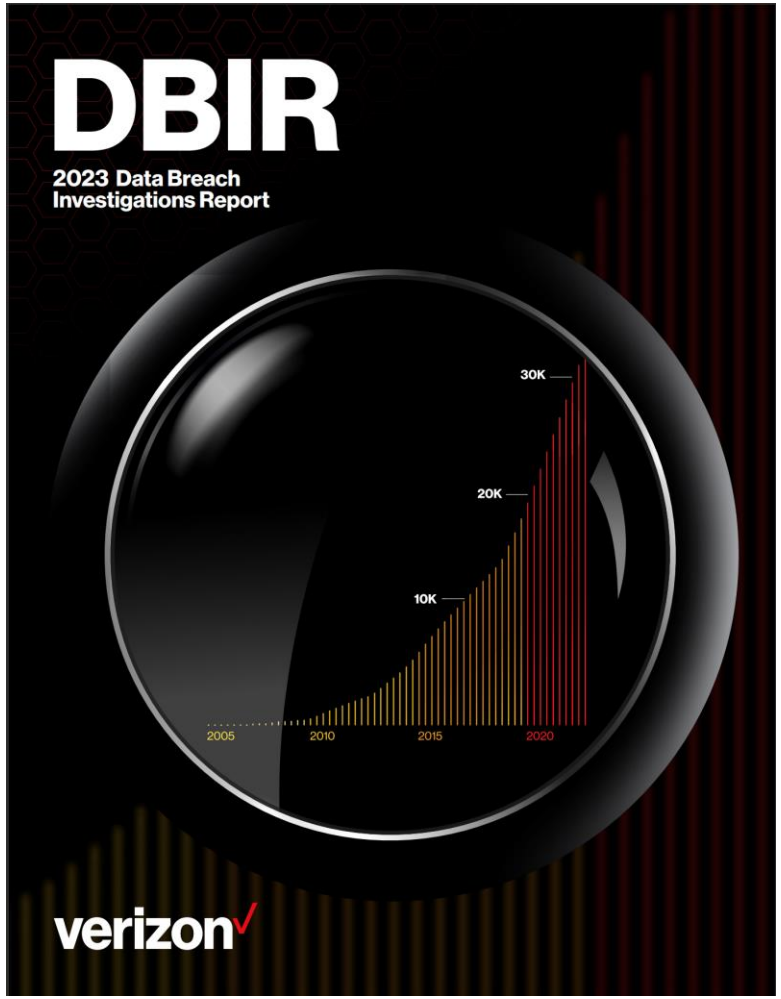
Information Systems Integration
MIS 4596

Class 2

Agenda

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

Threat Environment



	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

Based on analysis of 16,312 security incidents, of which 5,199 were confirmed data breaches

Threat Environment

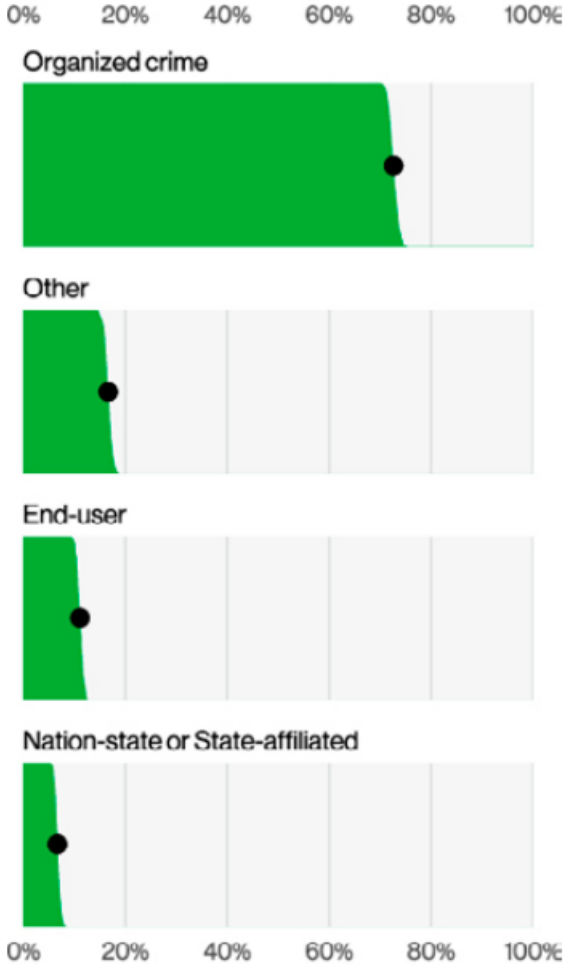


Figure 13. Threat actor Varieties in breaches (n=2,489)

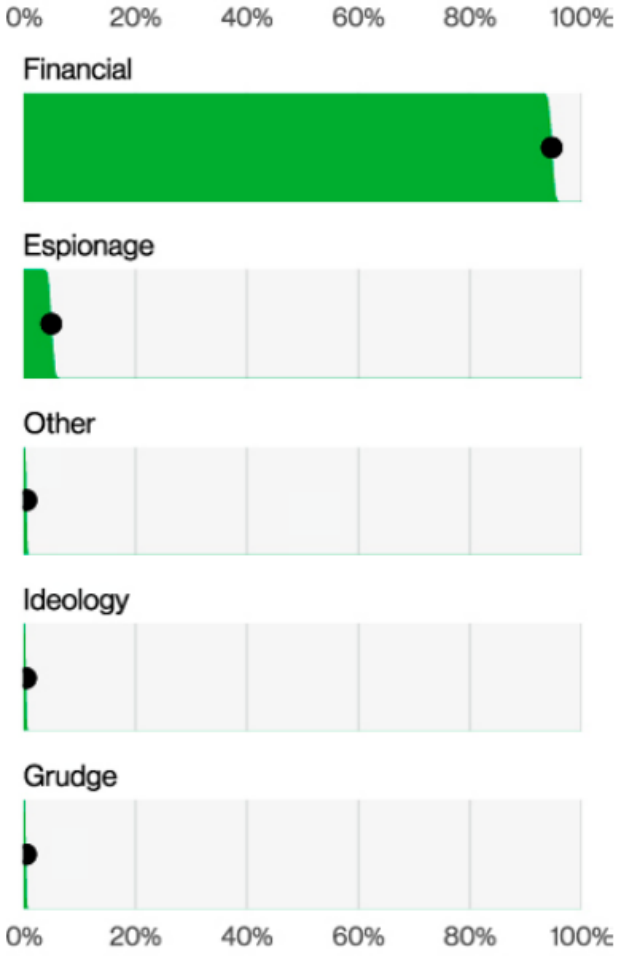


Figure 12. Threat actor Motives in breaches (n=2,328)

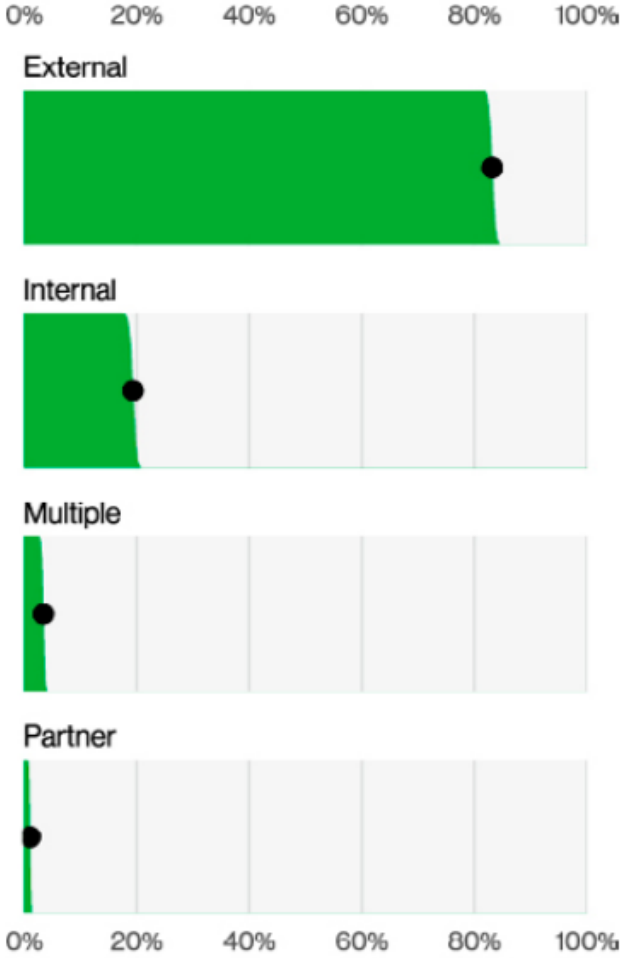
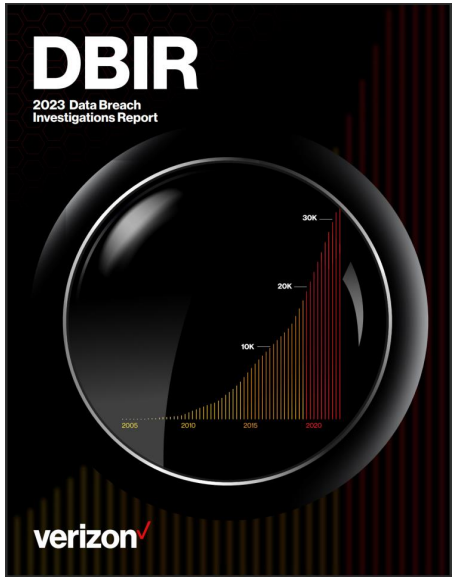


Figure 11. Threat actors in breaches (n=5,177)



Threat Environment

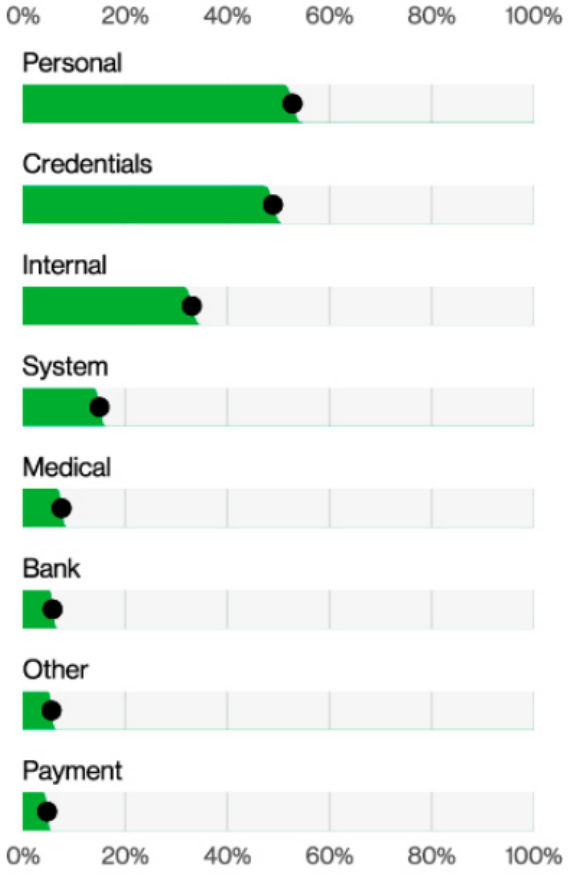
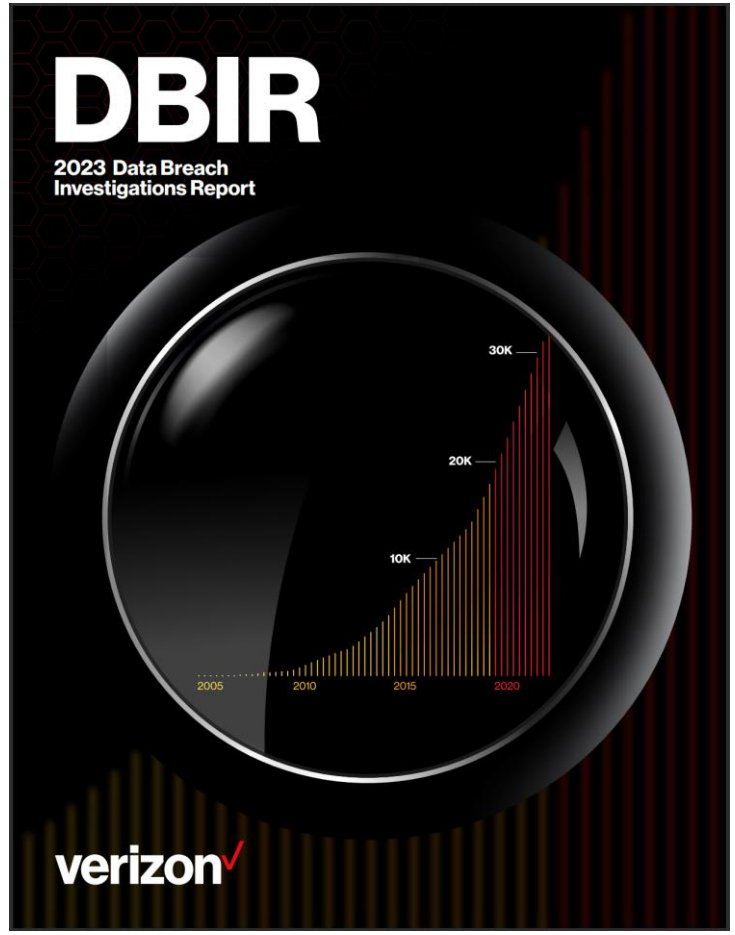


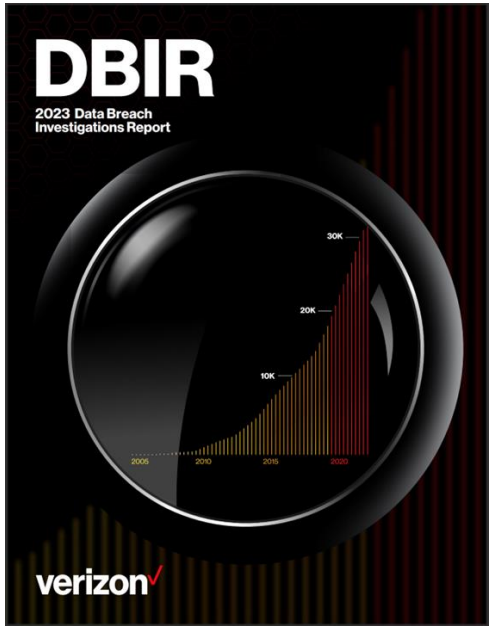
Figure 21. Top Confidentiality data varieties in breaches (n=5,010)

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

Figure 14. Top Action varieties in breaches (n=4,354)



Threat Environment



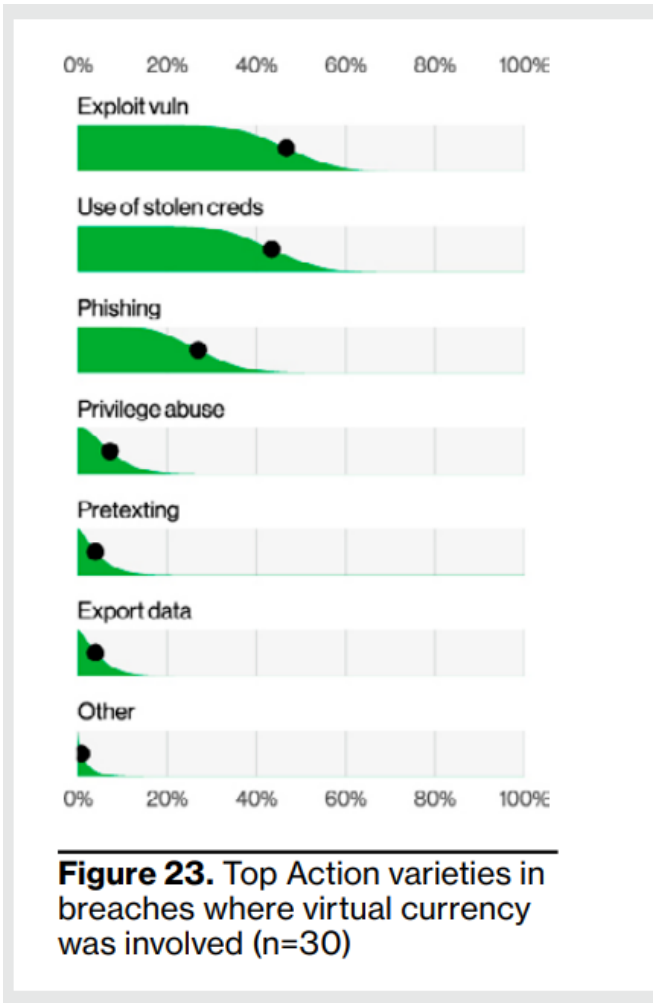


Figure 23. Top Action varieties in breaches where virtual currency was involved (n=30)

Figure 24. Top Action vectors in breaches where virtual currency was involved (n=48)

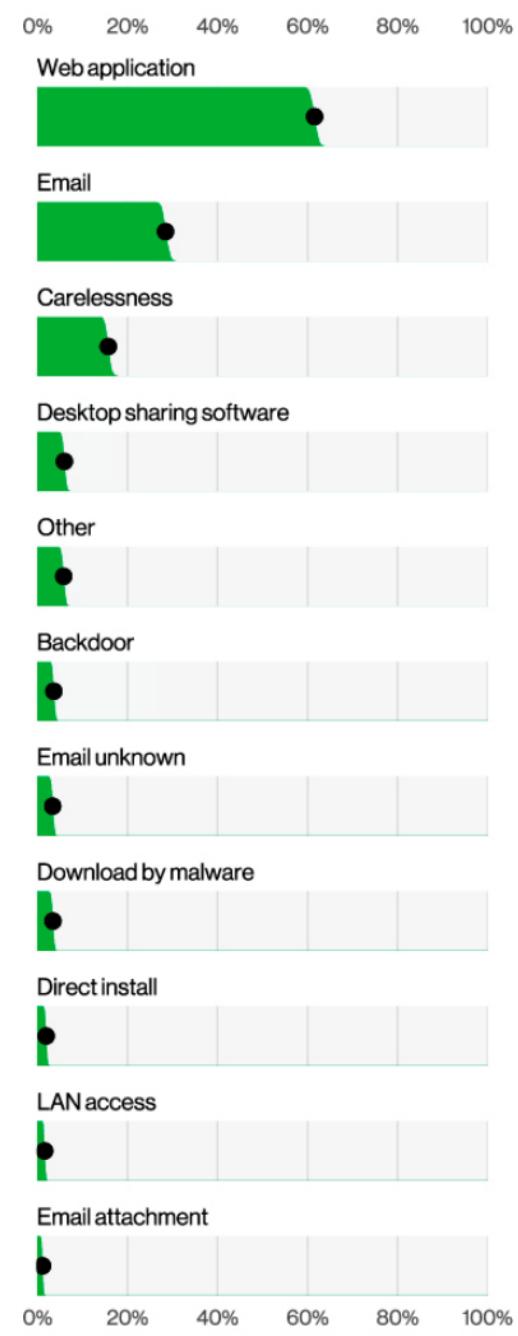
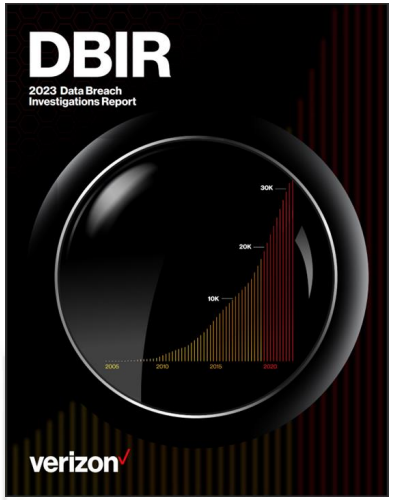


Figure 16. Top Action vectors in breaches (n=3,194)

Threat Environment



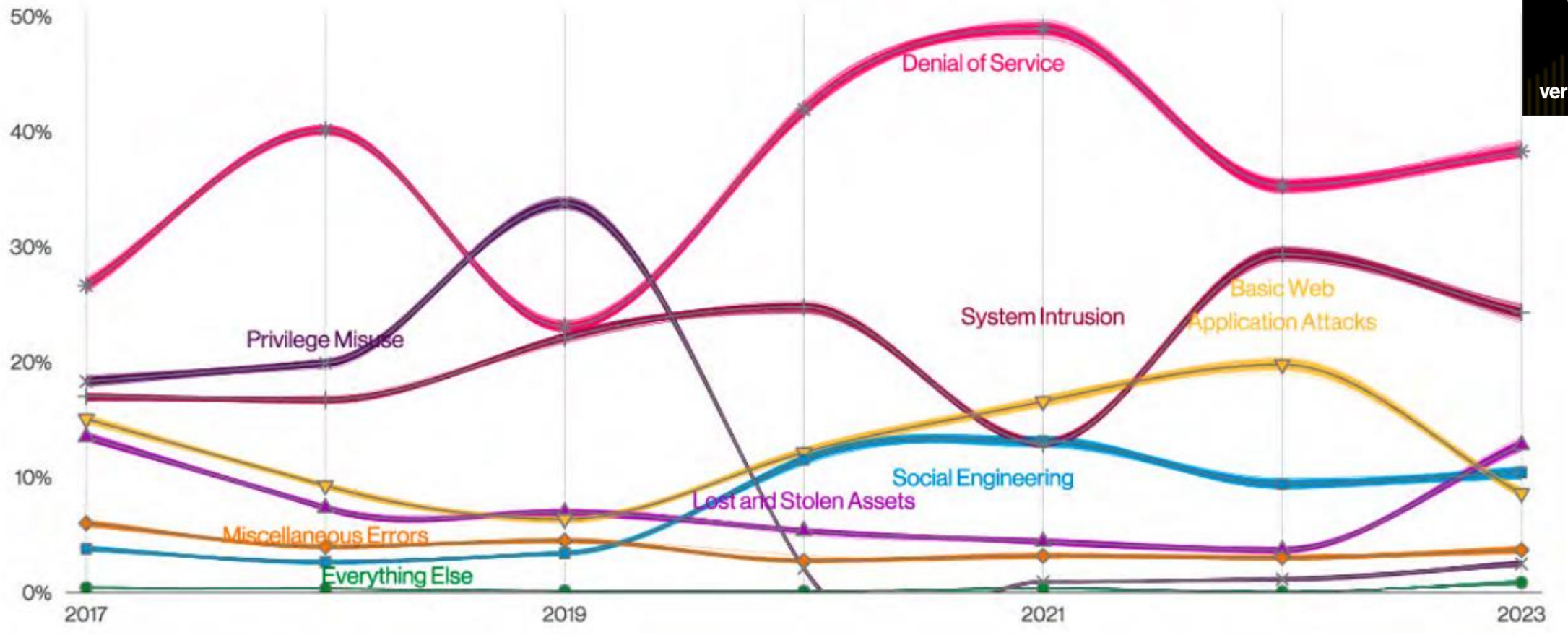
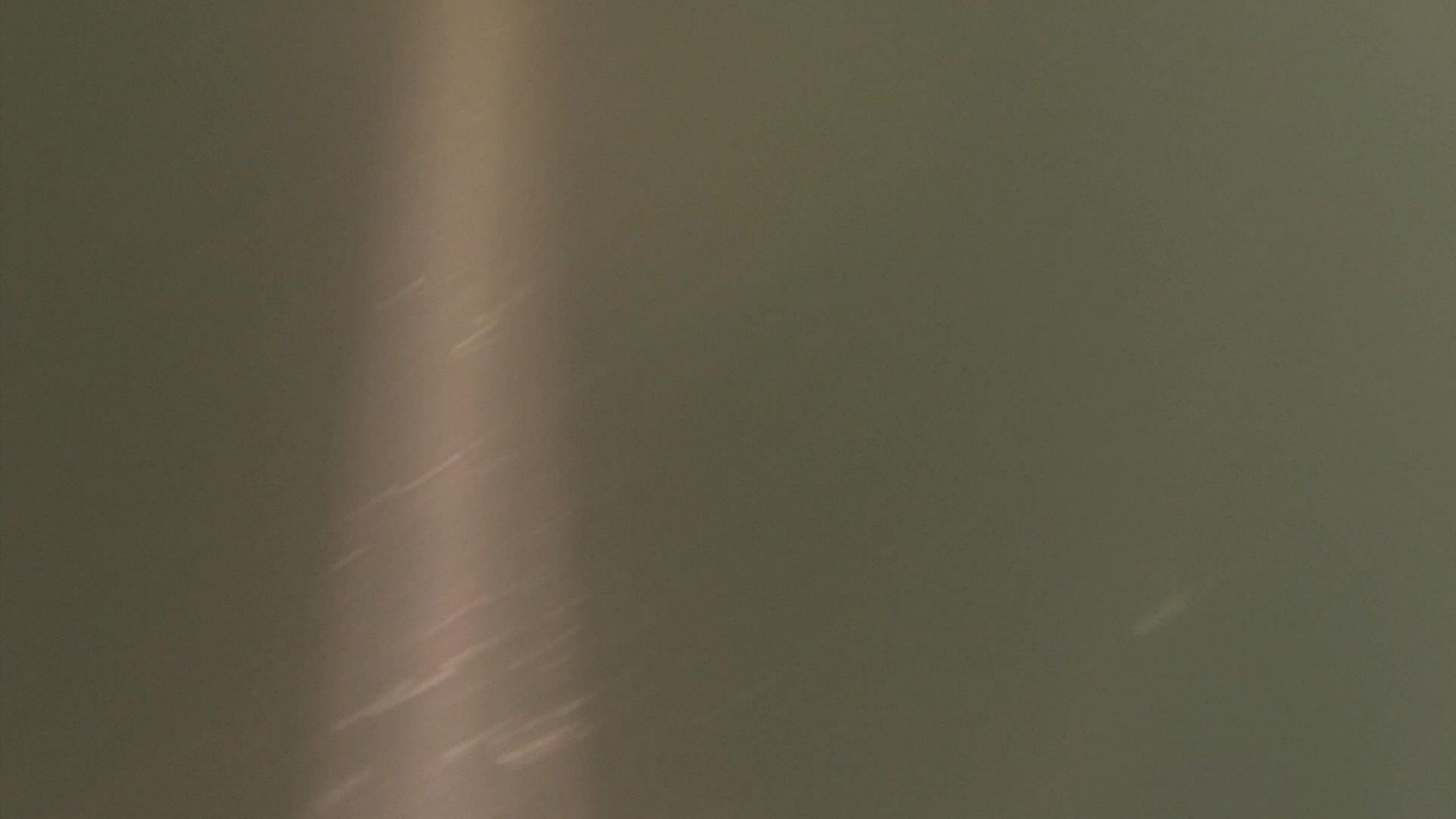


Figure 25. Patterns over time in incidents


Is this computer
100% secure?

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

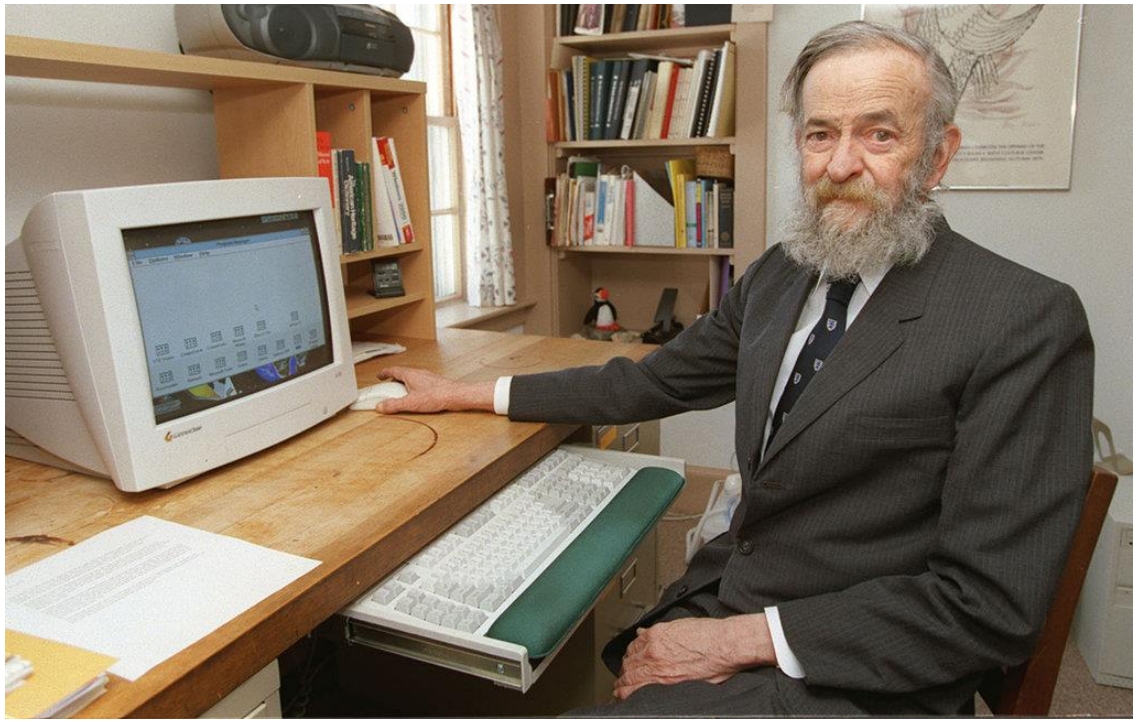


How can we make a computer 100% secure?

3 Golden Rules to ensure computer security:

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

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



Robert Morris

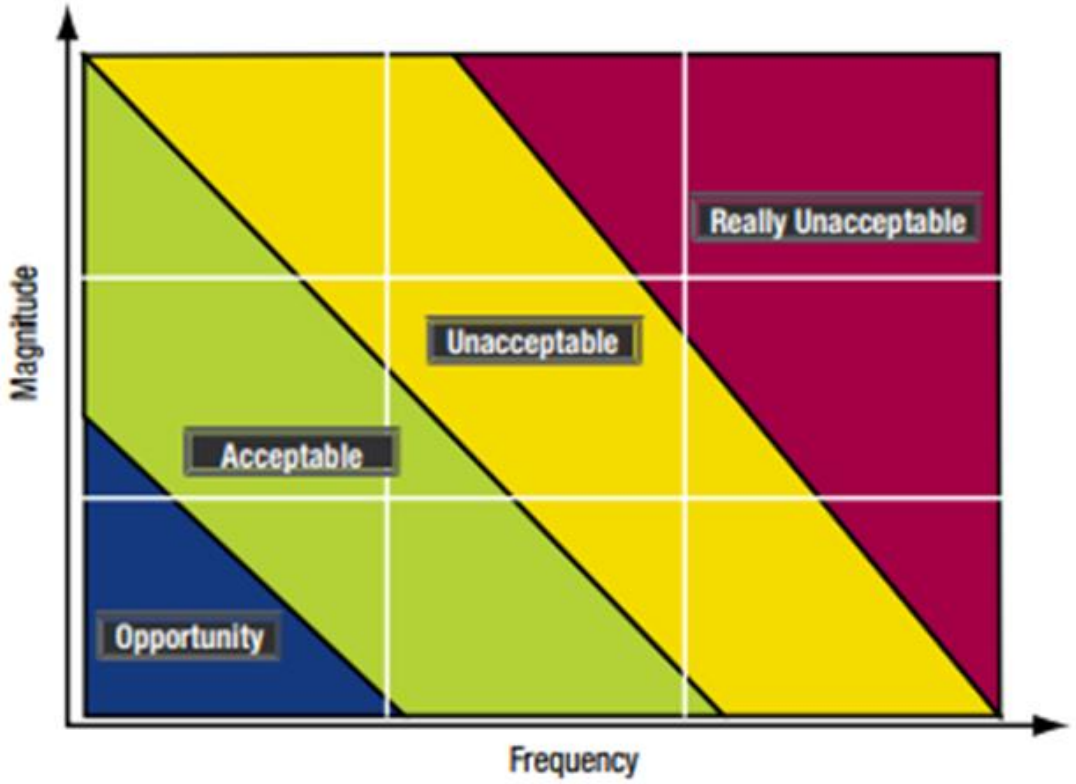
Chief Scientist, National Security Agency's (NSA) National Computer Security Center, 1986-1994

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 threat event 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

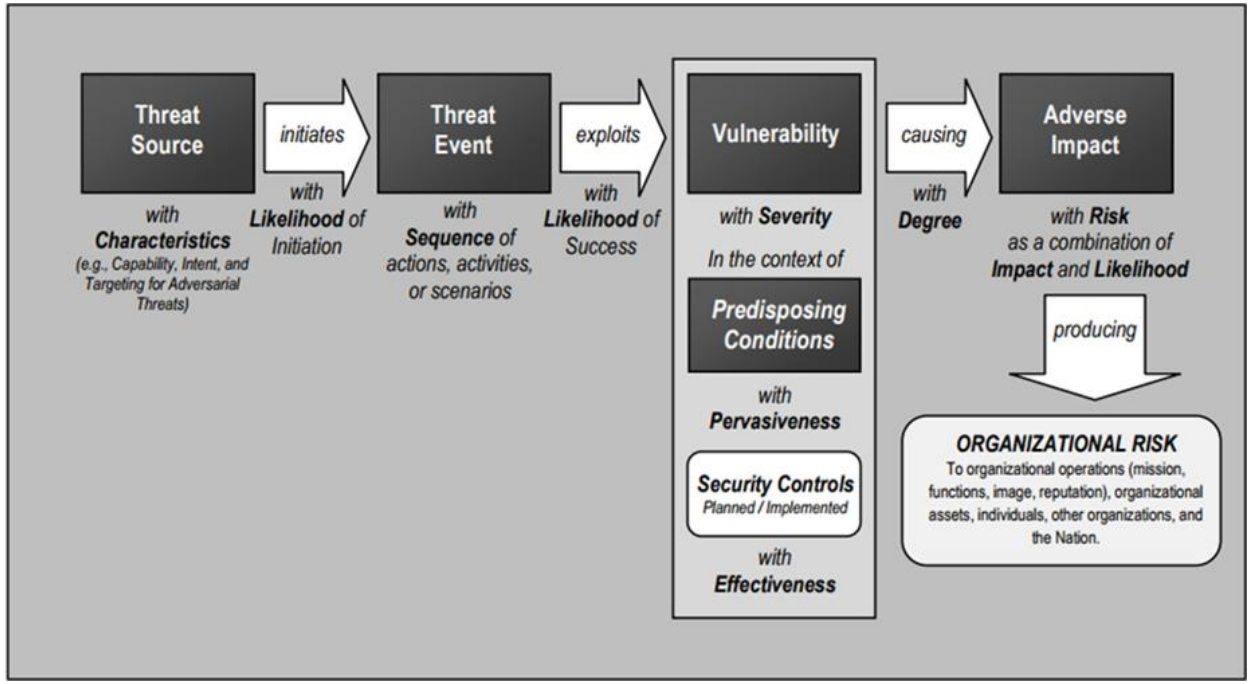
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could 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



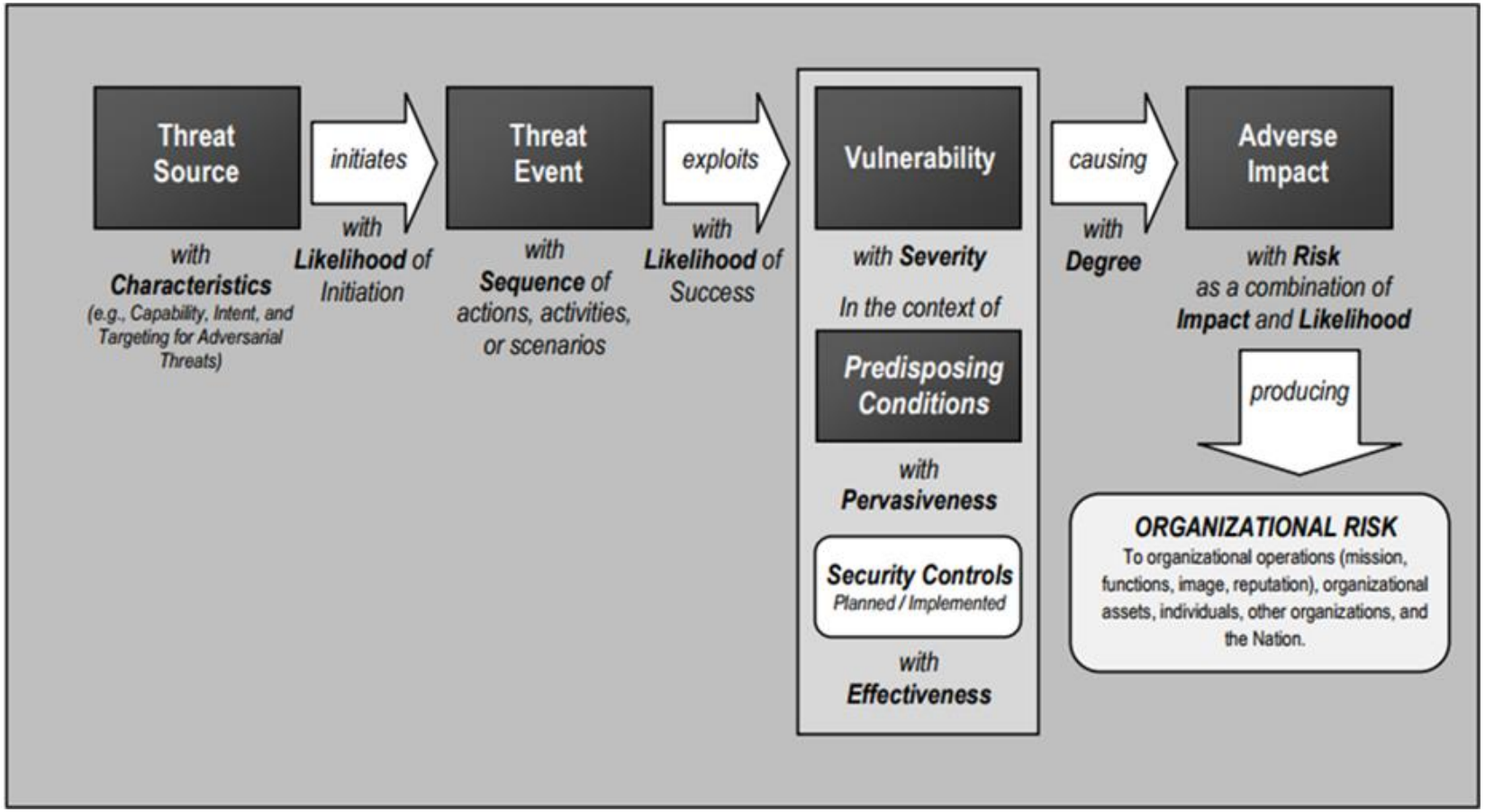
Agenda

- ✓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 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:

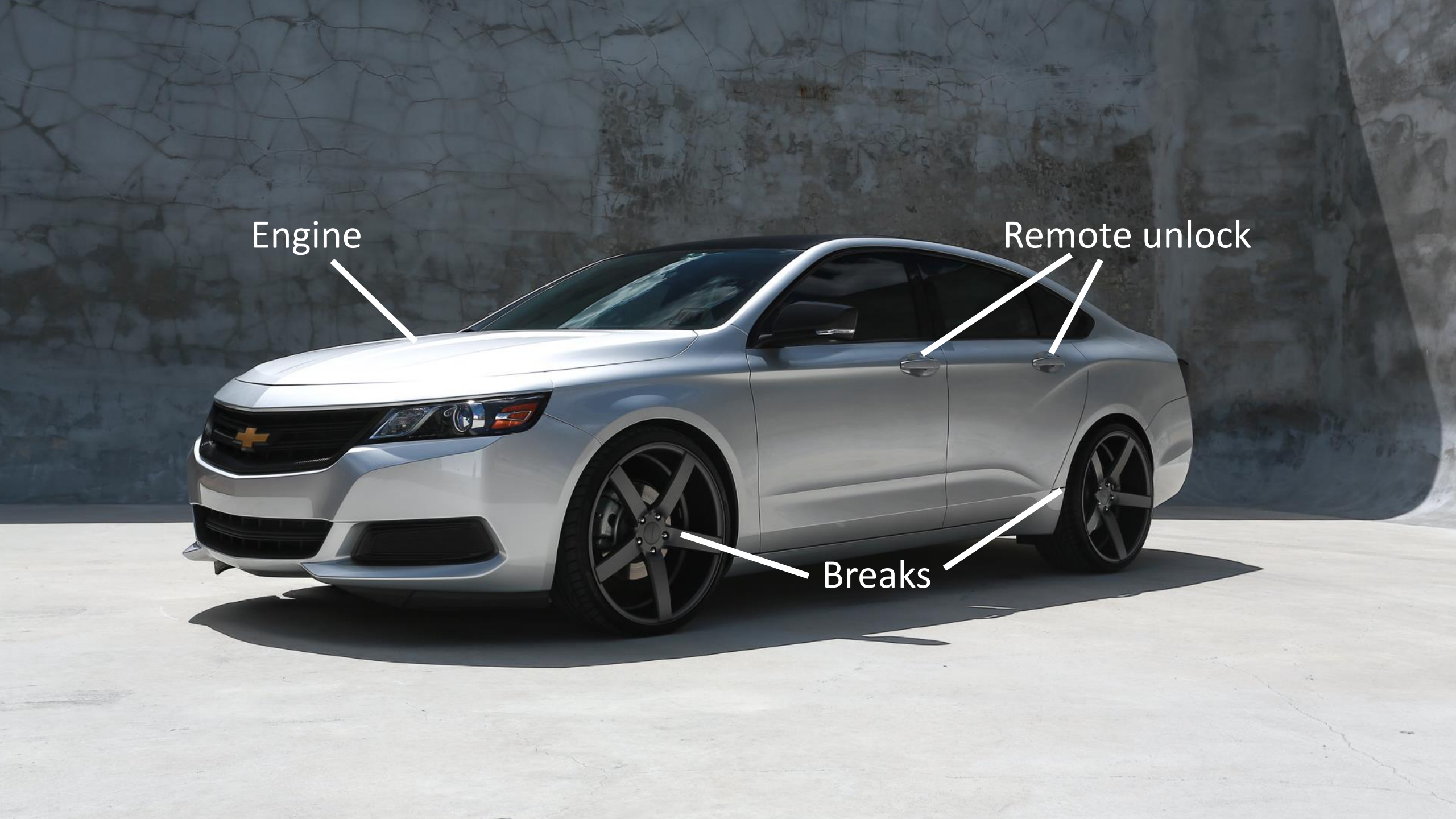
- **Spoofing** – Can an attacker gain access using a false identity?
- **Tampering** – Can an attacker modify data as it flows through the system?
- **Repudiation** – If an attacker denies doing something, can we prove he/she did it?
- **Information disclosure** – Can an attacker gain access to private 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

- https://community.mis.temple.edu/mis4596sec001spring2023/files/2021/08/Exercise-ThreatModeling-cards-deck.pdf

STRIDE Threat Modeling

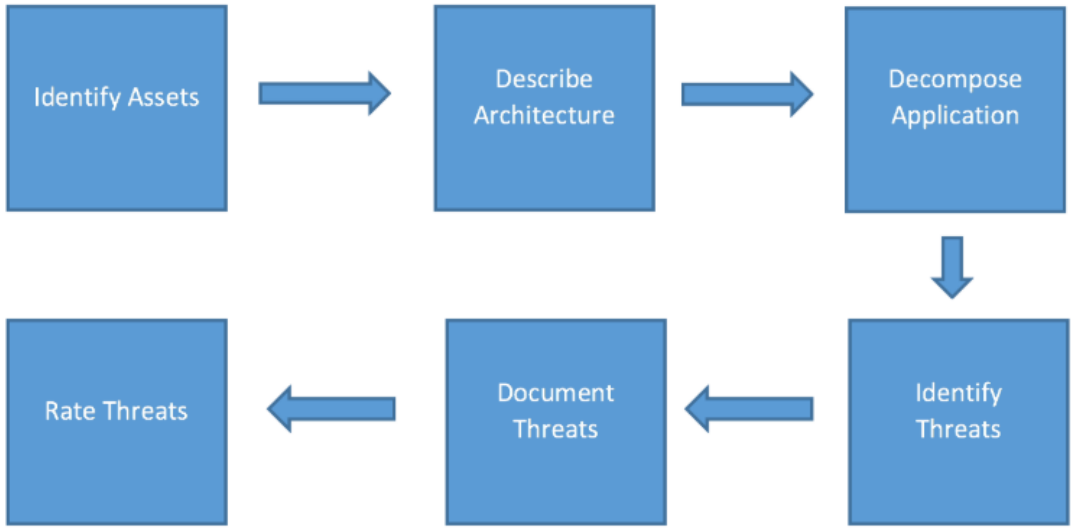
A security threat brainstorming activity

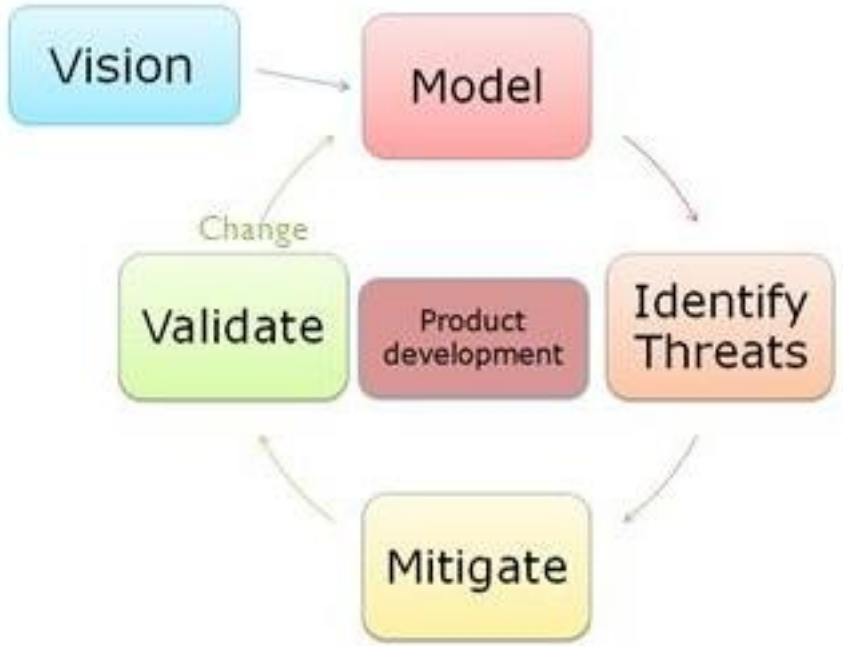
- Set aside the UW Security Cards, and use the STRIDE model
- Consider what methods adversaries might use for attacking modern car systems
  - Either think about one car, or think about the entire car product line
  - Rank order the threats from most relevant
  - Explain your 3 top choices

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



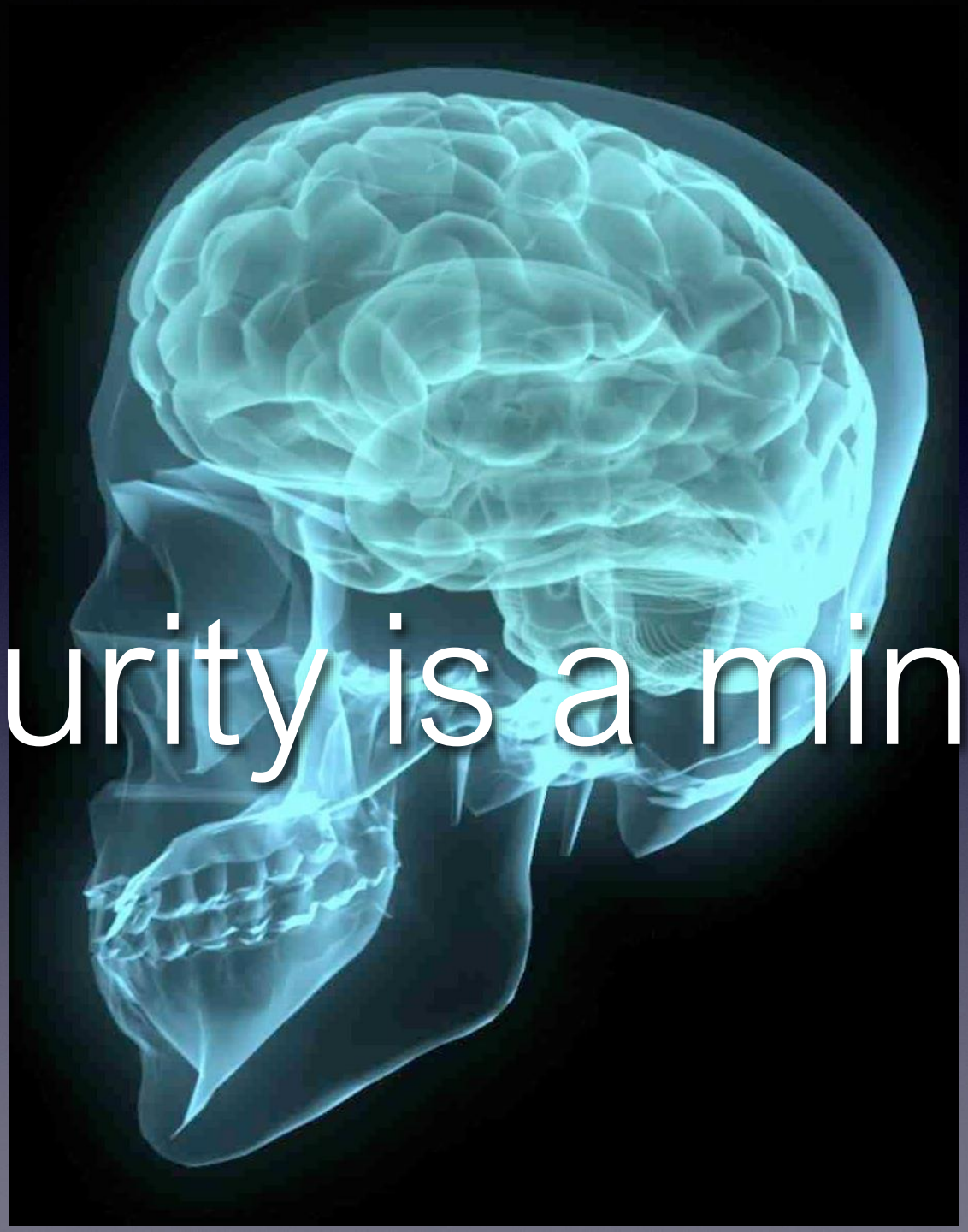


Agenda

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

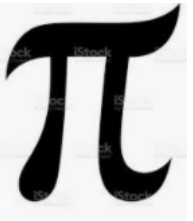
Caution

- The tools and techniques discussed and used in this course should only be used on systems you personally own or have written permission to use.
- Some of the tools used have the potential to disrupt or break computer systems.



Security is a mindset

Next Week's Quiz



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—**I want you to cheat**.
- How you choose to cheat is entirely up to you. However, I will observe you in Zoom via your camera. 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. **Cheating outside of this quiz will not be tolerated.**

Goal: Help you develop a Security Mindset

Agenda

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

Agenda

- ✓Threat Environment
- ✓Cybersecurity Risk
- ✓Threat Modeling
- ✓Caution
- ✓Next Week's Assignments
- ✓Next Week's Quiz
- ➢2 extra threat modeling activities… if there is time

University of Washington Security Cards

A security threat brainstorming activity

- Next move onto the **orange** “Adversary Motivation” suit
- Consider what motivations adversaries might have for attacking modern car systems
  - Either think about one car, or think about the entire car product line
  - Rank order the adversary motivations from most relevant to least
  - Explain your 3 top choices

University of Washington (UW) Security Cards

A security threat brainstorming activity

- Next move onto the red “Adversary’s Resources” suit
- Consider what resources adversaries might have for attacking modern car systems
  - 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