Photo by Andri from Pexels
https://is.gd/mhNM9G

System Administration

Week 11, Segment 2
System Security II: Defining a Threat Model

Department of Computer Science
Stevens Institute of Technology

Jan Schaumann
jschauma@stevens.edu
https://stevens.netmeister.org/615/

Threat Model

For each system/component/product/service/…

- identify *what* you're protecting
- identify *from whom* you're protecting it
  - identify *goals* of the attacker
  - identify *motivation* of the attacker
  - identify *capabilities* of the attacker
- identify threats you *cannot* defend against

Threat Model 101

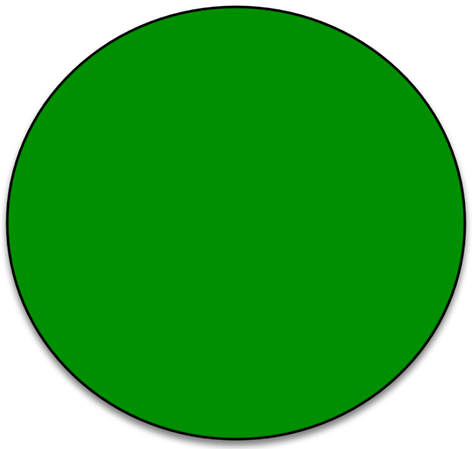
By James Mickens

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	◆ Magical amulets? ◆ Fake your own death, move into a submarine? ◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models

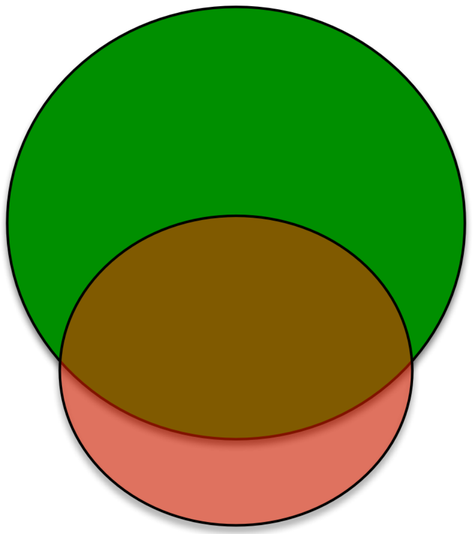
https://www.usenix.org/system/files/1401_08-12_mickens.pdf

Threats you know about.



Threats you know about.

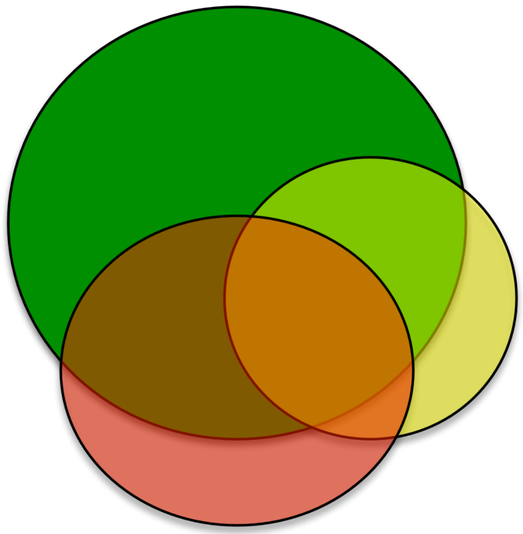
Threats you care about.



Threats you know about.

Threats you can defend against.

Threats you care about.

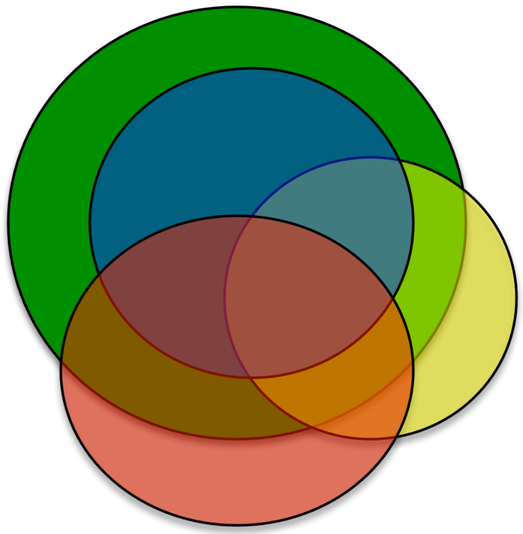


Threats you know about.

Threats you can defend against.

Threats you care about.

Threats you decided to defend against.

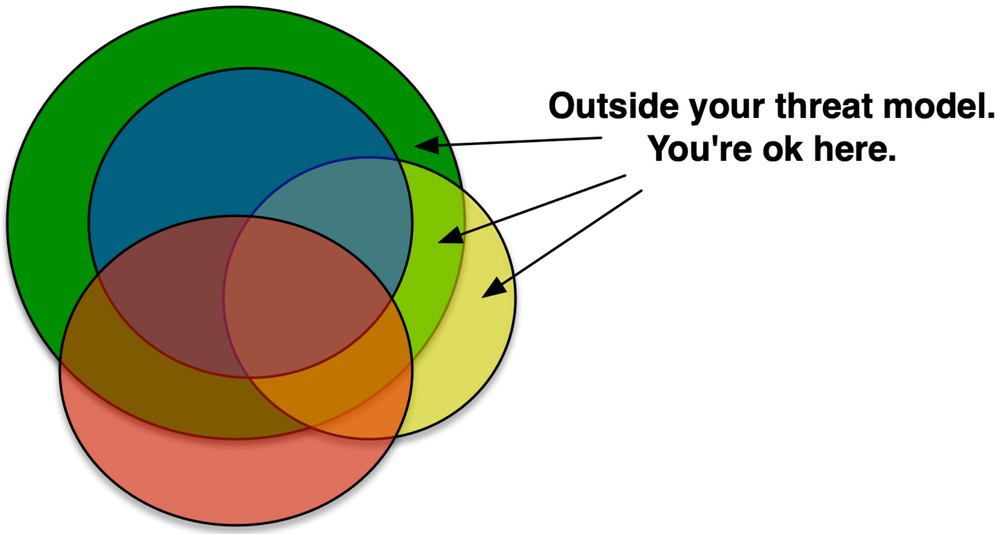


Threats you know about.

Threats you can defend against.

Threats you care about.

Threats you decided to defend against.

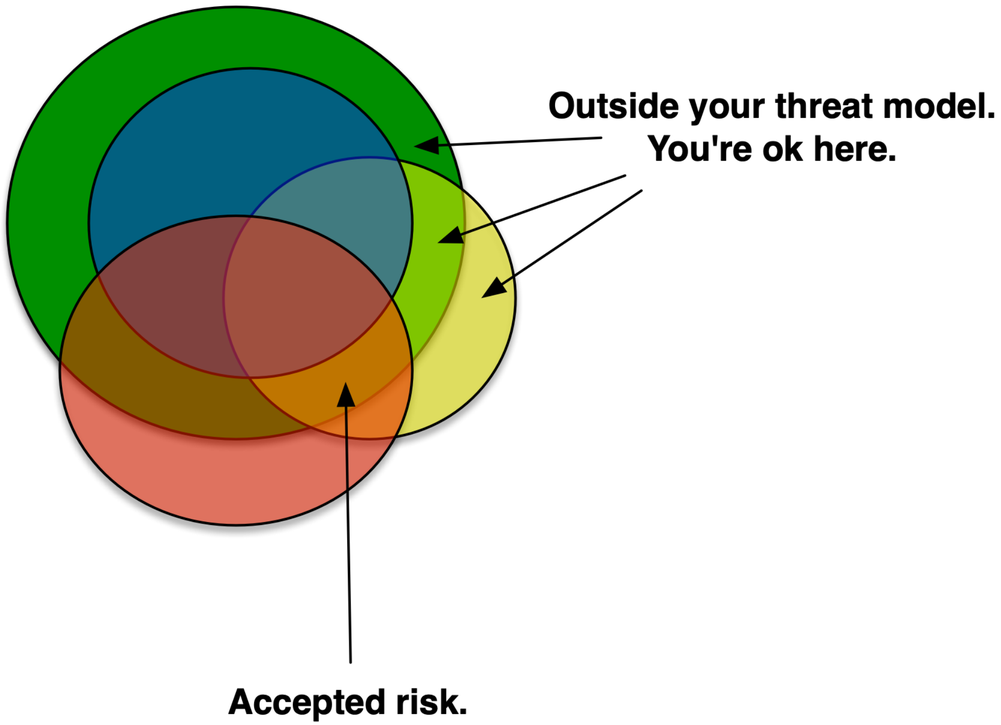


Threats you know about.

Threats you can defend against.

Threats you care about.

Threats you decided to defend against.

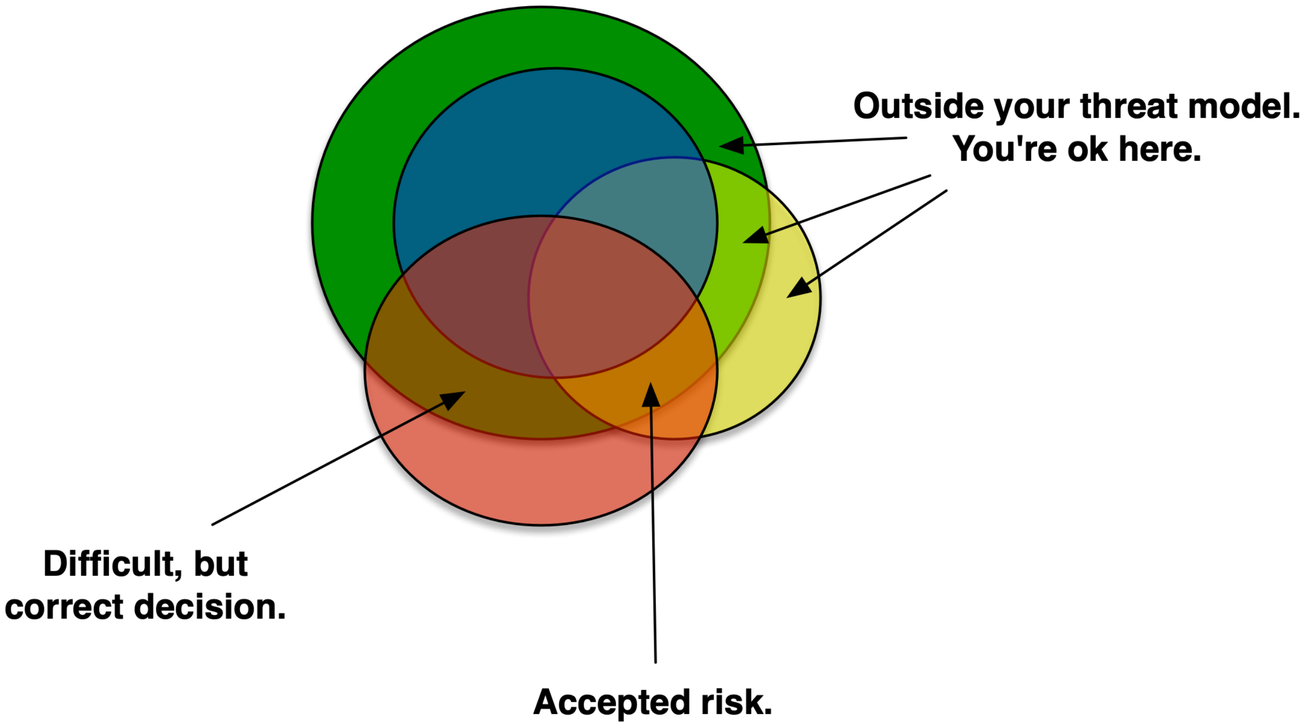


Threats you know about.

Threats you can defend against.

Threats you care about.

Threats you decided to defend against.

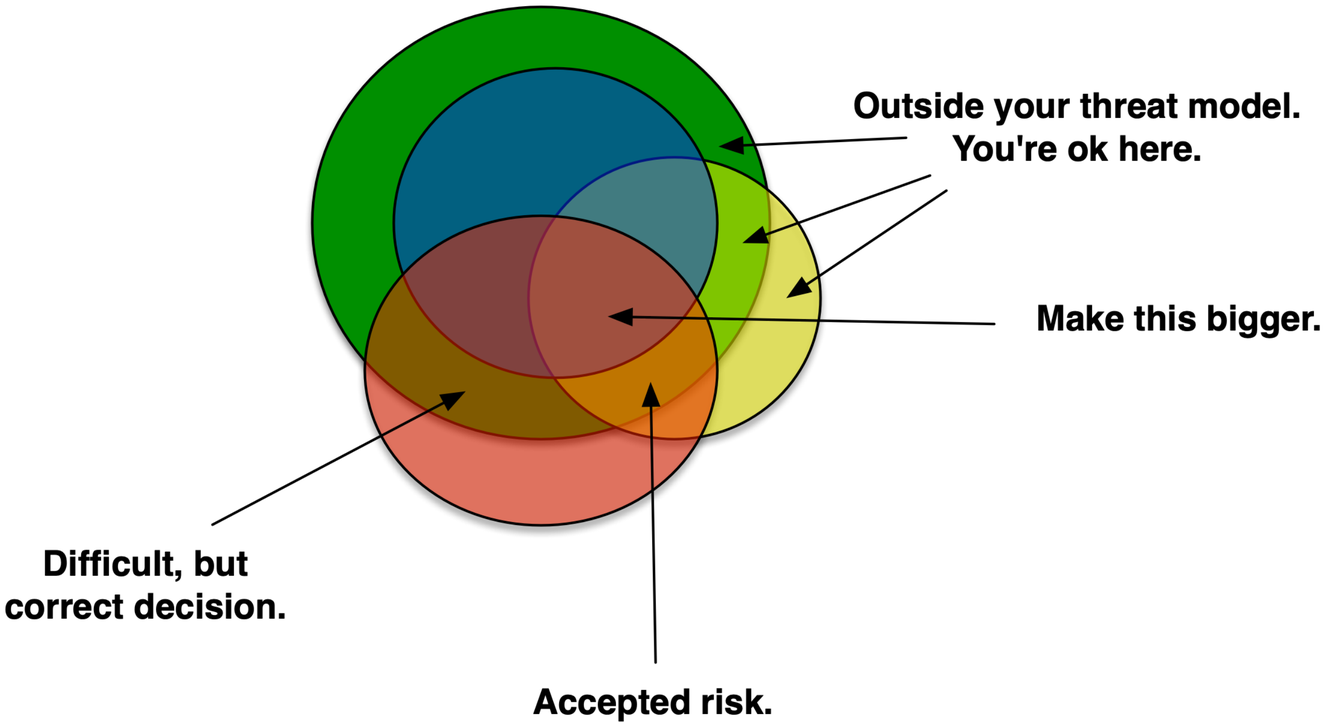


Threats you know about.

Threats you can defend against.

Threats you care about.

Threats you decided to defend against.

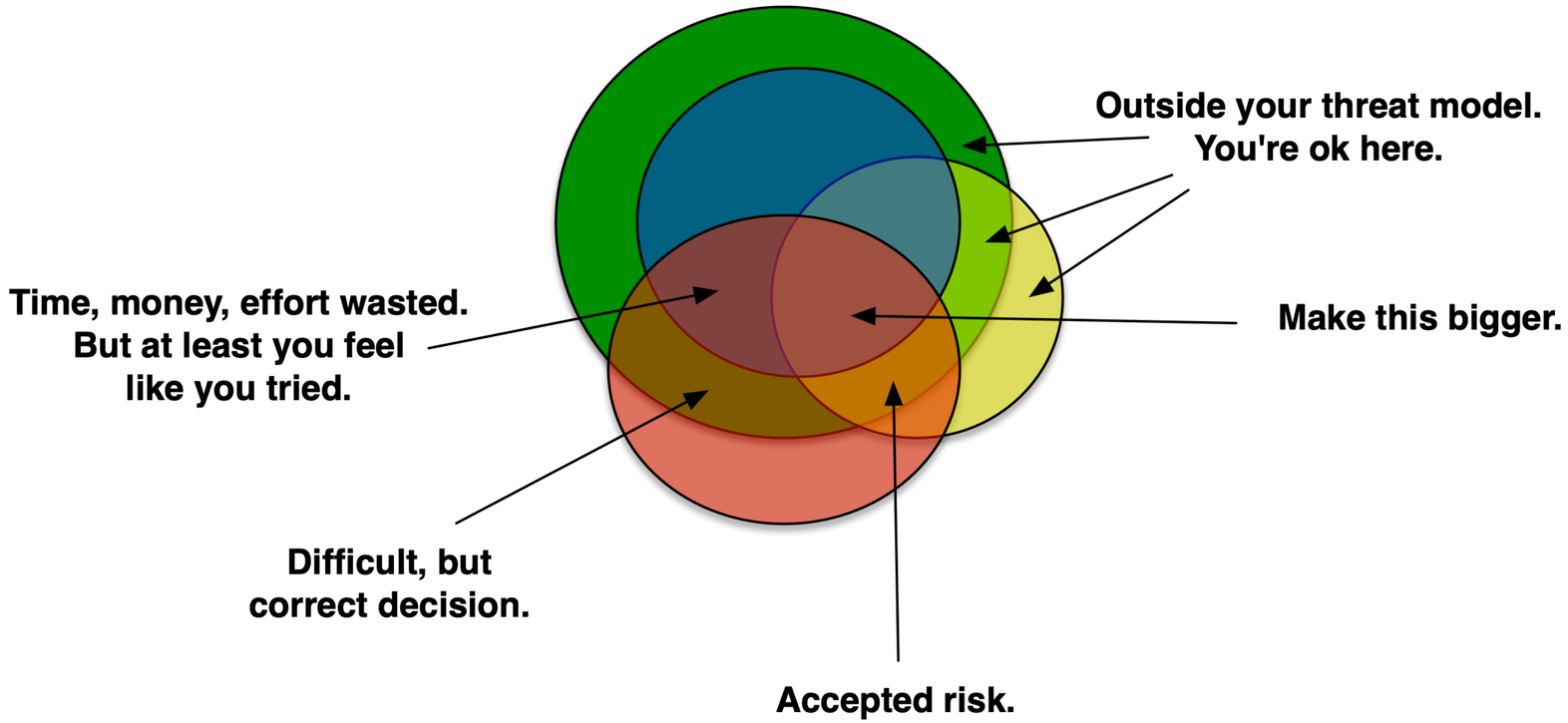


Threats you know about.

Threats you can defend against.

Threats you care about.

Threats you decided to defend against.

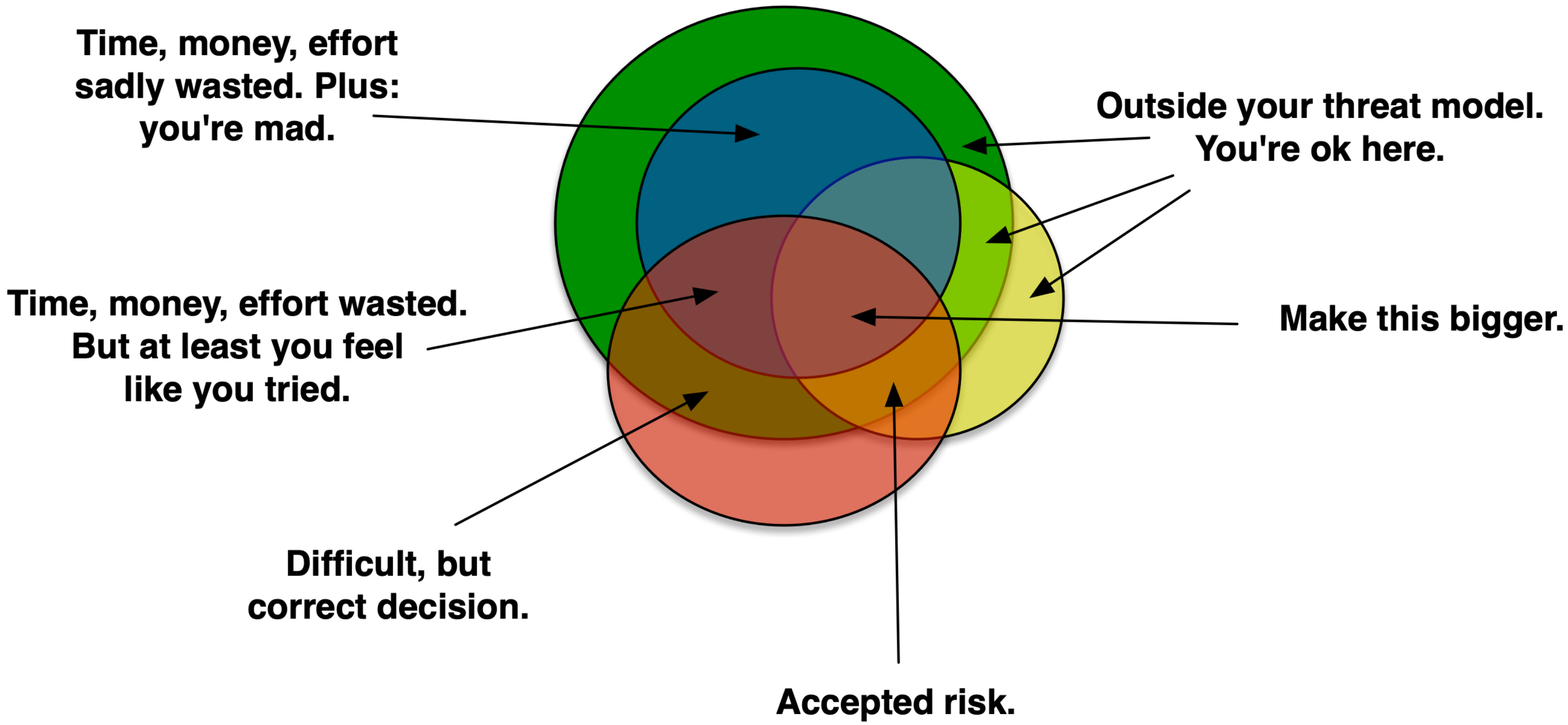


Threats you know about.

Threats you can defend against.

Threats you care about.

Threats you decided to defend against.

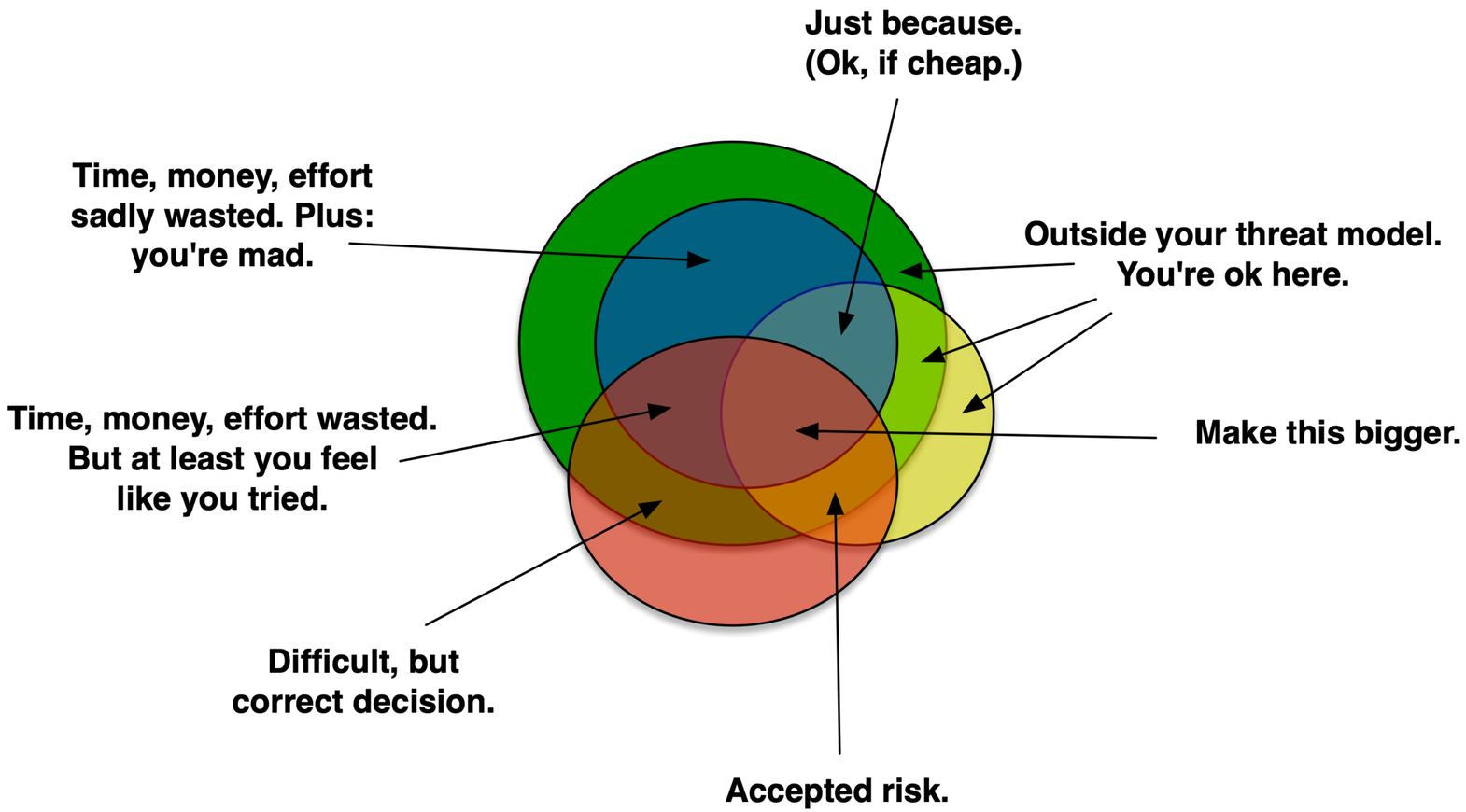


Threats you know about.

Threats you can defend against.

Threats you care about.

Threats you decided to defend against.

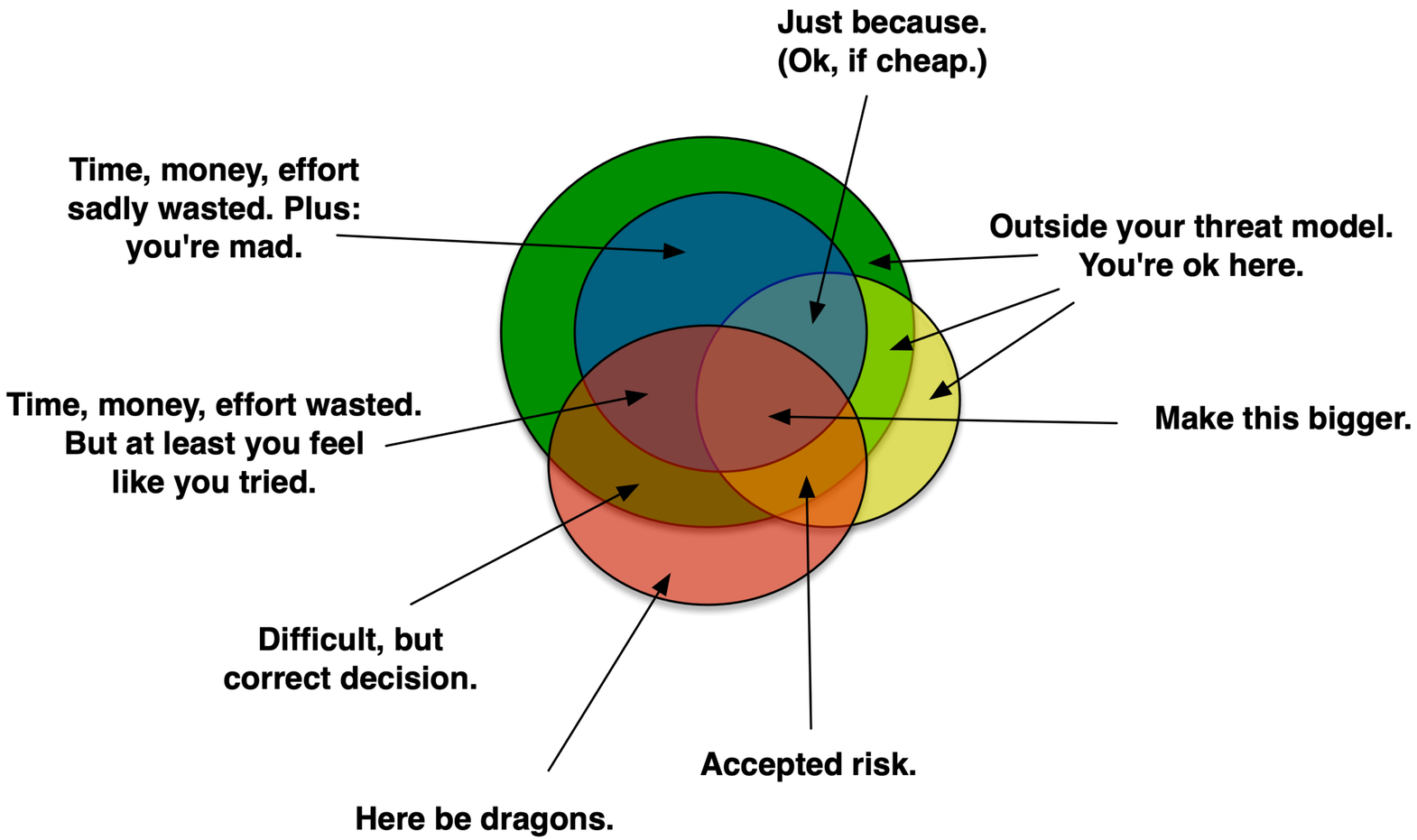


Threats you know about.

Threats you can defend against.

Threats you care about.

Threats you decided to defend against.

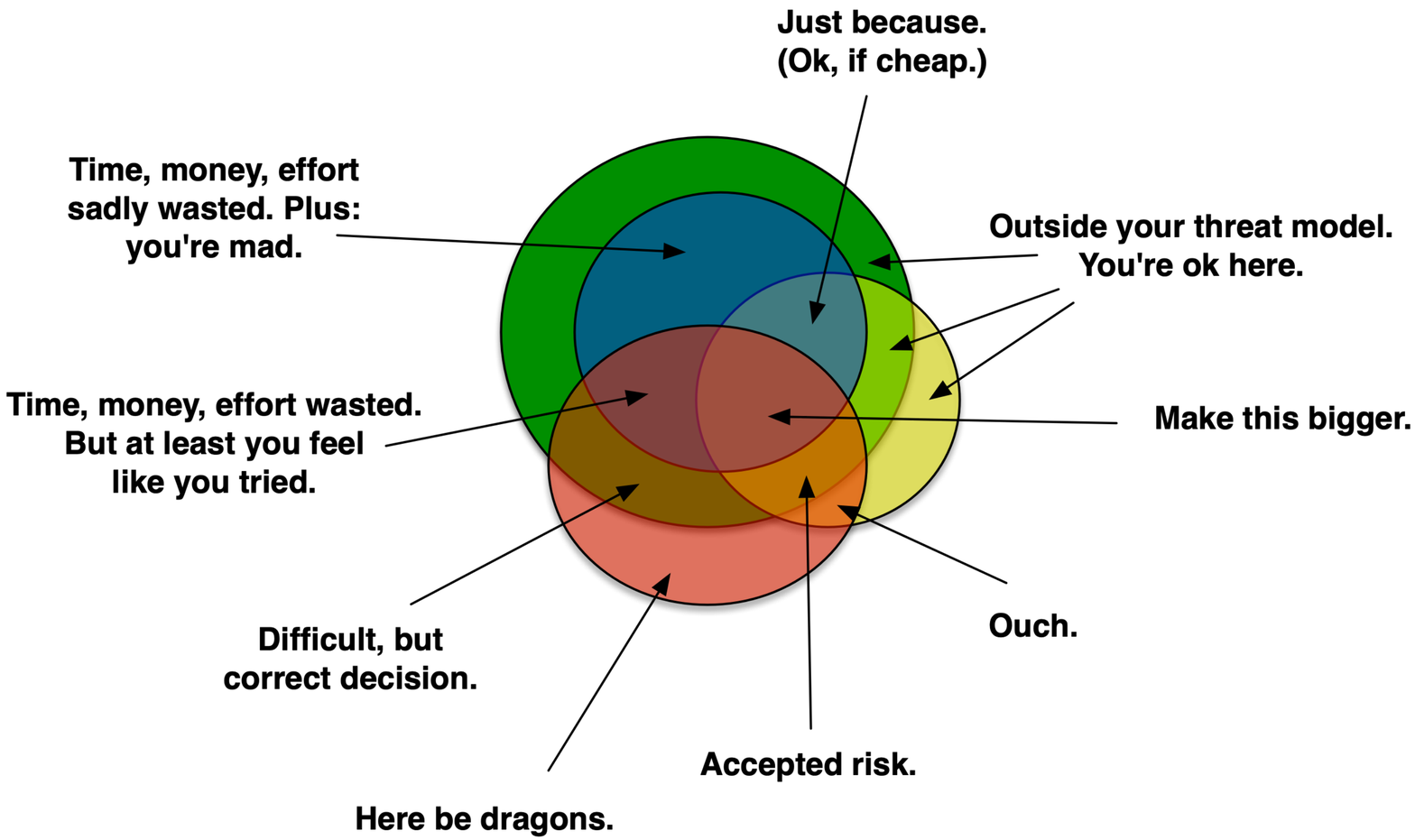


Threats you know about.

Threats you can defend against.

Threats you care about.

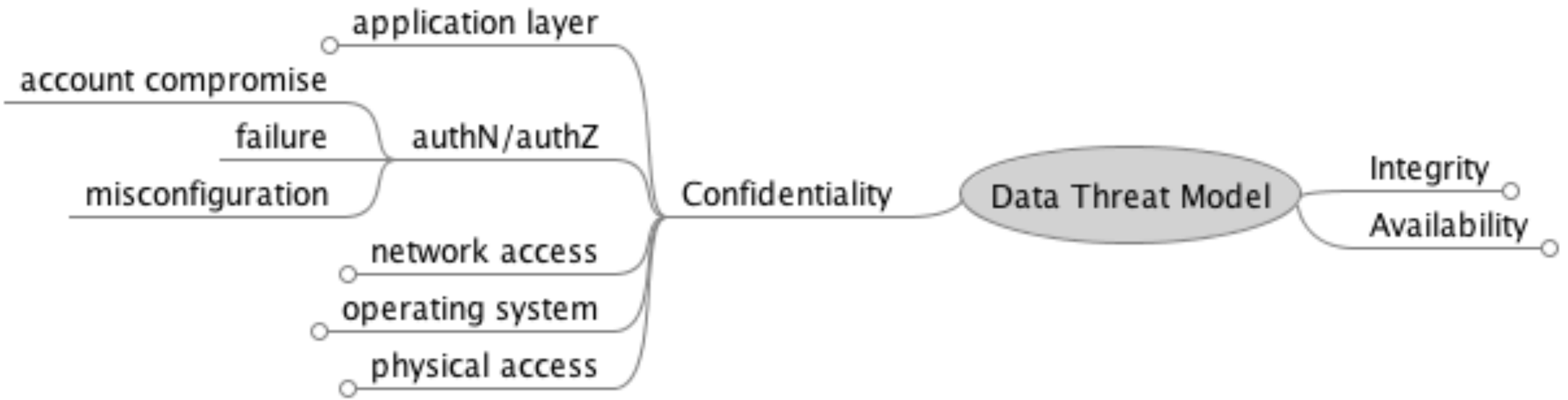
Threats you decided to defend against.

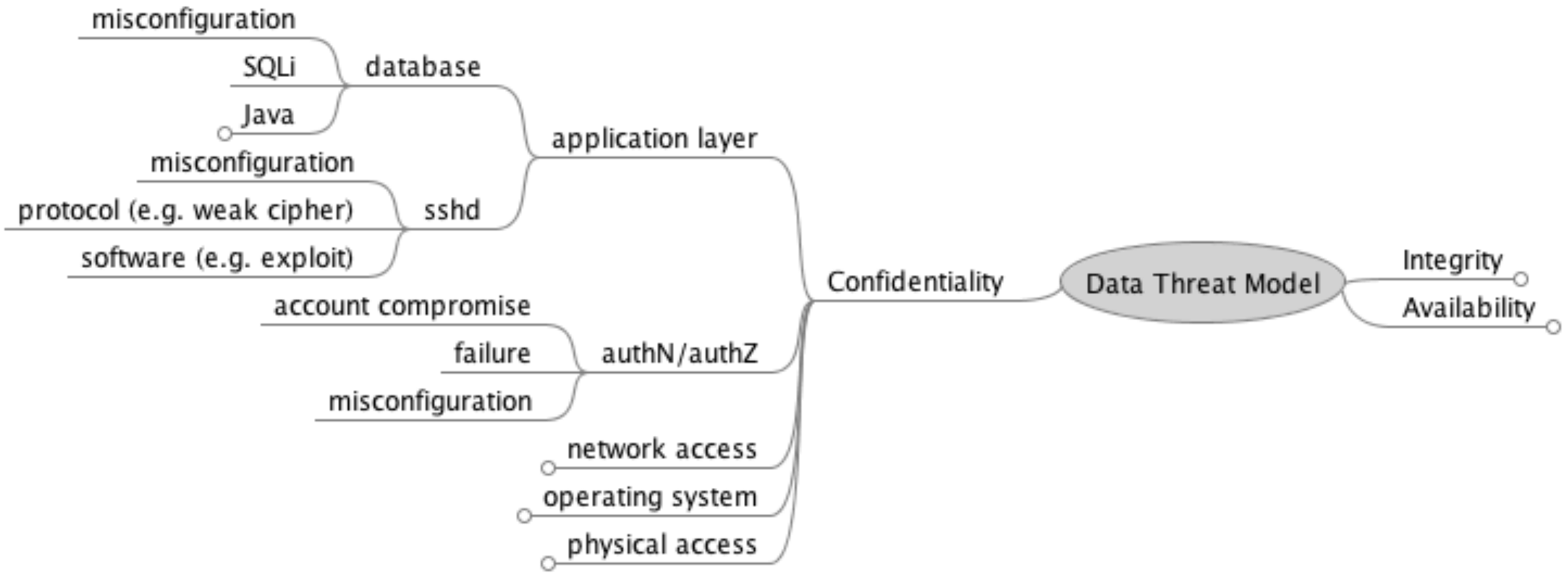


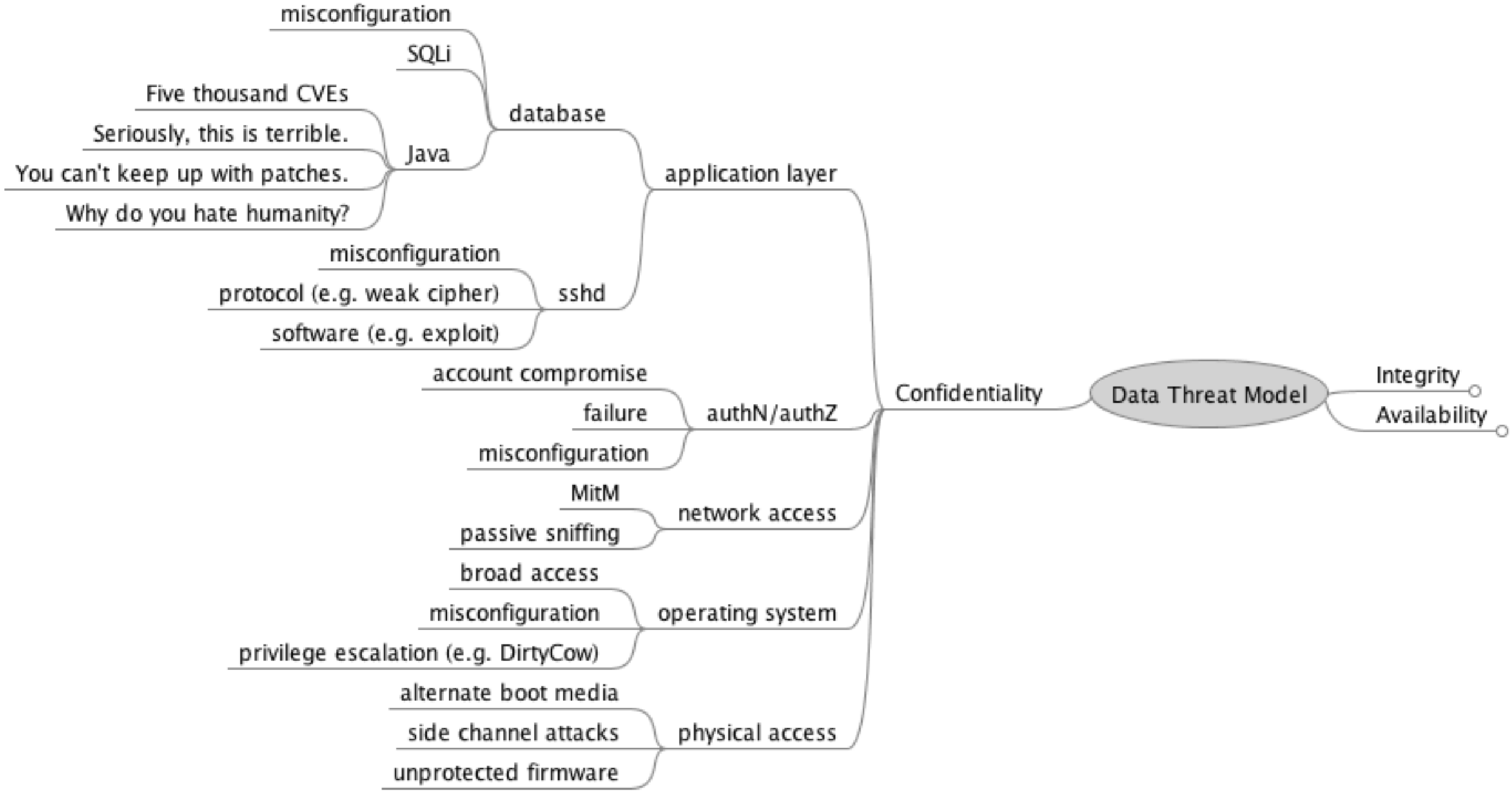
STRIDE

Threat	*Property*
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-Repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization


application layer
authN/authZ
network access
operating system
physical access
Confidentiality
Data Threat Model
Integrity
Availability


Data Threat Model
Confidentiality
Integrity
Availability
application layer
authN/authZ
account compromise
failure
misconfiguration
network access
operating system
physical access


Data Threat Model
Confidentiality
Integrity
Availability
application layer
database
misconfiguration
SQLi
Java
sshd
misconfiguration
protocol (e.g. weak cipher)
software (e.g. exploit)
authN/authZ
account compromise
failure
misconfiguration
network access
operating system
physical access

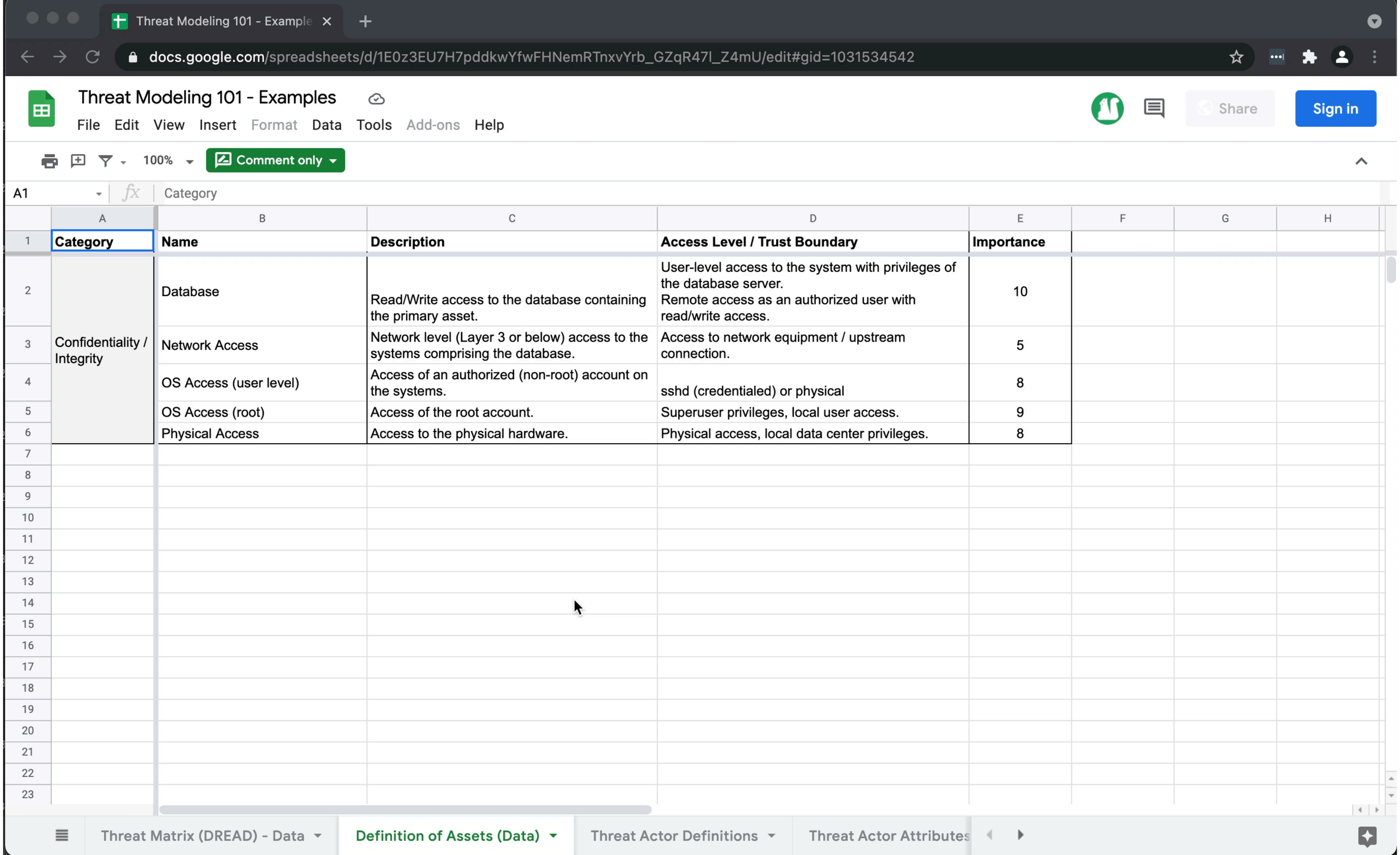

Data Threat Model
Confidentiality
Integrity
Availability
application layer
database
misconfiguration
SQLi
Java
Five thousand CVEs
Seriously, this is terrible.
You can't keep up with patches.
Why do you hate humanity?
sshd
misconfiguration
protocol (e.g. weak cipher)
software (e.g. exploit)
authN/authZ
account compromise
failure
misconfiguration
network access
MitM
passive sniffing
operating system
broad access
misconfiguration
privilege escalation (e.g. DirtyCow)
physical access
alternate boot media
side channel attacks
unprotected firmware

DREAD

Damage	How bad would the attack be?
Reproducability	How easy to recreate the attack?
Exploitability	How easy to launch the attack?
Affected Users	How many are impacted?
Discoverability	How easy to discover for attacker?

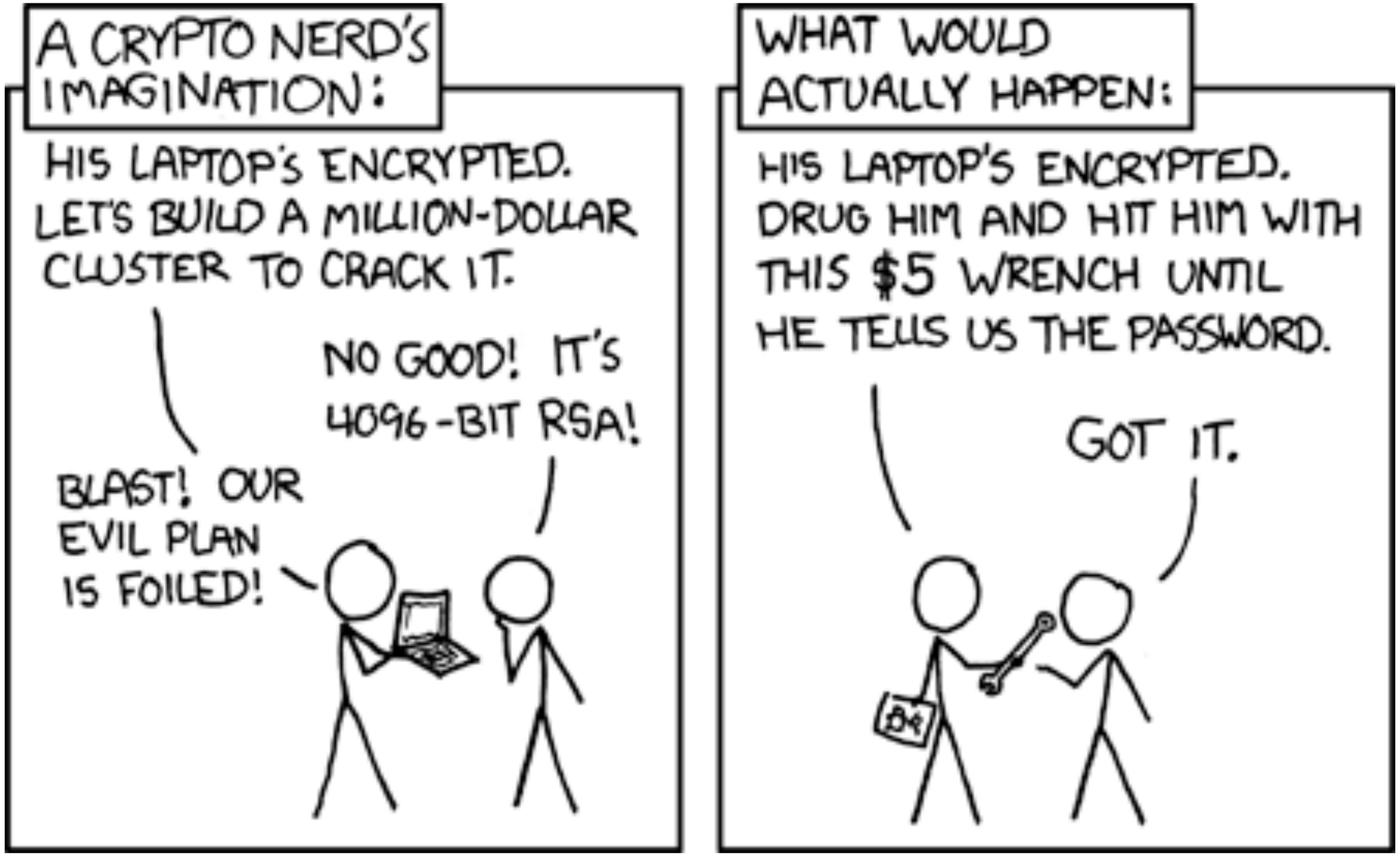
DREAD+D

Damage	How bad would the attack be?
Reproducability	How easy to recreate the attack?
Exploitability	How easy to launch the attack?
Affected Users	How many are impacted?
Discoverability	How easy to discover for attacker?
Detection	How hard to detect for defender?

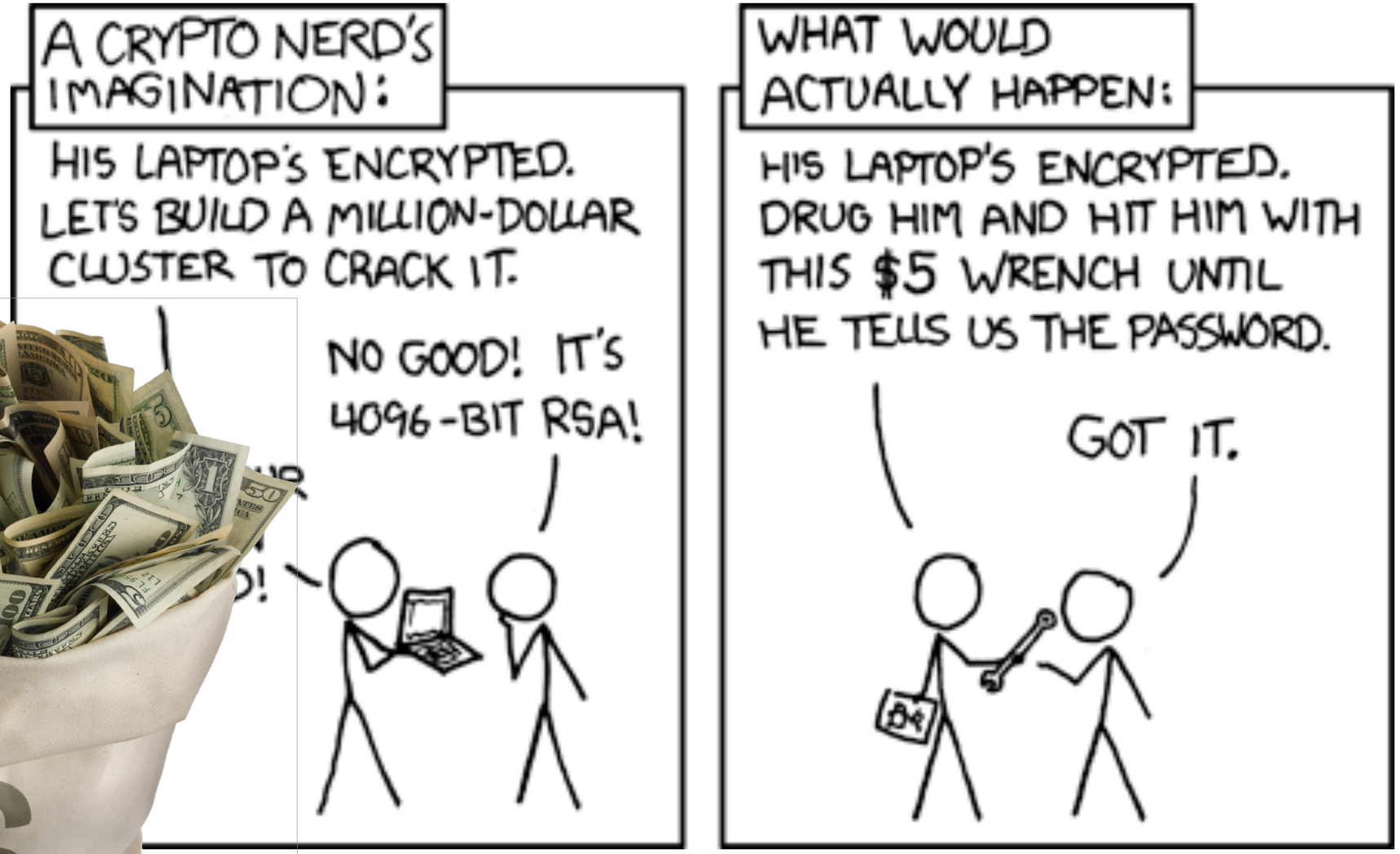


Category	Name	Description	Access Level / Trust Boundary	Importance
Confidentiality / Integrity	Database	Read/Write access to the database containing the primary asset.	User-level access to the system with privileges of the database server. Remote access as an authorized user with read/write access.	10
	Network Access	Network level (Layer 3 or below) access to the systems comprising the database.	Access to network equipment / upstream connection.	5
	OS Access (user level)	Access of an authorized (non-root) account on the systems.	sshd (credentialed) or physical	8
	OS Access (root)	Access of the root account.	Superuser privileges, local user access.	9
	Physical Access	Access to the physical hardware.	Physical access, local data center privileges.	8

https://xkcd.com/538/

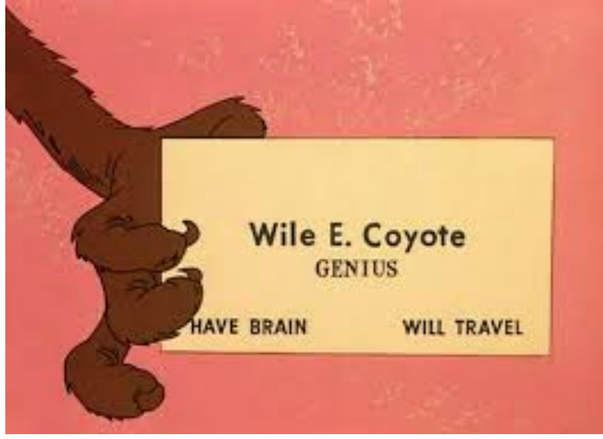


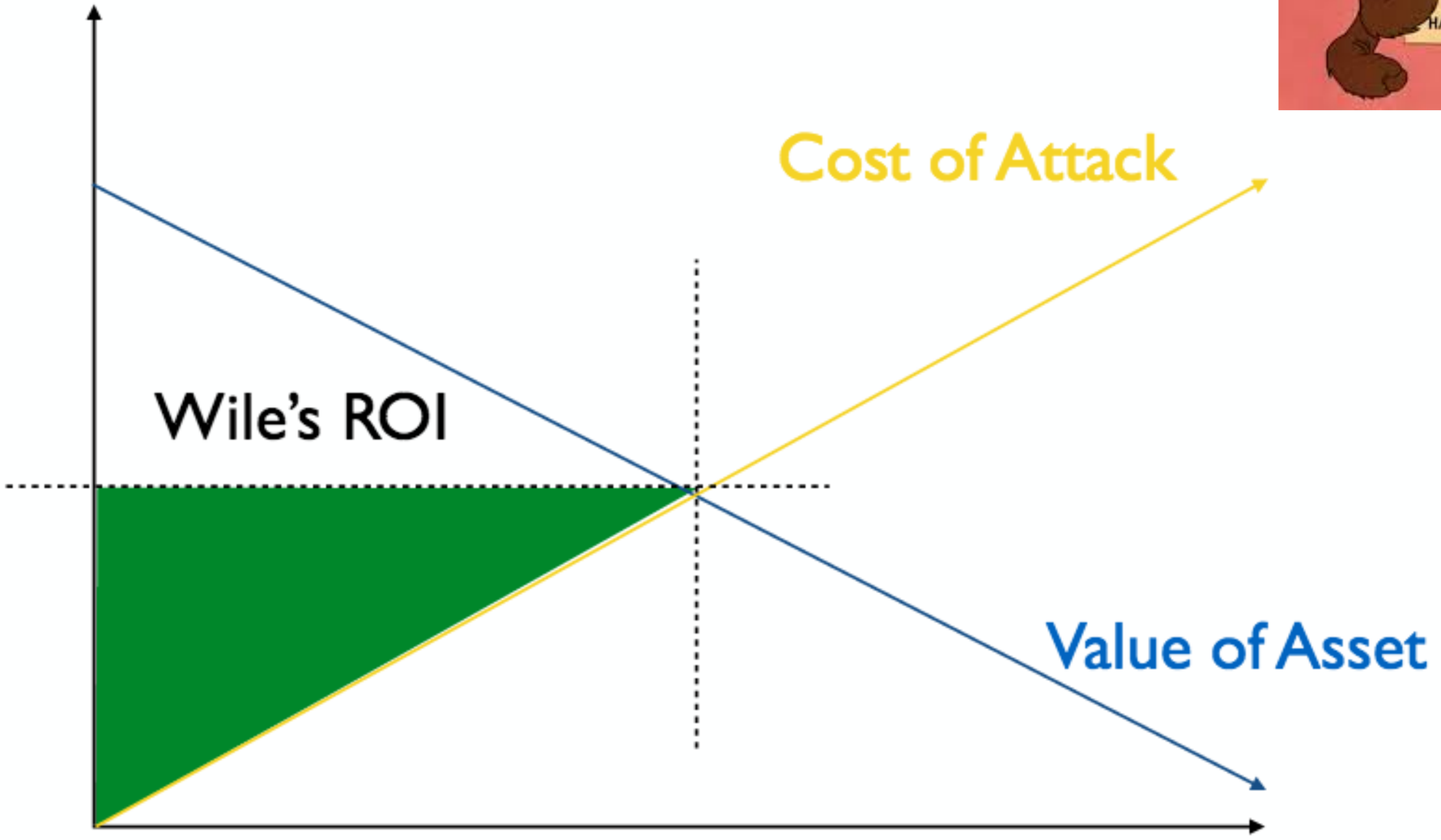
https://xkcd.com/538/



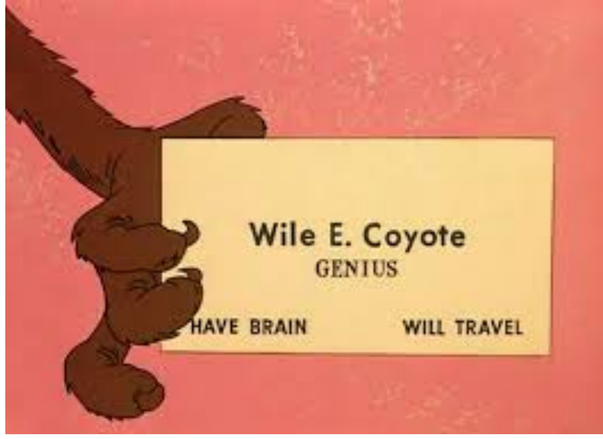
Also works.

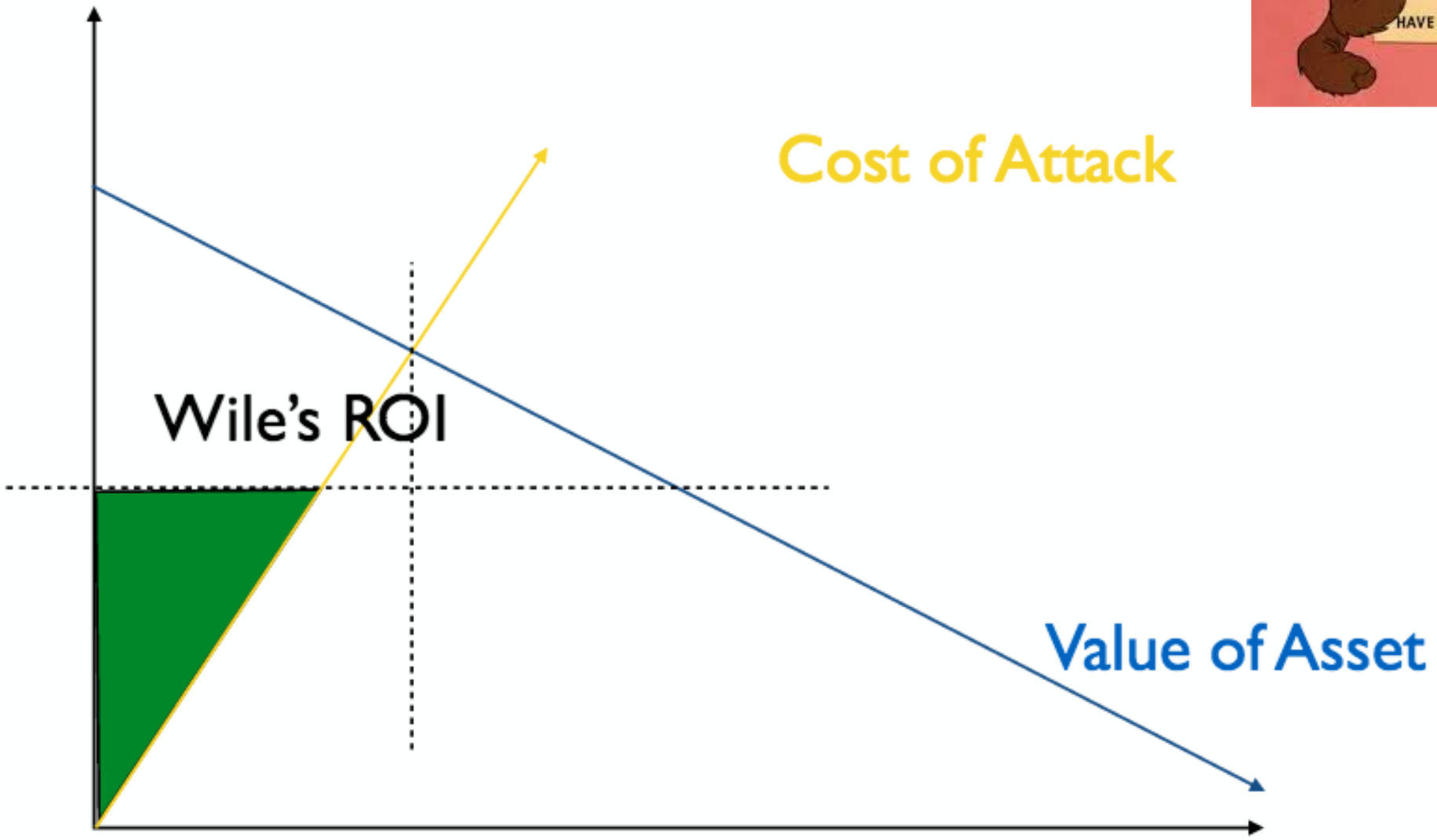
Wile E. Coyote has an MBA.



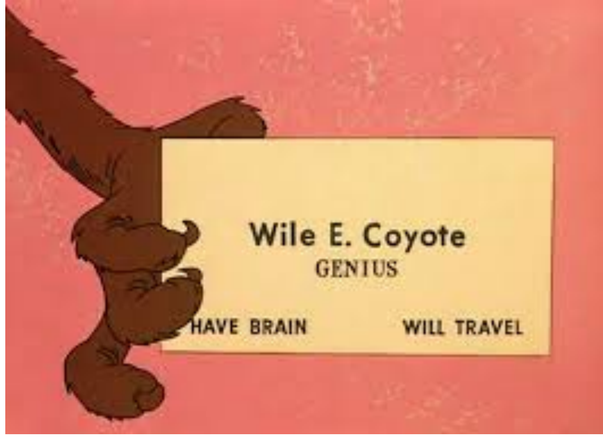


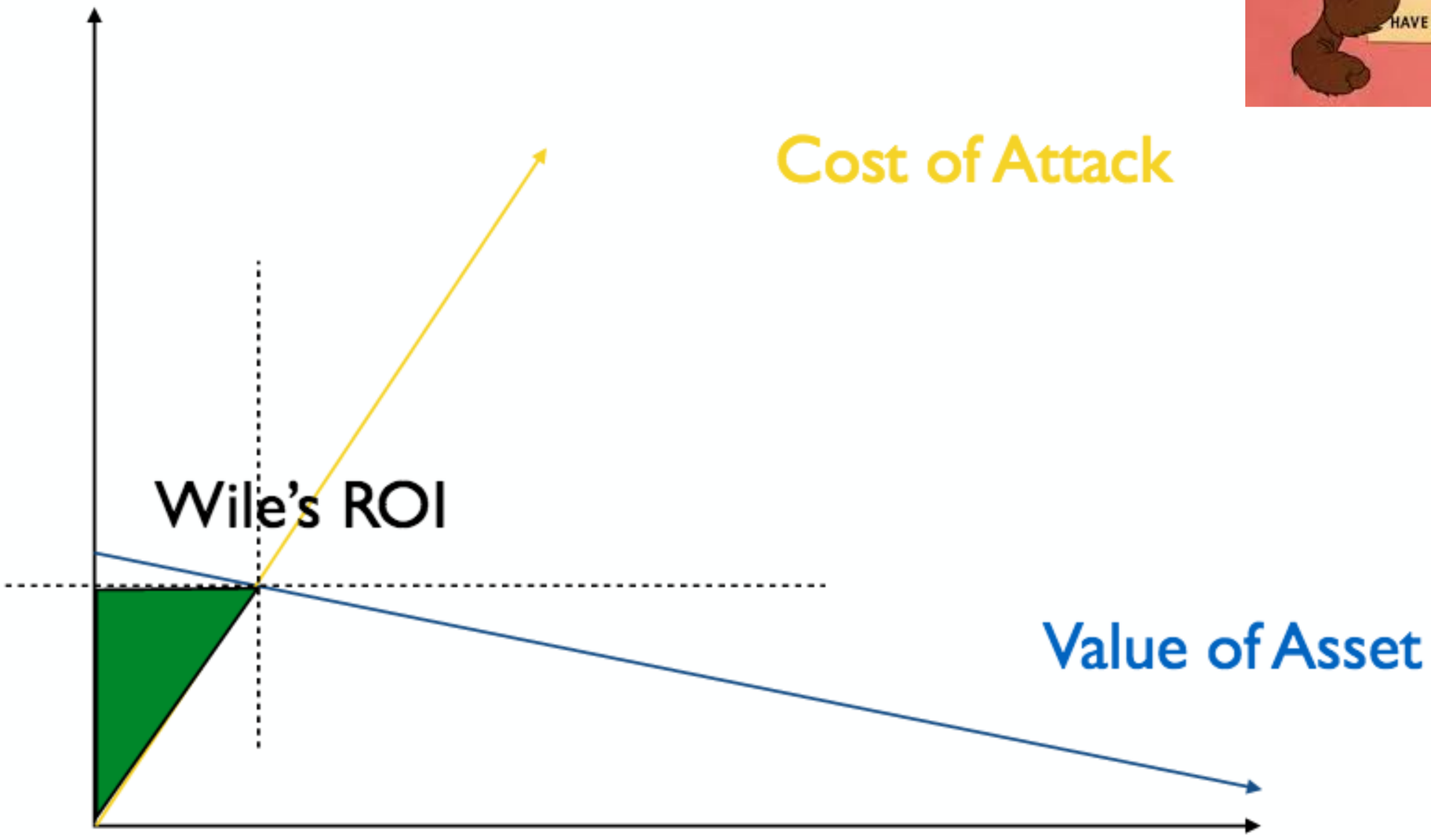
Wile E. Coyote has an MBA.





Wile E. Coyote has an MBA.





Threat Modeling Process

- identify assets, assign values
- use STRIDE to identify threats
- use DREAD+D to derive threat score
- determine / recommend defenses
- zoom out / zoom in & repeat

You can't defend against all threats all of the time.

Attackers will go for the lowest hanging fruit.

Raising the cost of attack – not eliminating the entire threat – is frequently sufficient.

Links

- https://www.usenix.org/system/files/1401_08-12_mickens.pdf
- https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions
- https://www.netmeister.org/blog/threat-model-101.html
- https://is.gd/YwbWKF