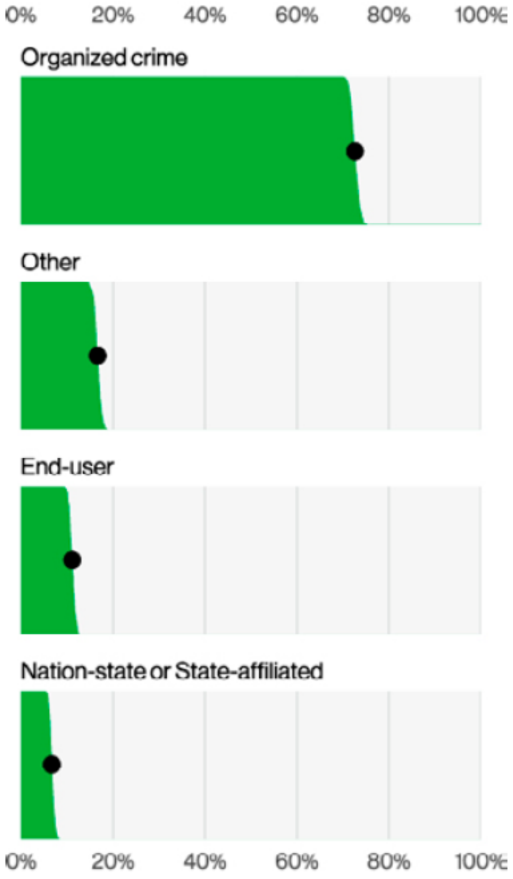
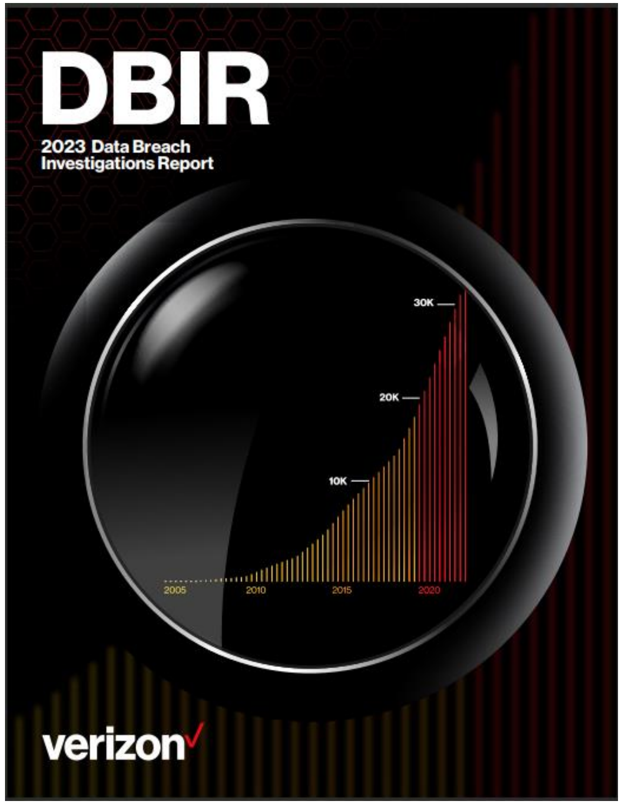


Figure 13. Threat actor Varieties in breaches (n=2,489)



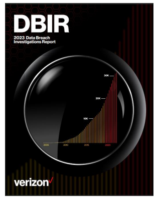
- External actors were responsible for 83% of breaches, while Internal ones account for 19%.

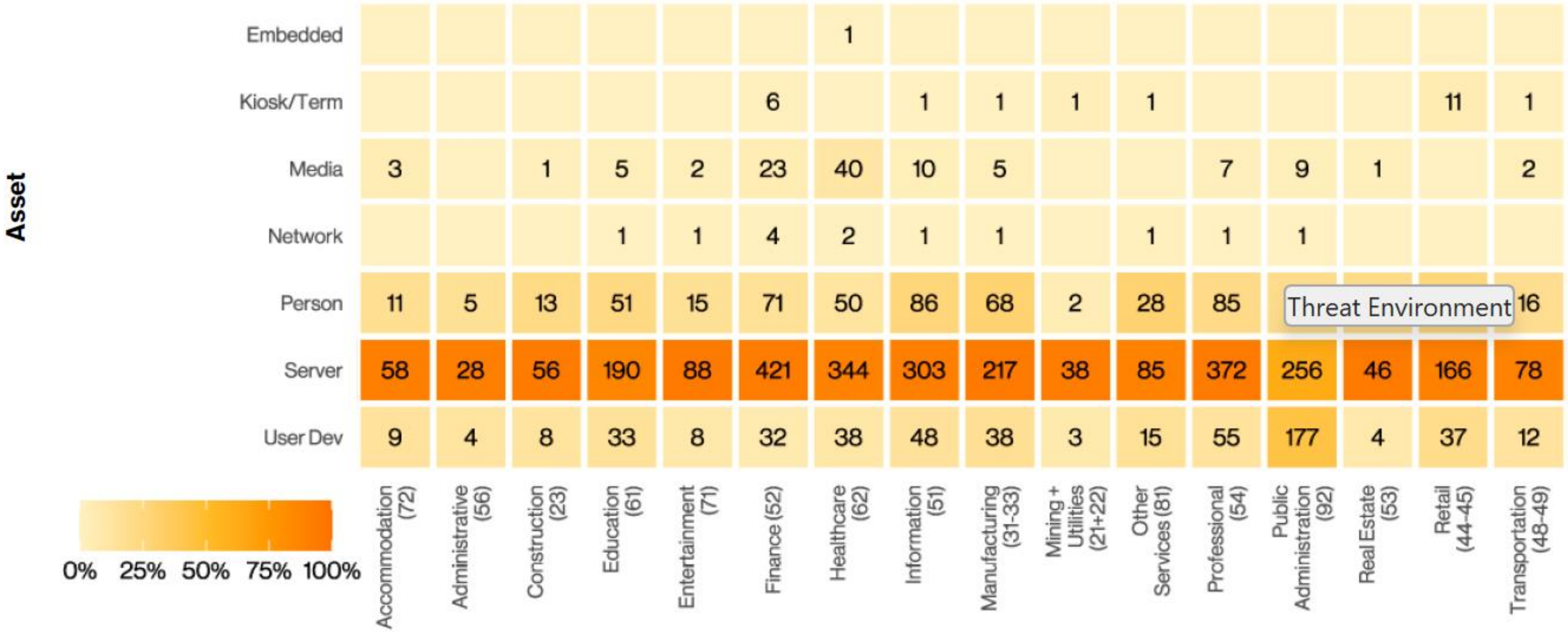
- Internal actors are responsible for intentional harm, and twice as likely to be responsible for Error actions.

End-users are organization employees mostly involved in breaches caused by:

- Misuse (“internal malicious activity”), and
- Errors (“accidents”).

Threat Environment– Breaches by Industry

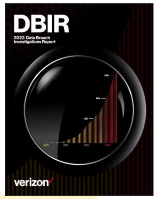


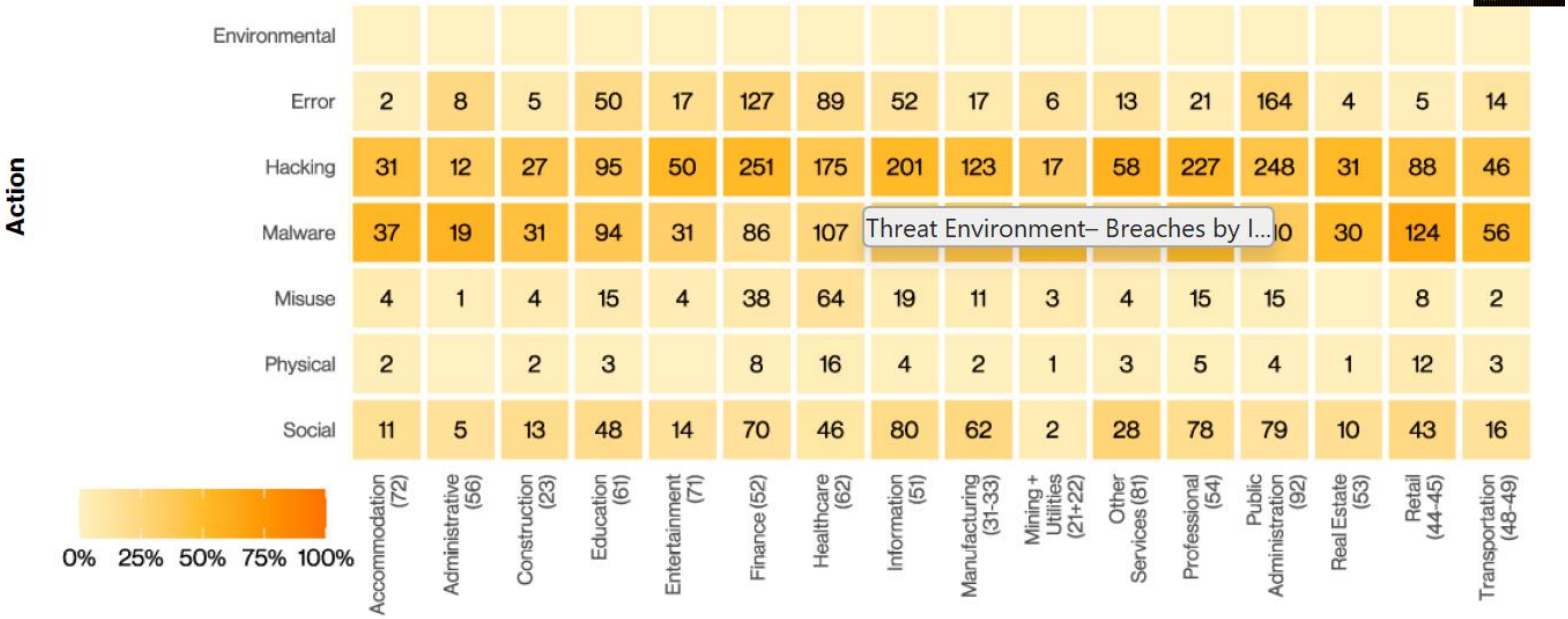


Asset	Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Embedded							1									
Kiosk/Term						6		1	1	1	1				11	1
Media	3		1	5	2	23	40	10	5			7	9	1		2
Network				1	1	4	2	1	1		1	1	1			
Person	11	5	13	51	15	71	50	86	68	2	28	85	[illegible]	[illegible]	[illegible]	16
Server	58	28	56	190	88	421	344	303	217	38	85	372	256	46	166	78
User Dev	9	4	8	33	8	32	38	48	38	3	15	55	177	4	37	12

The 2023 DBIR examined 16,312 incidents, of which 5,199 were confirmed data breaches

Threat Environment– Breaches by Industry



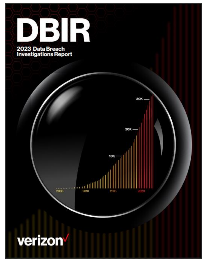


Action	Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Environmental																
Error	2	8	5	50	17	127	89	52	17	6	13	21	164	4	5	14
Hacking	31	12	27	95	50	251	175	201	123	17	58	227	248	31	88	46
Malware	37	19	31	94	31	86	107	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	30	124	56
Misuse	4	1	4	15	4	38	64	19	11	3	4	15	15		8	2
Physical	2		2	3		8	16	4	2	1	3	5	4	1	12	3
Social	11	5	13	48	14	70	46	80	62	2	28	78	79	10	43	16

Threat Environment– Breaches by I...

The 2023 DBIR examined 16,312 incidents, of which 5,199 were confirmed data breaches

Threat Environment



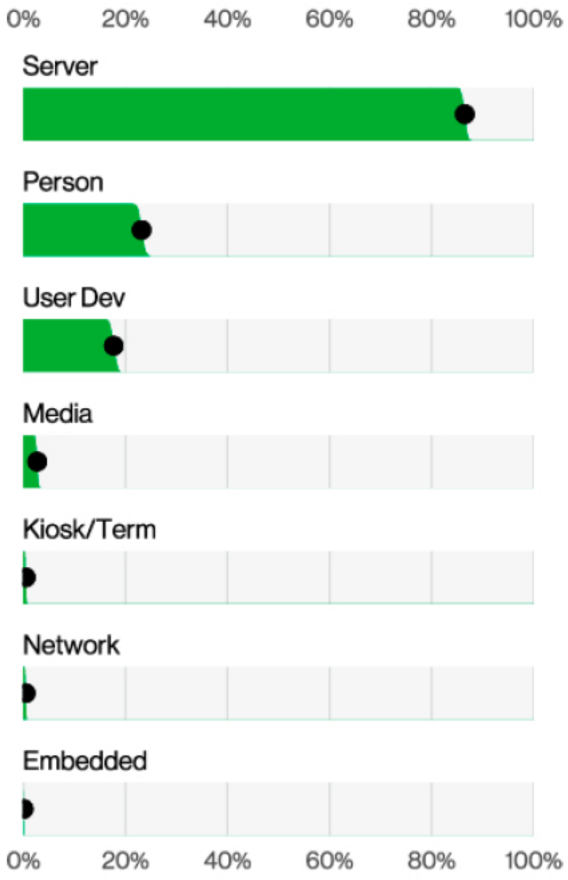


Figure 19. Assets in breaches (n=4,433)

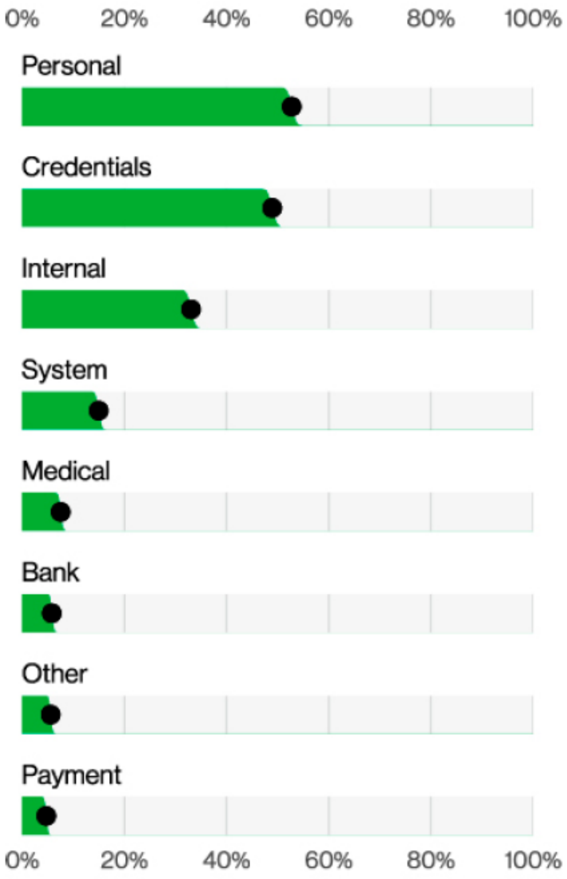
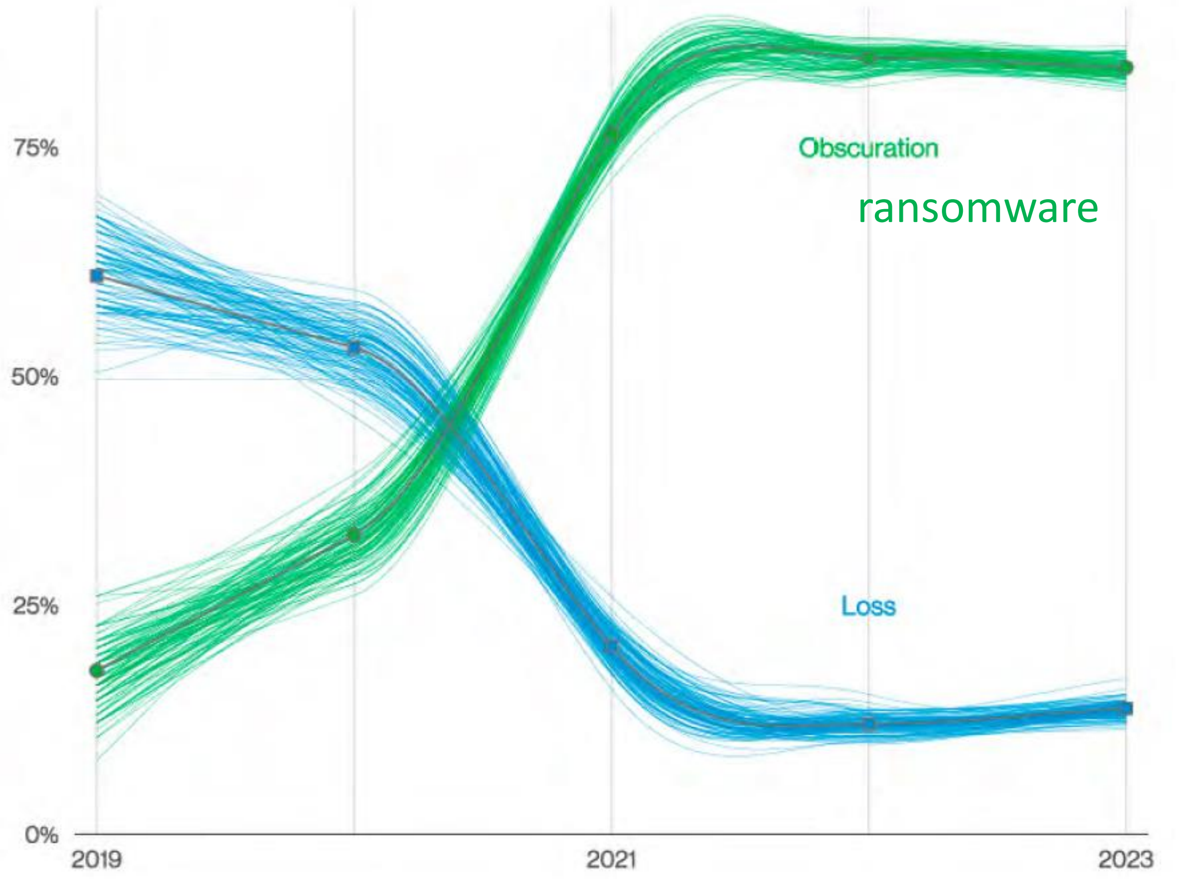


Figure 21. Top Confidentiality data varieties in breaches (n=5,010)



ransomware

Figure 22. Availability variety over time

Threat Environment

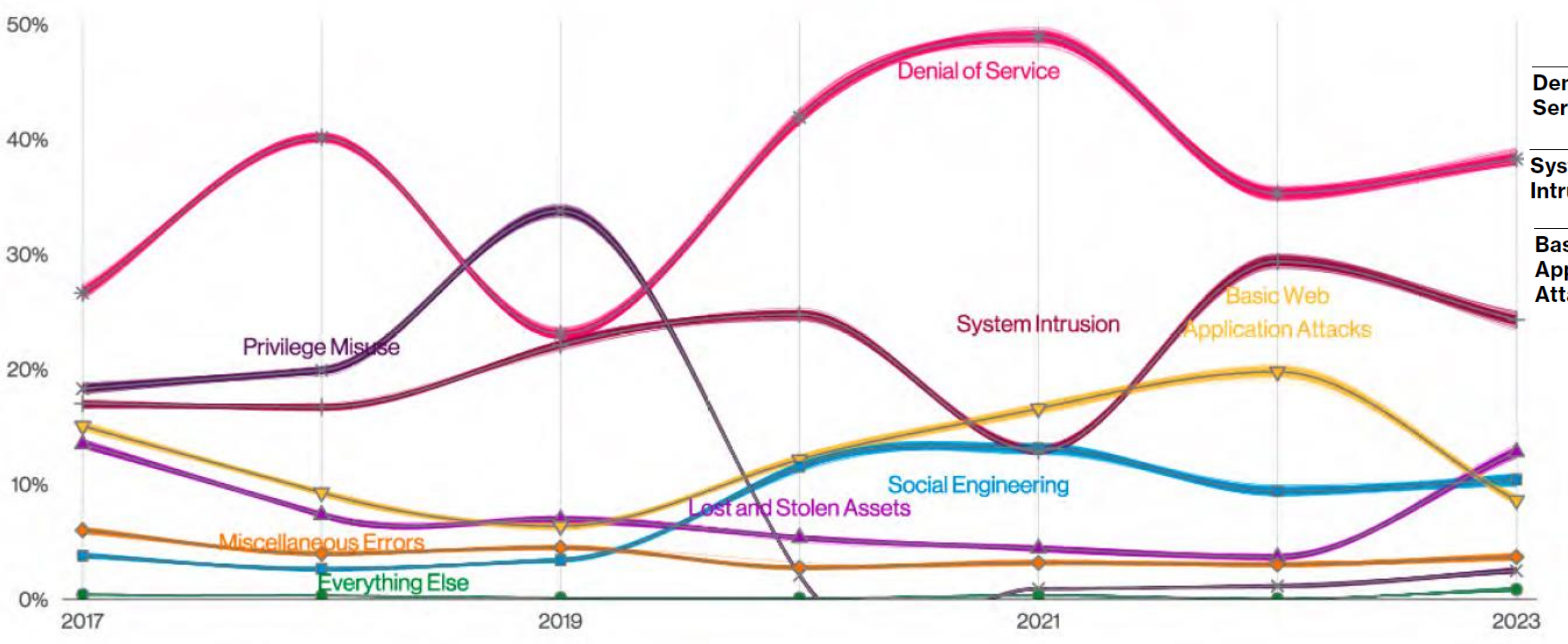
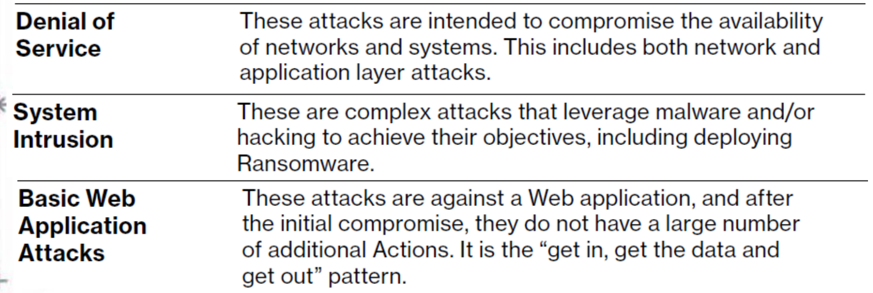


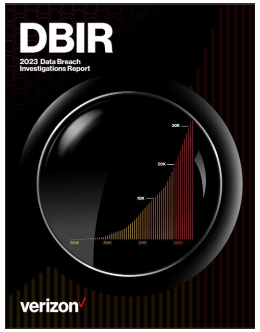
Figure 25. Patterns over time in incidents



Denial of Service	These attacks are intended to compromise the availability of networks and systems. This includes both network and application layer attacks.
System Intrusion	These are complex attacks that leverage malware and/or hacking to achieve their objectives, including deploying Ransomware.
Basic Web Application Attacks	These attacks are against a Web application, and after the initial compromise, they do not have a large number of additional Actions. It is the “get in, get the data and get out” pattern.

What are the implications for cybersecurity protections ?

Threat Environment



DBIR

2023 Data Breach Investigations Report

verizon

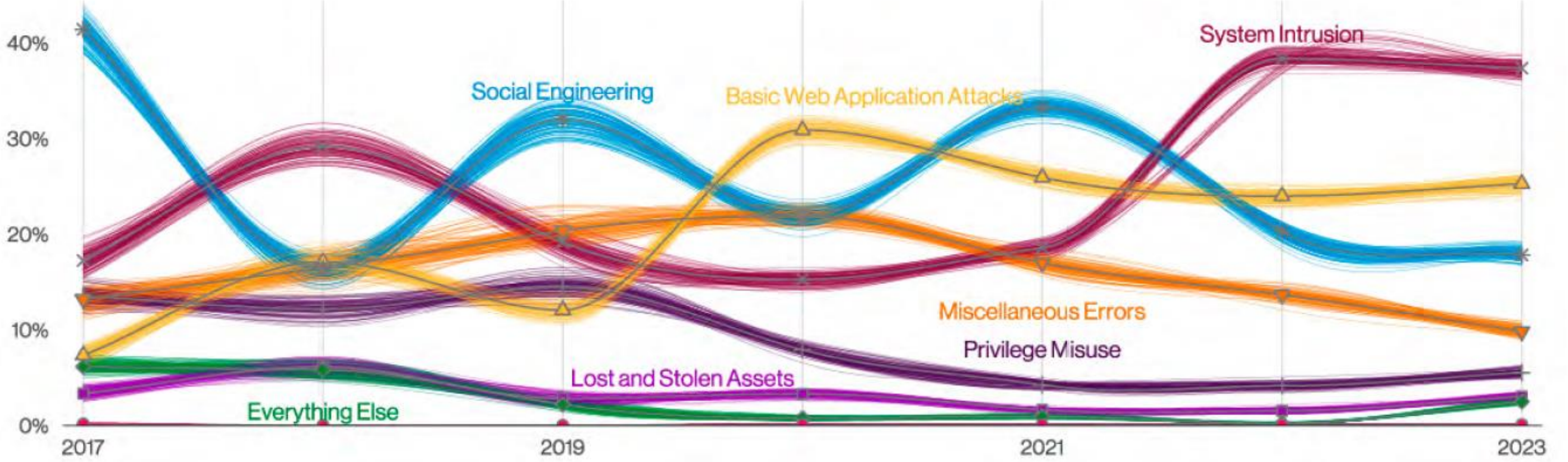


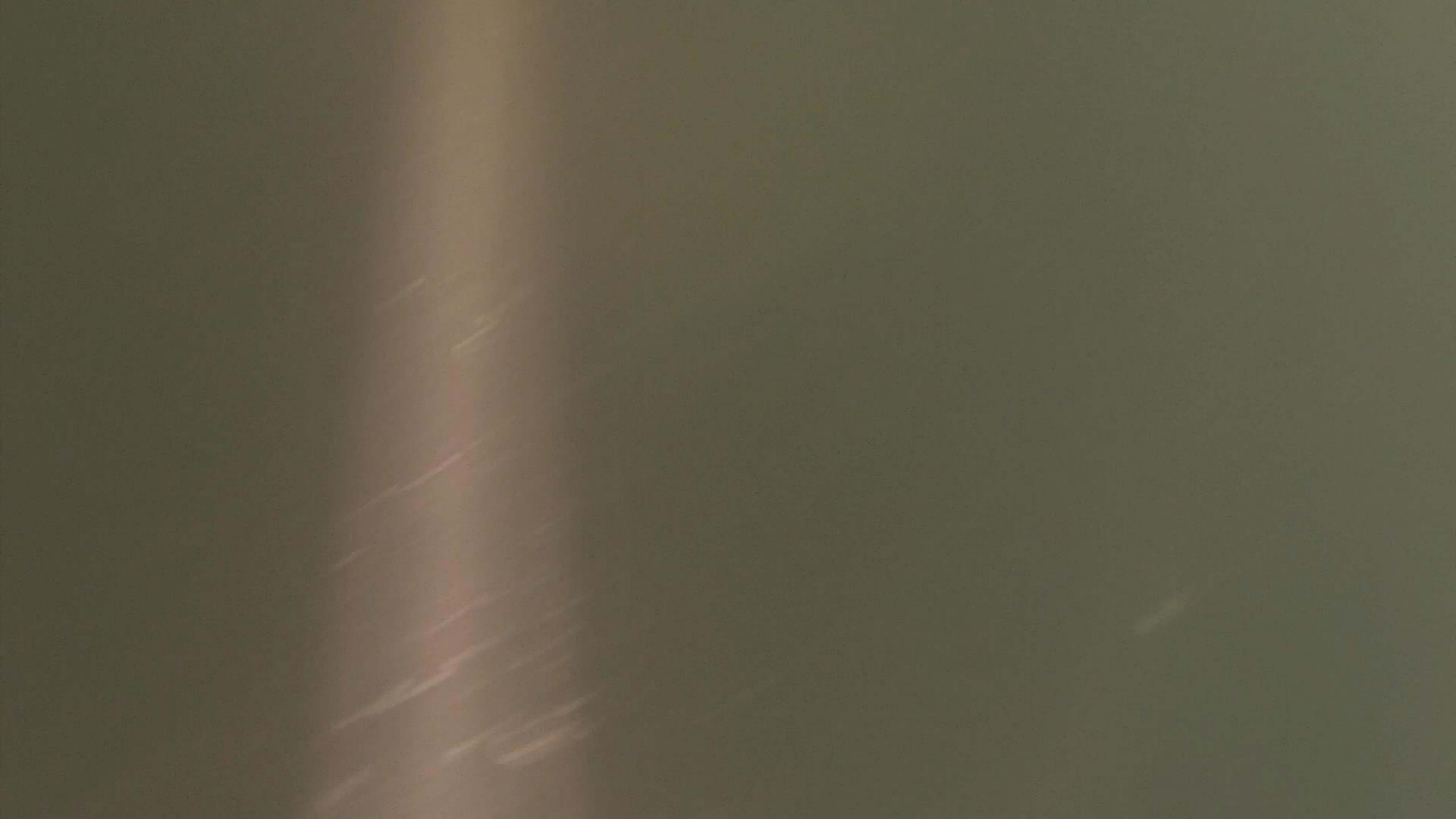
Figure 26. Patterns over time in breaches

What are the implications for cybersecurity protections?

Updated 2024 Reports posted on community site

Is this computer 100% secure?

“How can we make a computer 100% secure?”



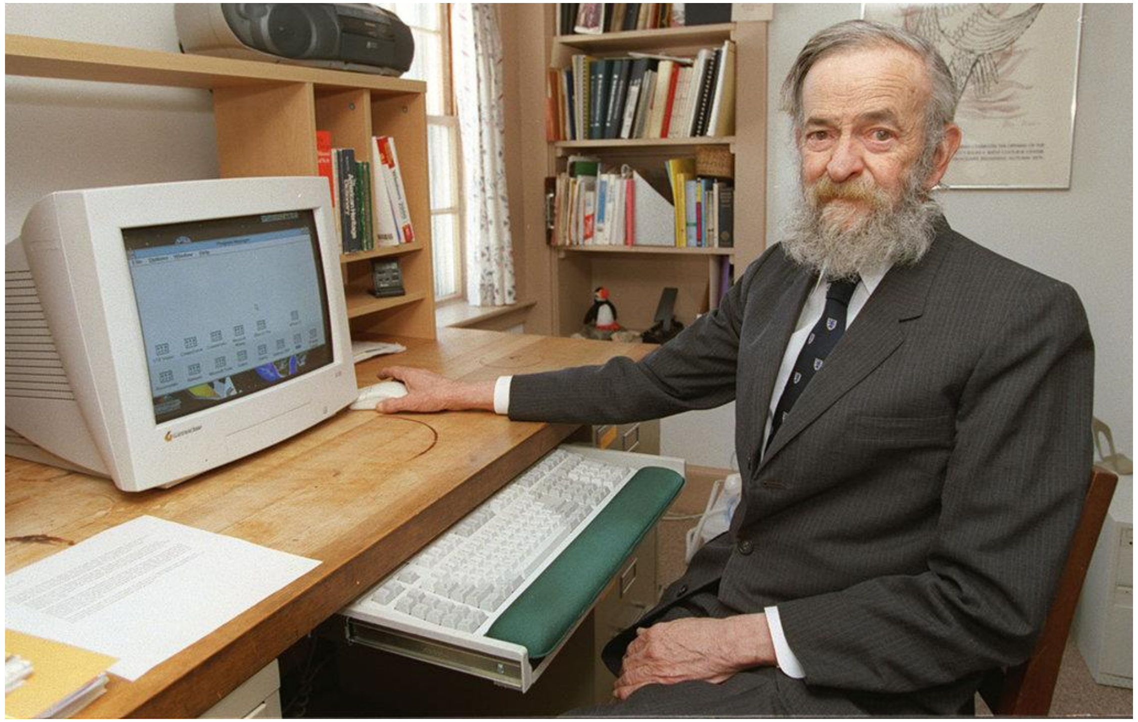
How can we make a computer 100% secure?

3 Golden Rules to ensure computer security:

1. Do not own a computer
2. Do not power it on
3. Do not use it

Robert Morris

Cryptographer who helped develop the Unix computer operating system, which controls many of the world's computers and touches almost every aspect of modern life

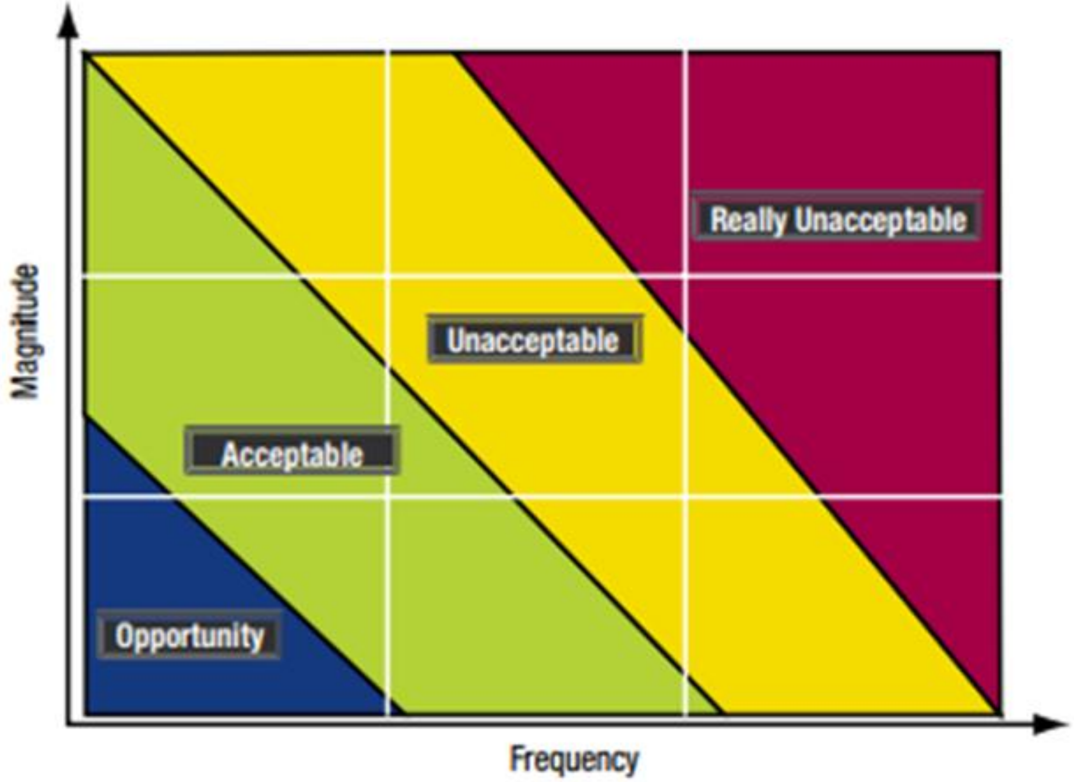


Agenda

- ✓Threat Environment
- Cybersecurity Risk
- Threat Modeling
- Caution
- Next Week’s Assignments
- Next Week’s Quiz

Businesses cannot eliminate risk, but they can manage to acceptable level of risk, by

1. Avoidance
2. Acceptance
3. Transfer
4. Mitigation (“Controls”)



Quantitative definition of risk

Risk = Impact × Probability

- *Risk is an “expected value”, which is a quantitative measure of impact a CIA breach would have on the organization times the probability that it might happen*

Annualize Loss Expectancy (ALE) = Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

ALE = SLE X ARO

Single Loss Expectancy (SLE) = Asset value X Exposure factor

- Calculations of SLE consider such things as: replacement cost of the asset, opportunity cost of delays because asset is no longer available, cost for purchasing credit monitoring for customers, fines and other economic impacts of the loss of confidentiality, integrity and availability of the information or information system.

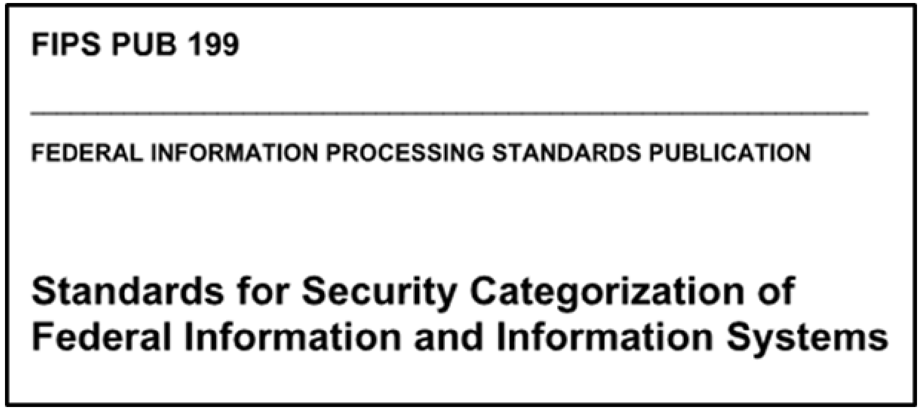
- Exposure factor is the % damage that a realized threat would have on the asset

Annual Rate of Occurrence (ARO) is a probability indicating how many times this is expected in one year?

It is often difficult to put a monetary value that captures the full extent of impacts breaches of confidentiality, integrity or availability have businesses and individuals

Risk is often dependent on the business and organizational context

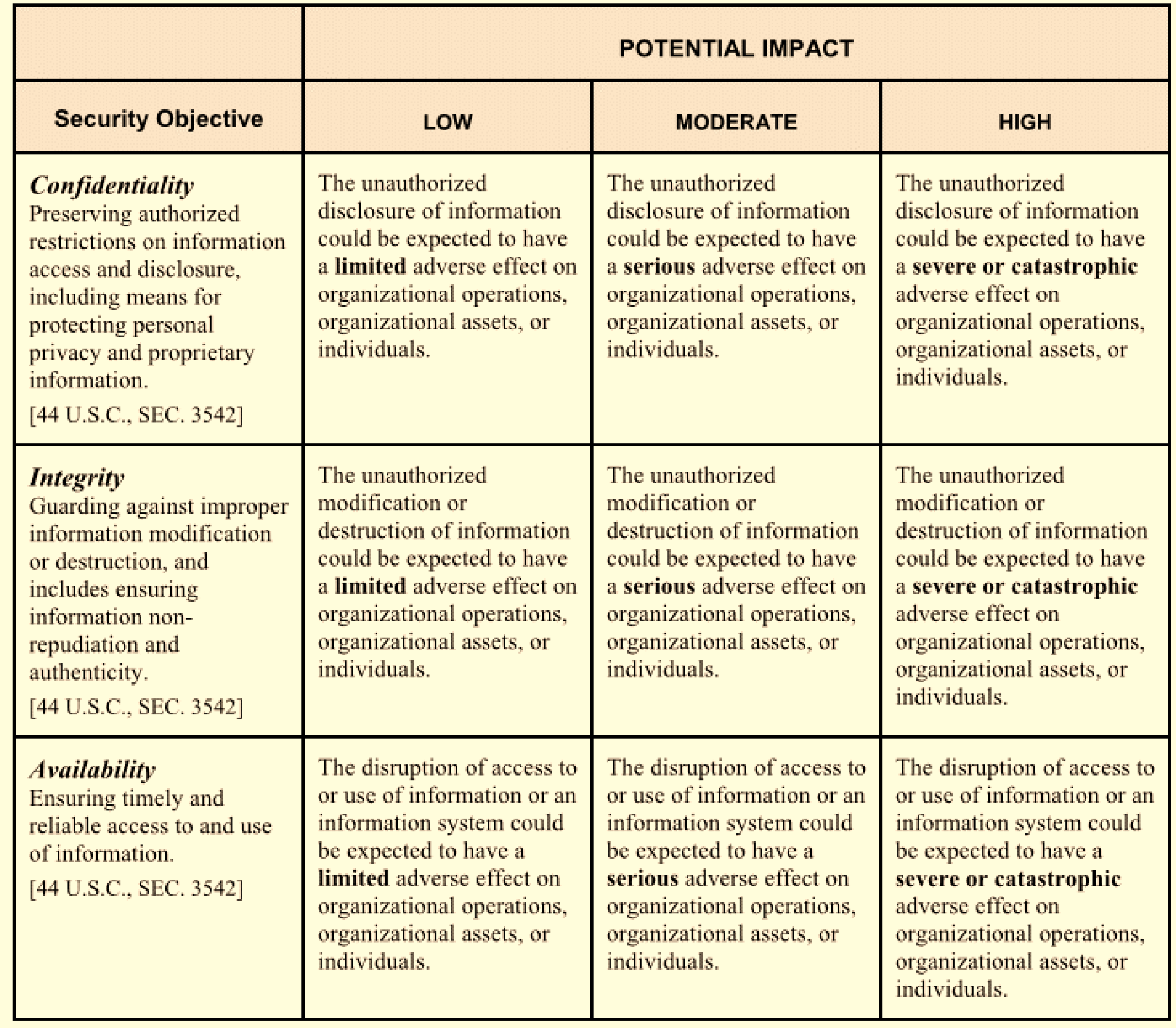
This is where qualitative measures of impact come in to help…



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems



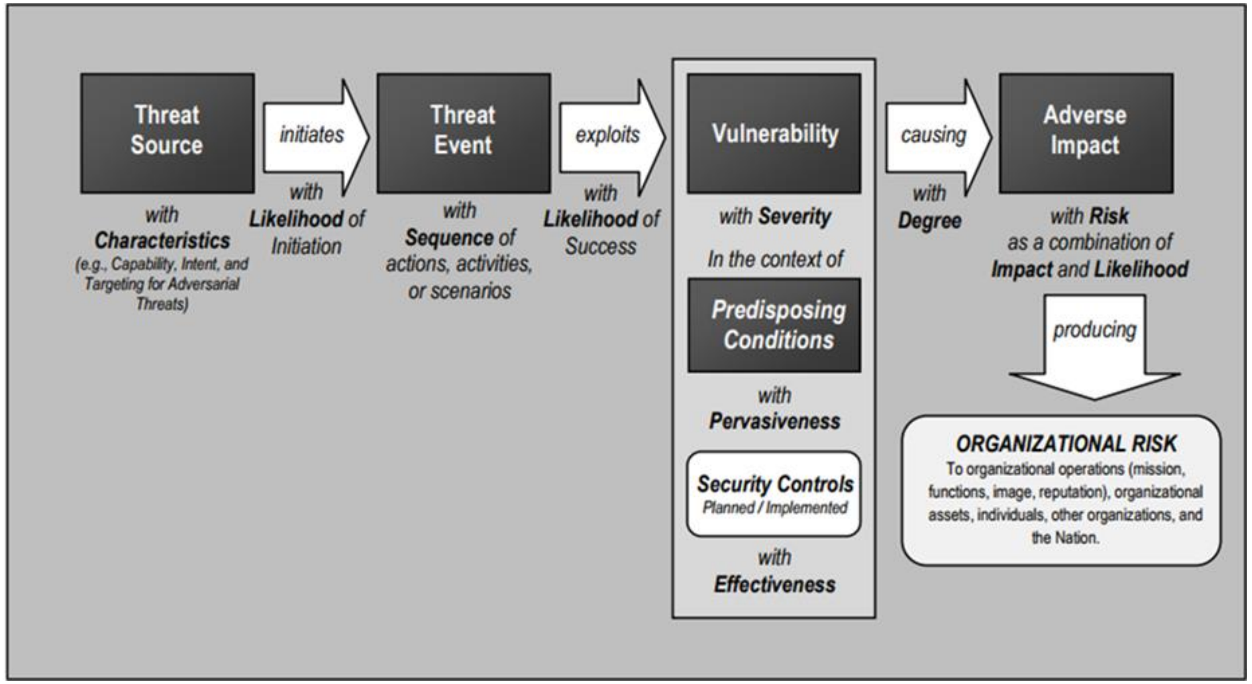
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Qualitative descriptions of elements of risk can be expressed in quantitative format…

Risk = Asset × Vulnerability × Threat

- An *asset* is a thing that we are trying to protect
- A *vulnerability* is a weakness or gap in our protection efforts
- A *threat* is what we're trying to protect against –
  - a *motivated attacker* with *specific methods* and *resources*

…and can also be described as causal sequences



Threat Source
with Characteristics (e.g., Capability, Intent, and Targeting for Adversarial Threats)
initiates
with Likelihood of Initiation
Threat Event
with Sequence of actions, activities, or scenarios
exploits
with Likelihood of Success
Vulnerability
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls
Planned / Implemented
with Effectiveness
causing
with Degree
Adverse Impact
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

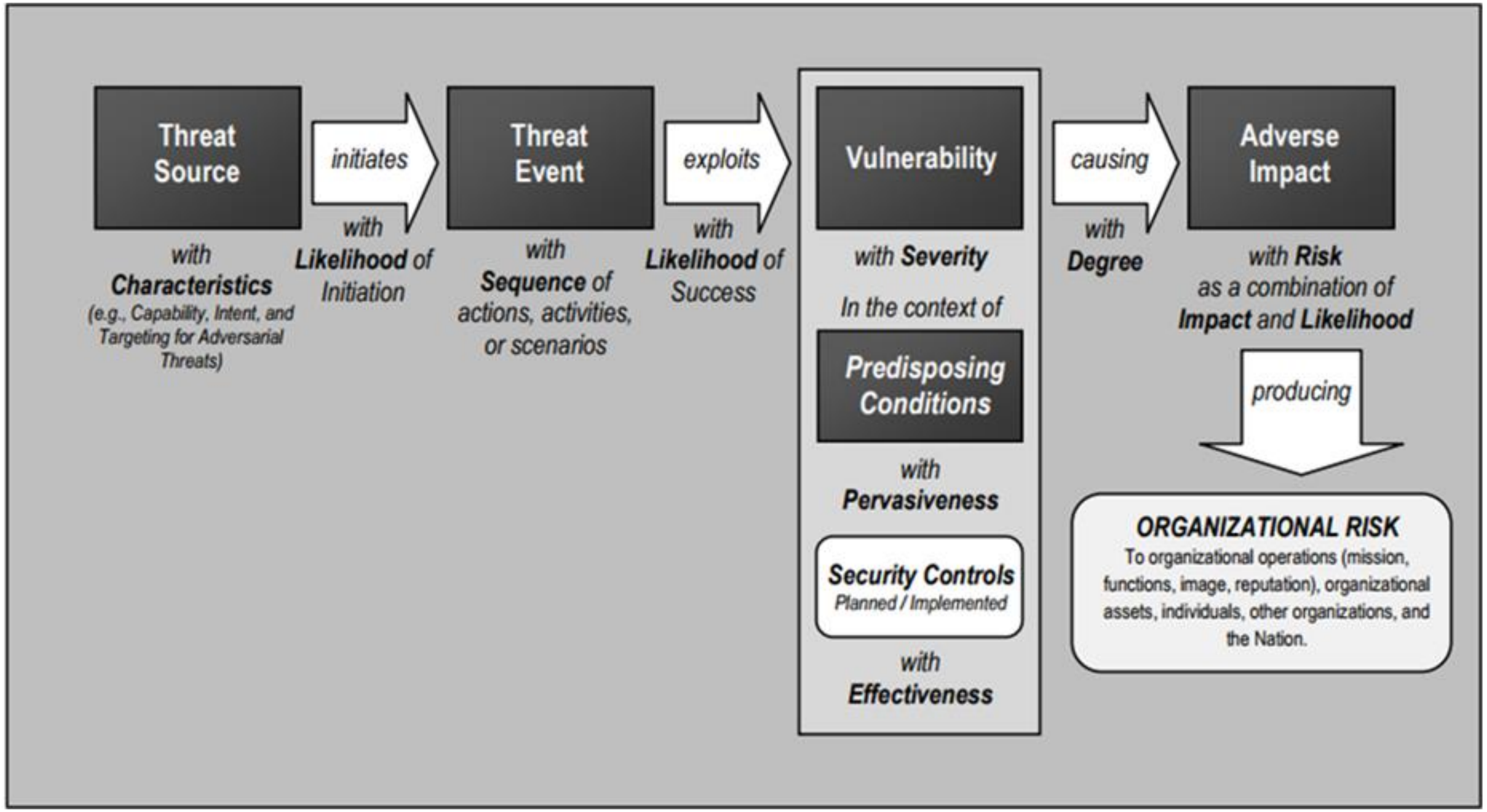
Agenda

- ✓Threat Environment
- ✓Cybersecurity Risk
- Threat Modeling
- Caution
- Next Week’s Assignments
- Next Week’s Quiz

Threat modeling helps us understand vulnerabilities and their relative importance to organizations

The most critical weaknesses can be prioritized for mitigation

assuring rational risk management investments to improve security


Threat Source
with Characteristics
(e.g., Capability, Intent, and Targeting for Adversarial Threats)
initiates
with Likelihood of Initiation
Threat Event
with Sequence of actions, activities, or scenarios
exploits
with Likelihood of Success
Vulnerability
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls
Planned / Implemented
with Effectiveness
causing
with Degree
Adverse Impact
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

Threat Modeling

The purpose of threat modeling is to provide defenders with a systematic analysis of what mitigations (i.e. controls or defenses) need to be included, based on the

- Assets most desired by an attacker
- Nature of the system
- Probable attacker's profile
- Most likely attack vectors

Threat modeling answers:

- *“What are the most relevant threats?”*
- *“Where am I most vulnerable to attack?”*
- *“What do I need to do to safeguard against these threats?”*

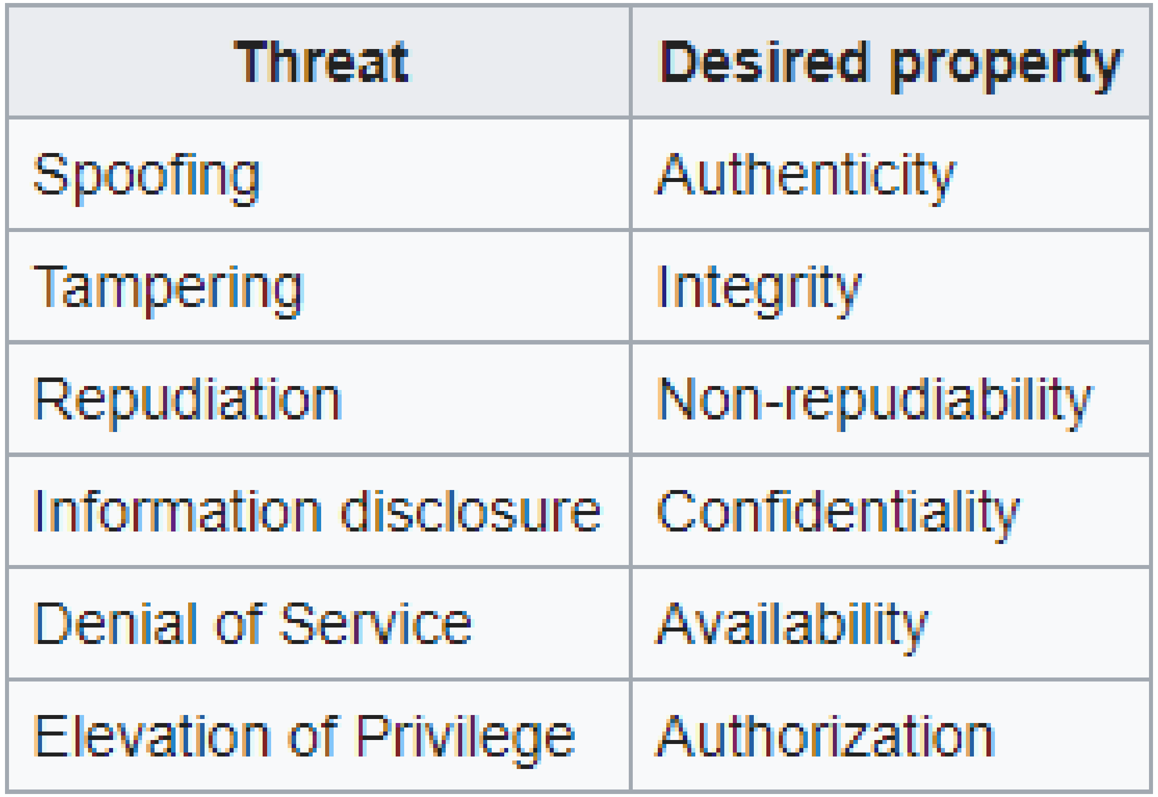
https://en.wikipedia.org/wiki/Threat_model

STRIDE

Threat modeling technique created by Microsoft, based 6 categories of threats:

- **Spoofing** – Can an attacker gain access using a false identity?
- **Tampering** – Can an attacker modify data as it flows through the system?
- **Repudiation** – If an attacker denies doing something, can we prove he/she did it?
- **Information disclosure** – Can an attacker gain access to private or potentially injurious data?
- **Denial of service** – Can an attacker crash or reduce the availability of the system?
- **Elevation of privilege** – Can an attacker assume the identify of a privileged user?

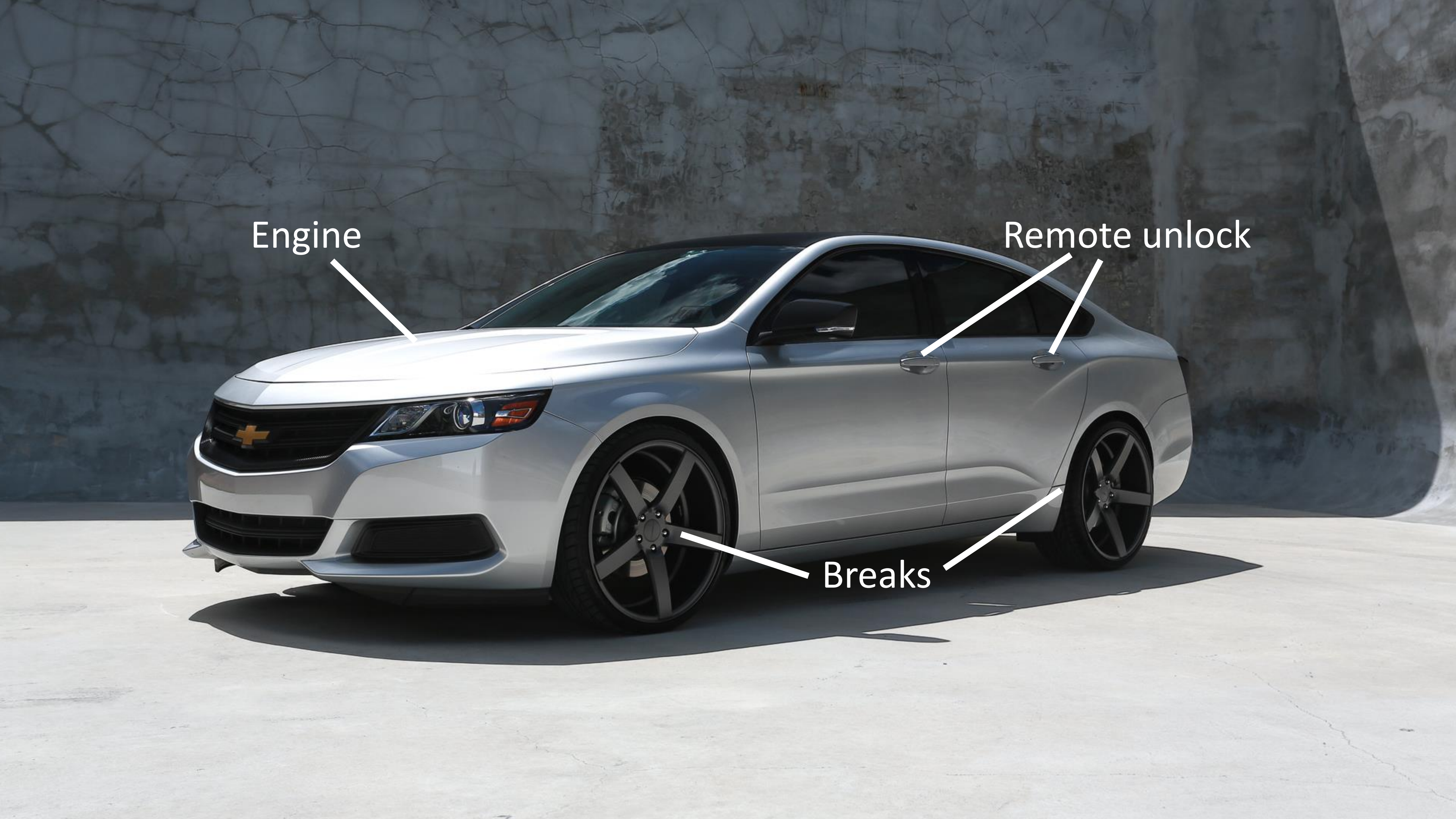
STRIDE threats and desired properties they impact



Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Modern Cars

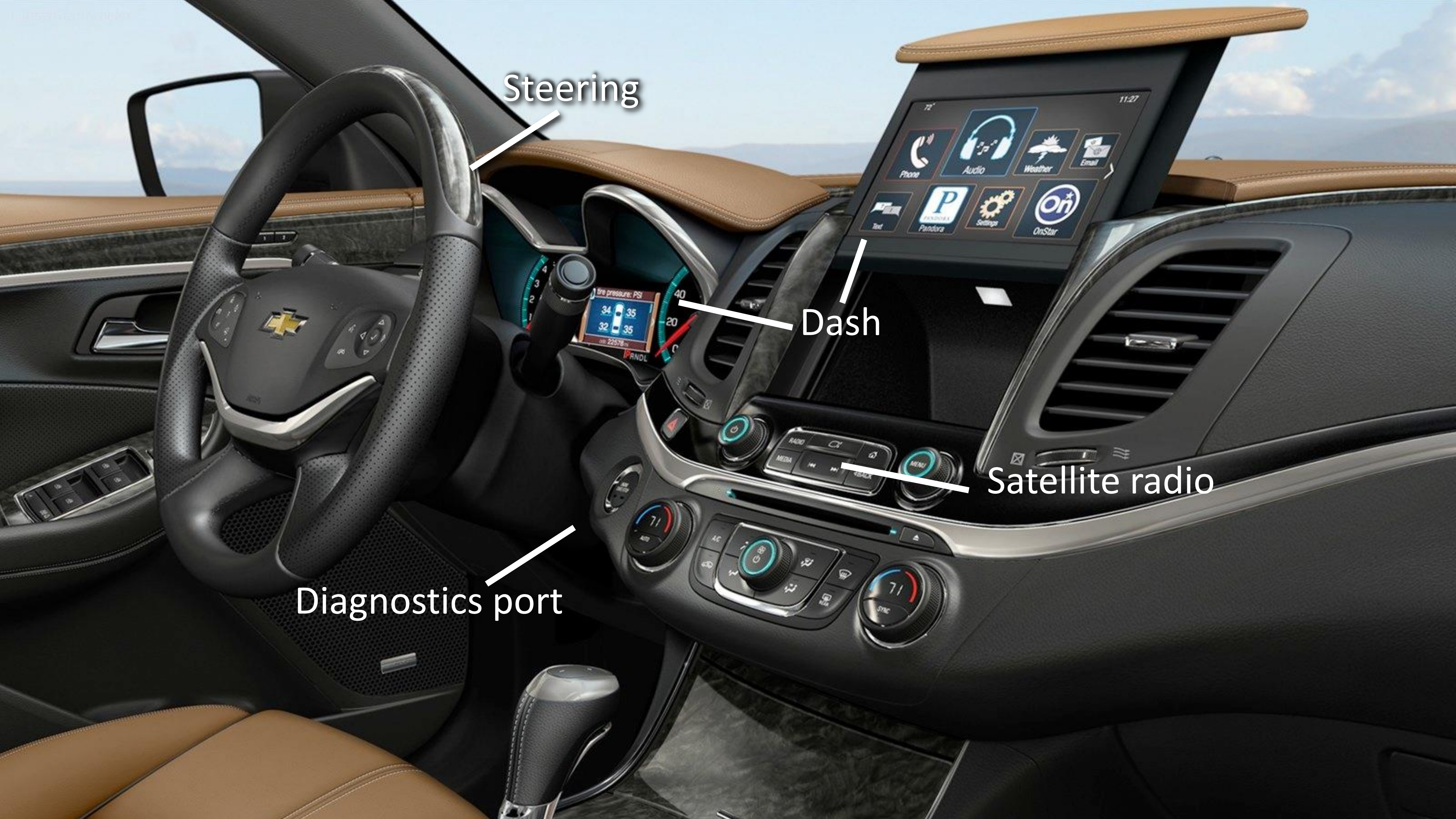
…are computer networks on wheels, with most have many computers that control various aspects of the car



Engine

Remote unlock

Breaks



Steering

Dash

Satellite radio

Diagnostics port

University of Washington Security Cards

A security threat brainstorming activity – Access Cards Here

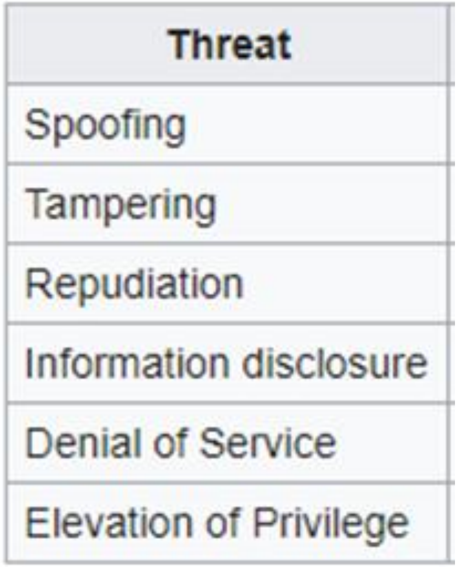
Break up into groups of 2:

- Pretend you are security professionals
  - A car company tasked you with thinking through the security implications of the modern car computer systems
- Start with the blue suit of cards ("Human Impact"), consider what impacts to people would result if an attacker misused modern car systems like the attack you just witnessed
  - Either think about one car, or think about the entire car product line
  - Rank order the cards from most relevant
  - Explain your 3 top choices

STRIDE Threat Modeling

A security threat brainstorming activity

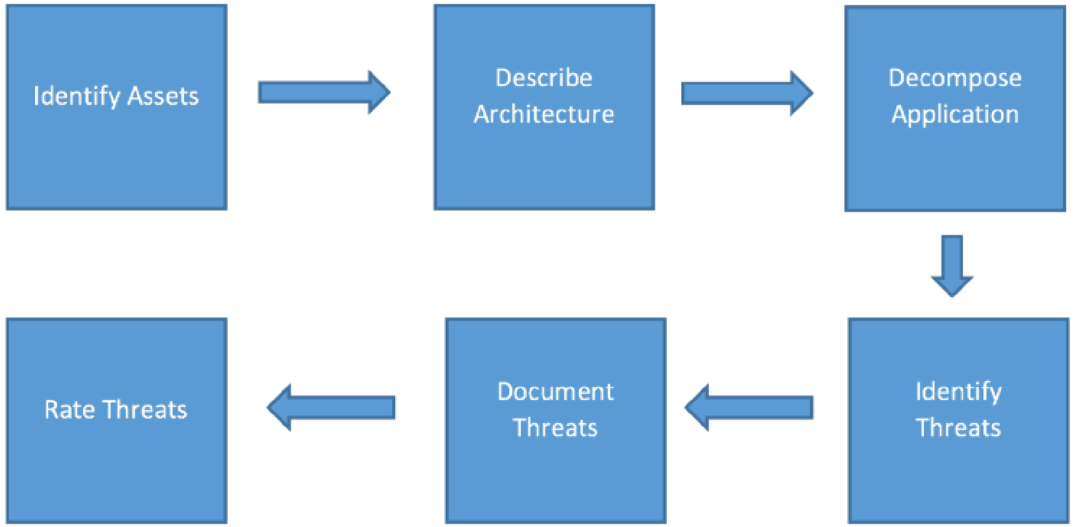
- Set aside the UW Security Cards, and use the STRIDE model
- Consider what methods adversaries might use for attacking modern car systems
  - Either think about one car, or think about the entire car product line
  - Rank order the threats from most relevant
  - Explain your 3 top choices

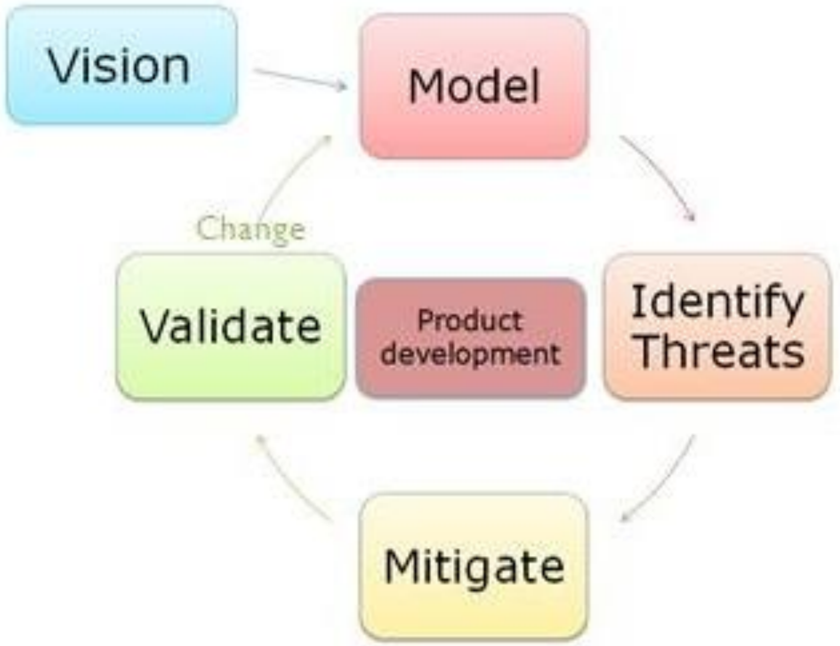


Threat
Spoofing
Tampering
Repudiation
Information disclosure
Denial of Service
Elevation of Privilege

Threat Modeling

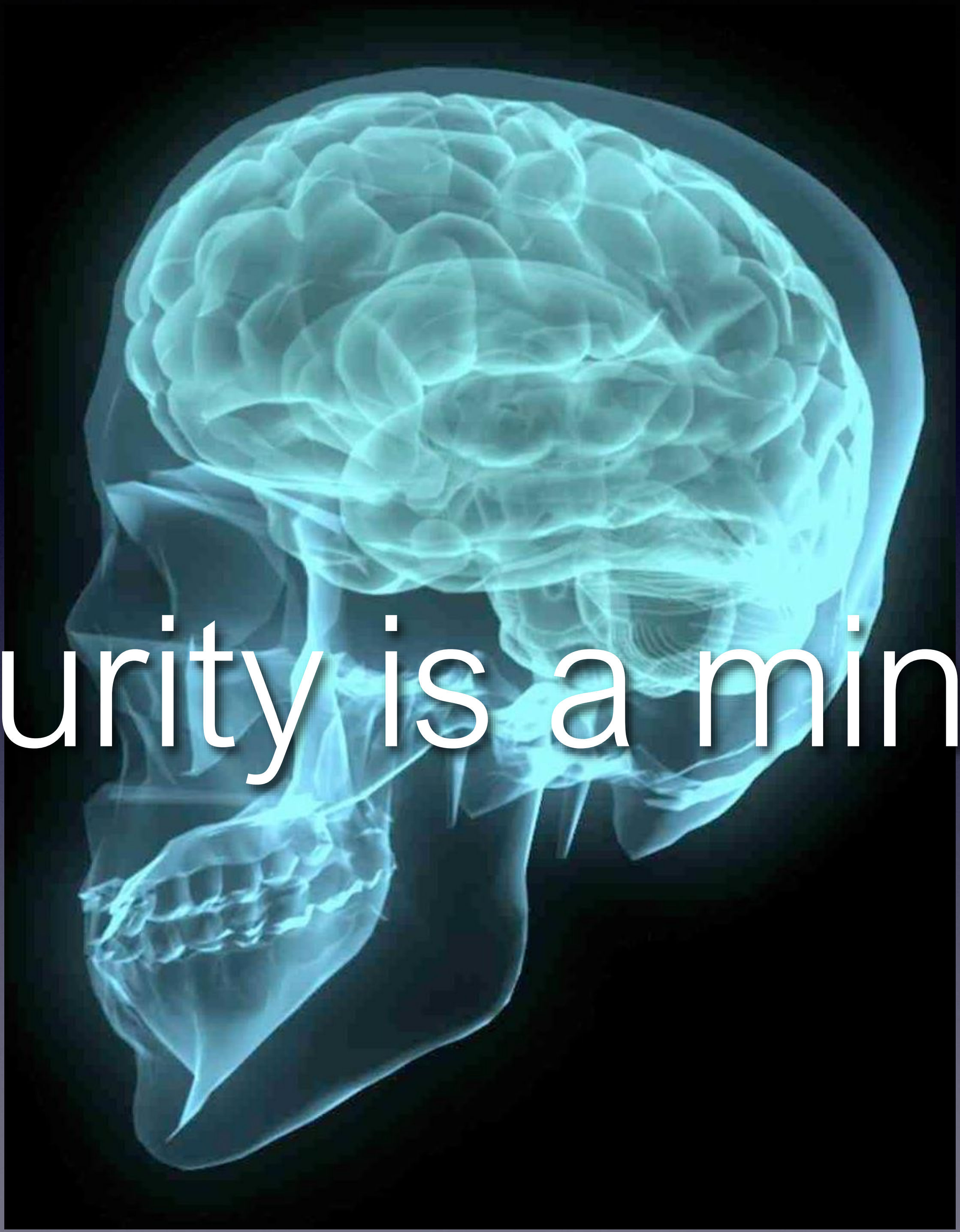
- Can be a full-time job for cyber security professionals
- Is now a skill information systems designers, developers and architects need to have





Agenda

- ✓Threat Environment
- ✓Cybersecurity Risk
- ✓Threat Modeling
- Security Mindset / Next Week’s Quiz



Security is a mindset

Next Week's Activity

At the start of next class, I will give you five minutes to write out the first 100 digits of pi, from memory, on a sheet of paper

- When time is up, you will show the paper to me
- I will not make you clear your desk, but you will need to close your laptop and put your phone face down on the table or away in your bag or pocket
- I do not expect you to actually memorize the digits of pi—**<u>I want you to cheat</u>**.
- How you choose to cheat is entirely up to you. However, I will observe you. If you are caught cheating, you will fail the quiz. Collaborative cheating is also allowed, but everyone involved will fail the quiz if caught.
- The class will vote on the most creative and effective cheating technique.
- The objective of the exercise is to learn how an adversary thinks and operates by deliberately loosening traditional academic rules and tapping personal creativity. To avoid any misunderstanding, this exception to the traditional ban on cheating only applies to this quiz and not to other graded assignments in the course. **<u>Cheating outside of this quiz will not be tolerated.</u>**

Goal: Help you develop a <u>Security Mindset</u>

Agenda

✓Threat Environment

✓Cybersecurity Risk

✓Threat Modeling

✓Next Week’s Quiz