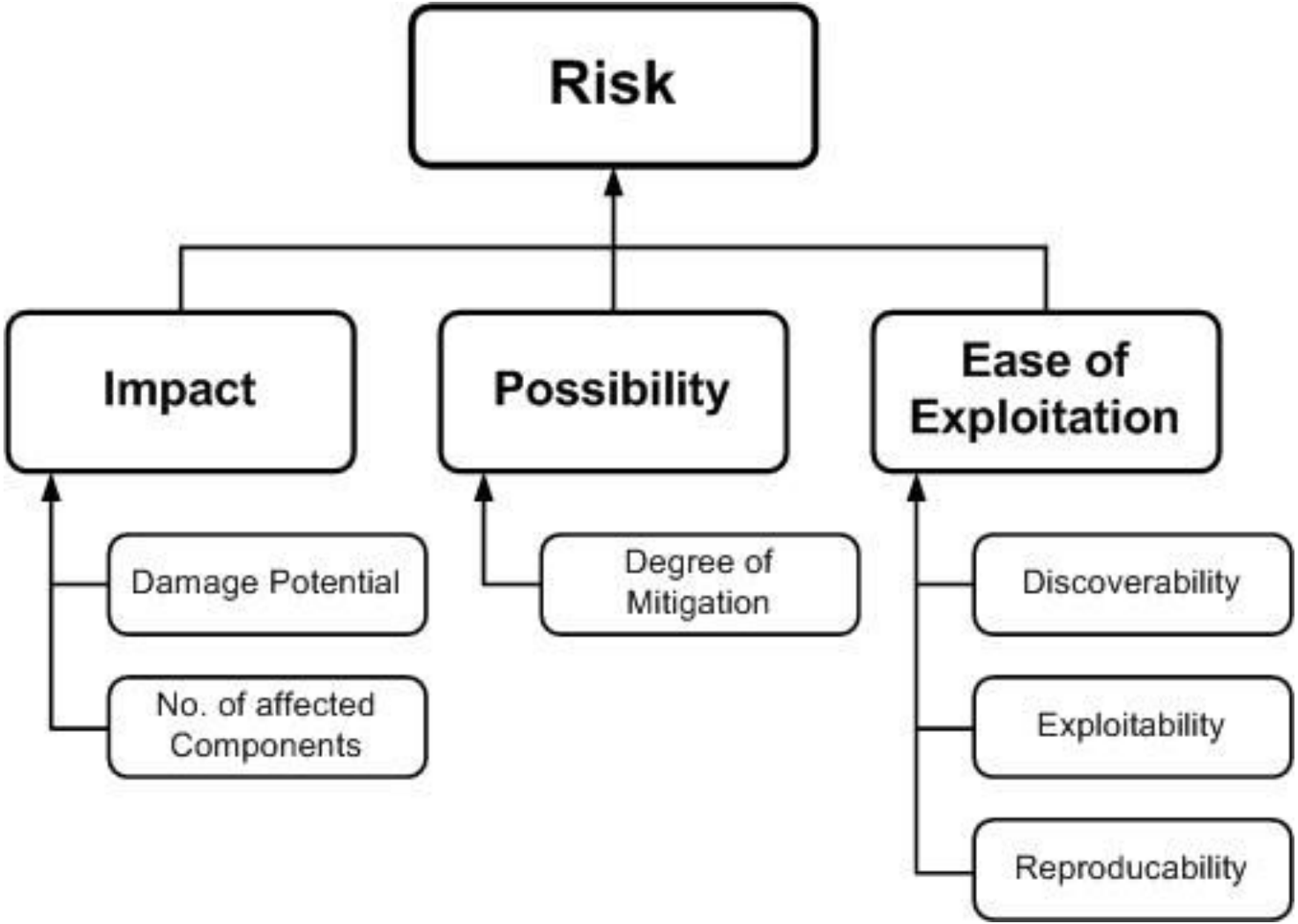
Online Privacy and Safety

Use Signal, Use Tor


Risk
Impact
Possibility
Ease of Exploitation
Damage Potential
No. of affected Components
Degree of Mitigation
Discoverability
Exploitability
Reproducability

Threat Modeling

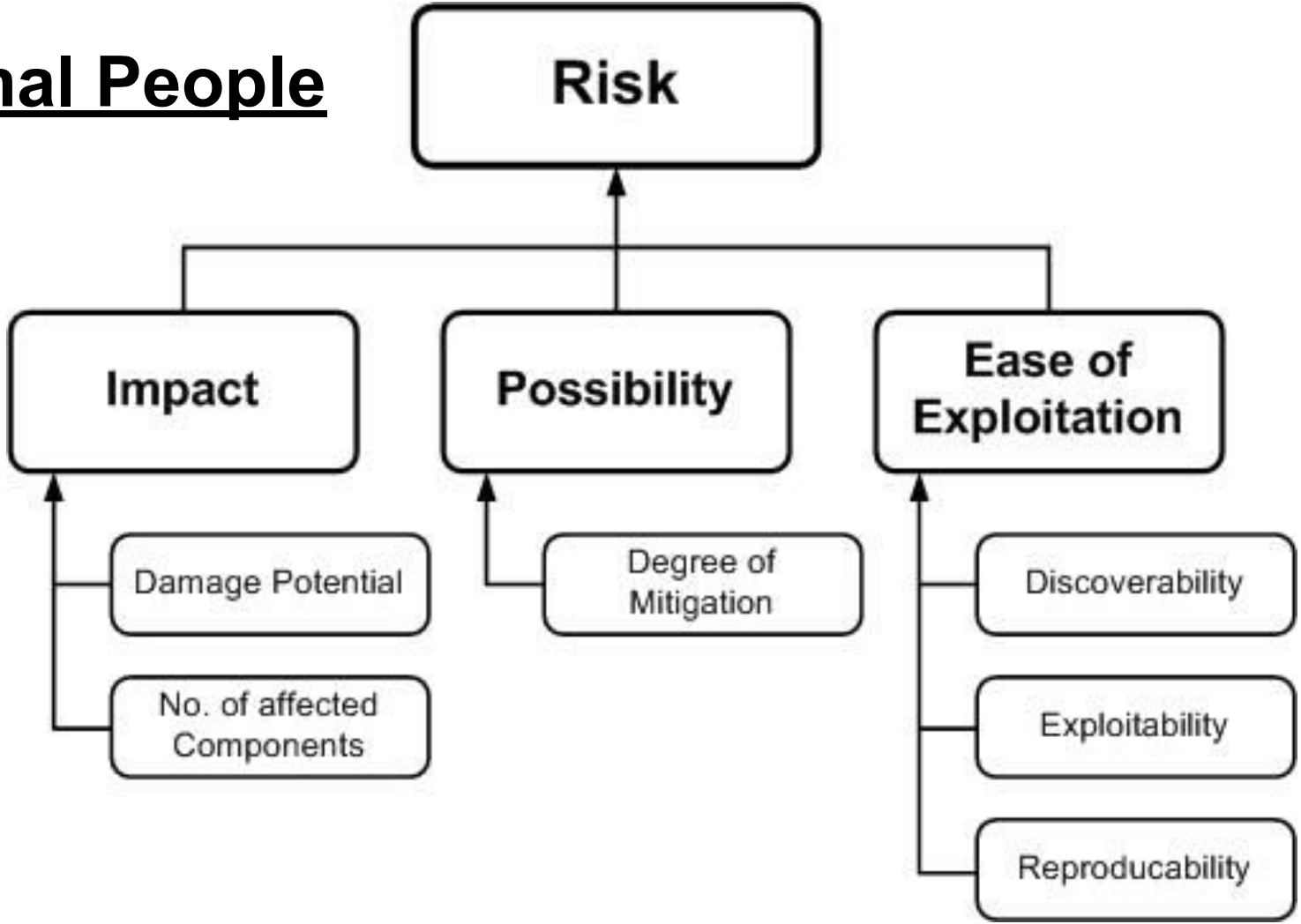
Employers, Family, Friends, Not-Friends

Random criminals

Actual criminals (includes China and Russia)

NSA/Mossad Unit 8200/FSB (on a good day)

Normal People



Don’t Get Ken Bone’d

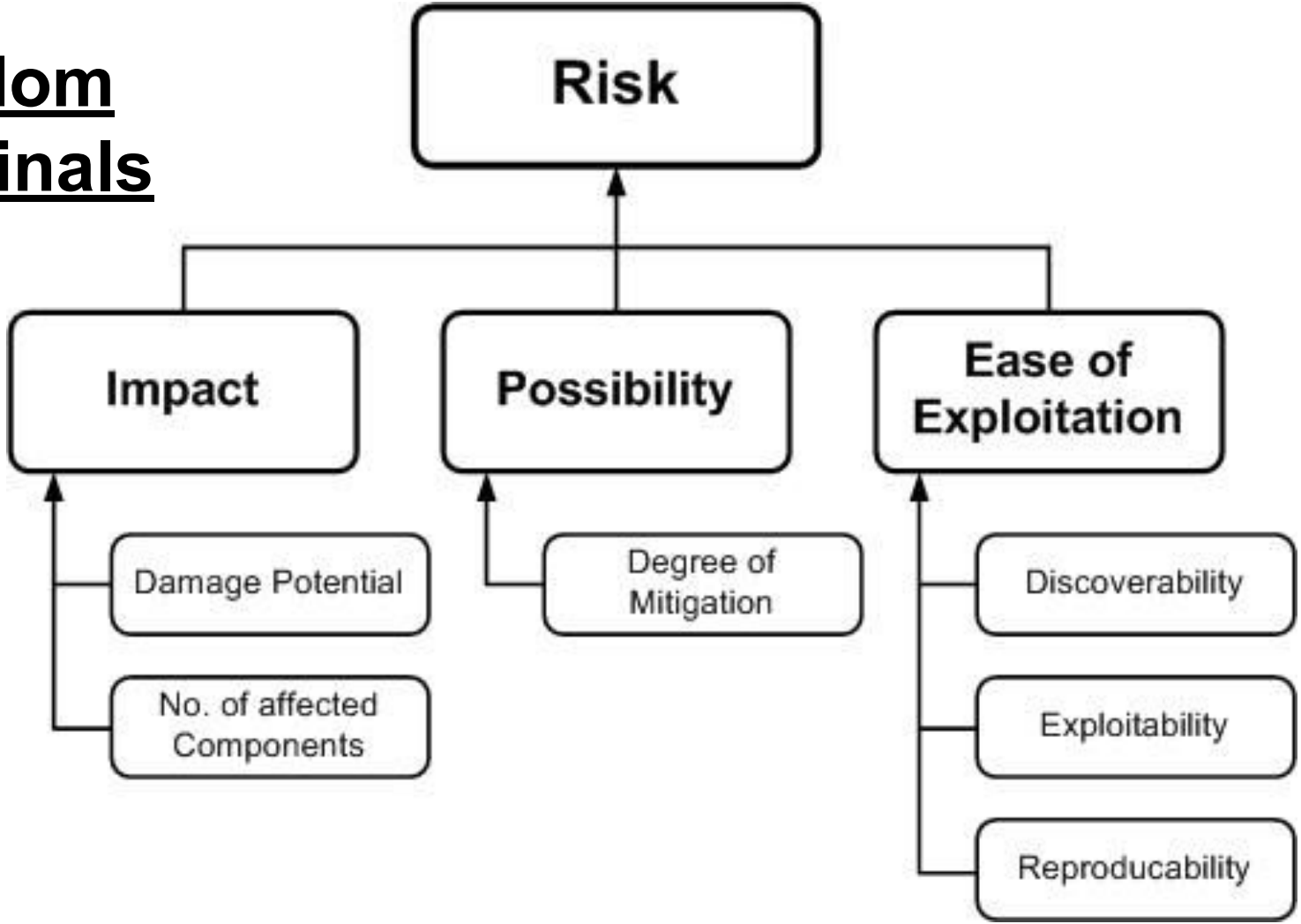
If someone Googles your name, what will they find?

Exercise!!!!

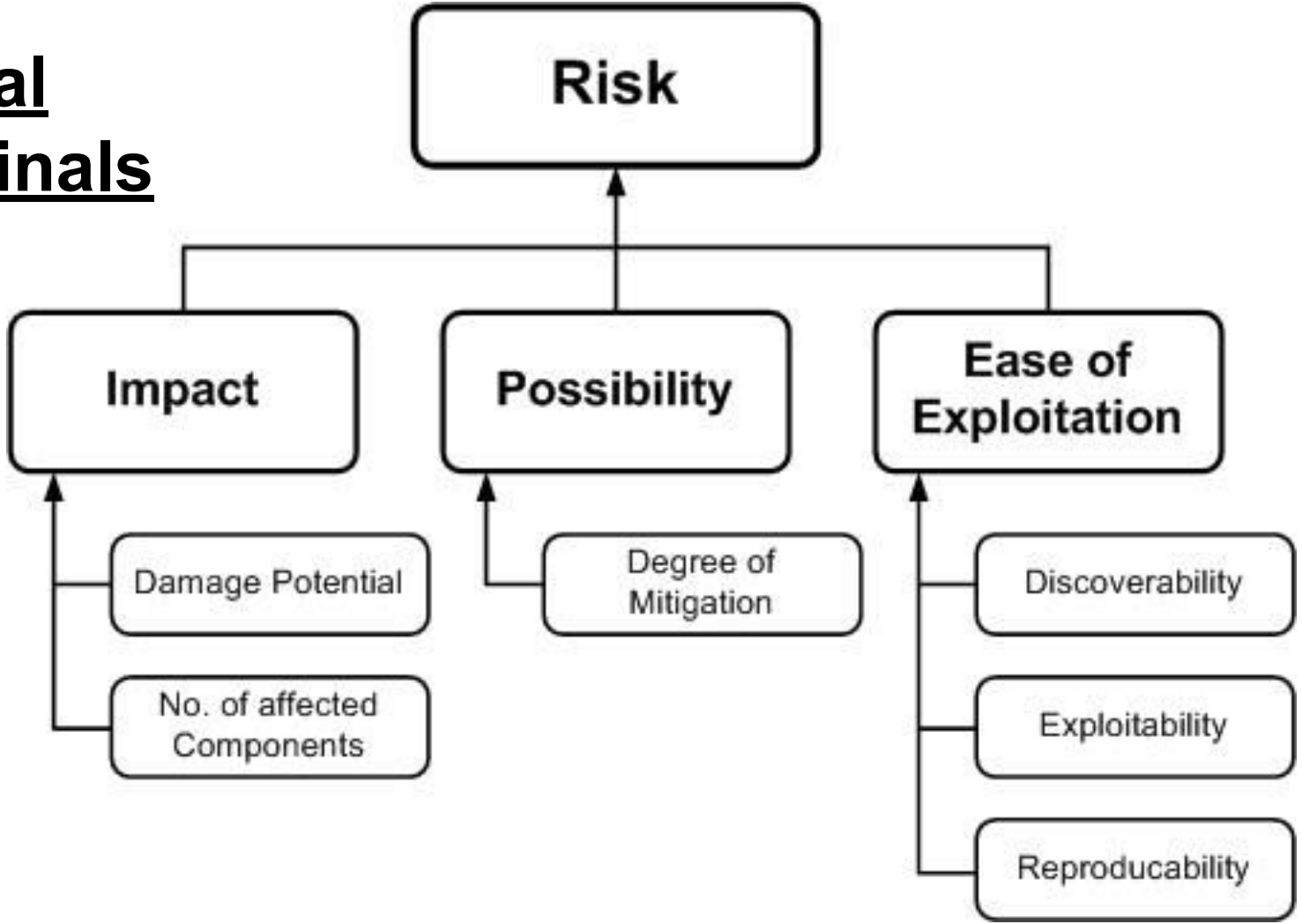
Username reuse?

Social Media Sharing Settings

Random Criminals



Actual Criminals



Risks

Phishing

Database Dump

Browser exploit

Adobe 0-Day

Flash 0-Day

Word/Excel Macro

Malicious Executable

- Backdoored Tools

OS Level Mitigations

Fully patched and updated machine and use chrome

EMET

Disable macros

Disable Flash/Uninstall

Anti-Malware= Malwarebytes

Mobile Mitigations

Use a patched iPhone

alternatively …

Don’t use Android

Or if you have to use Android:

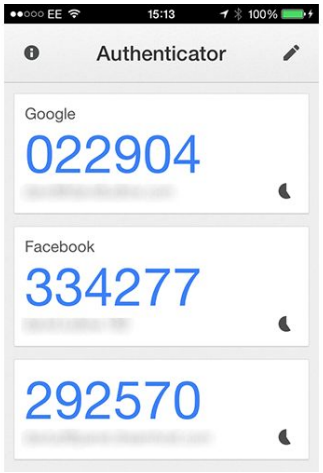
- On Nexus device or on up-to-date Cyanogen mod
- Non-Rooted
- Developer Mode off
- Don’t download any sketchy apps

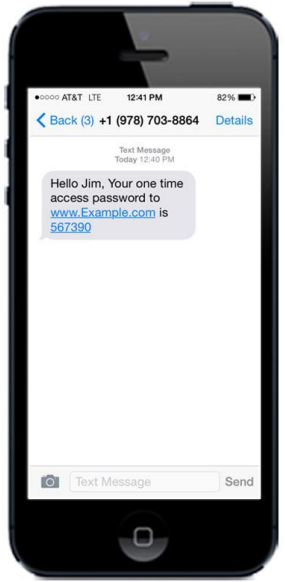
Browser Level Mitigations

Password Manager= LastPass ****

Two Factor Authentication

- SMS
- Applications
- Yubikey



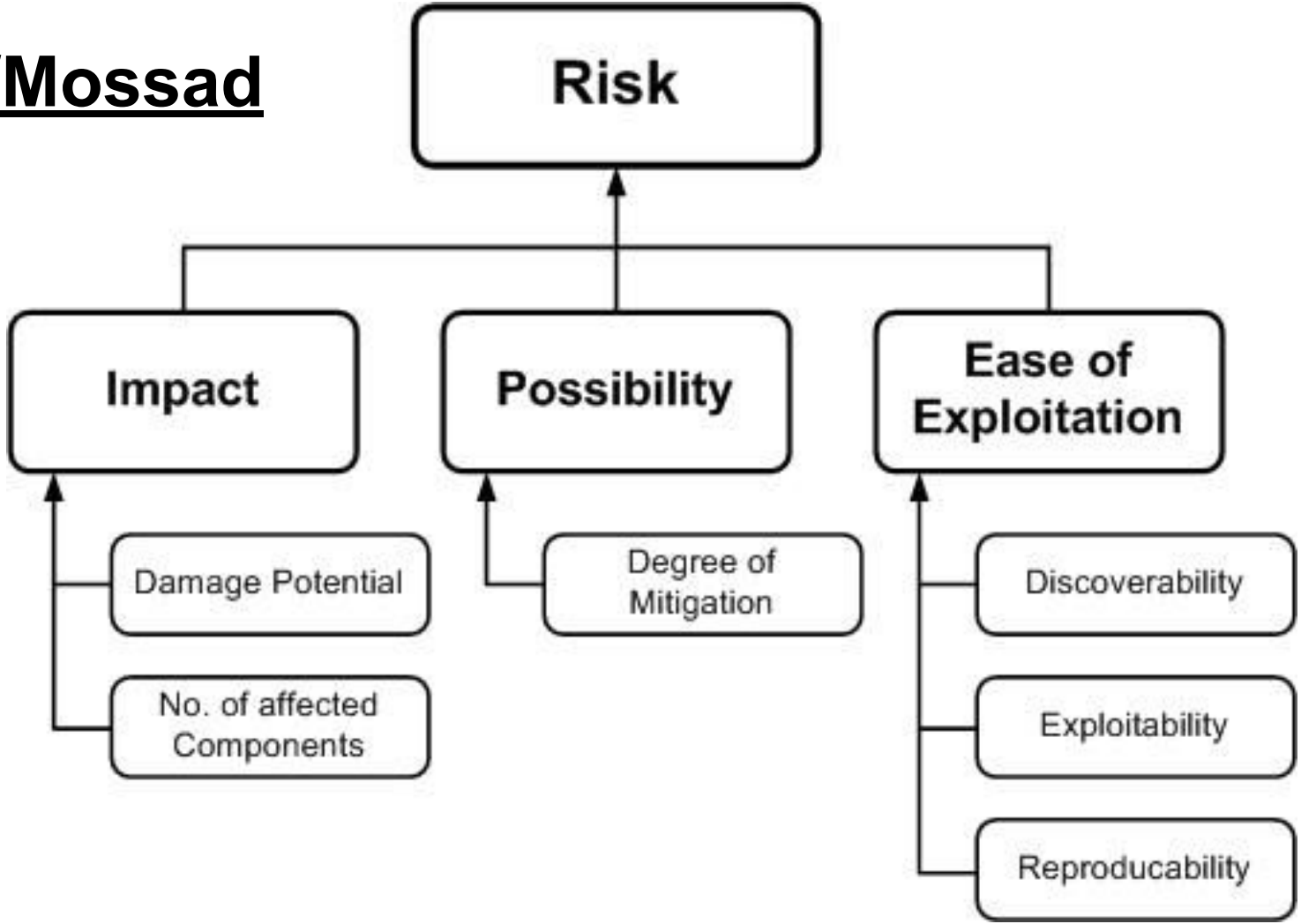


Ad Blocker= uBlock Origin

Encrypted= HTTPS Everywhere

Tracking= Ghostery, Disconnect

NSA/Mossad


Risk
Impact
Possibility
Ease of Exploitation
Damage Potential
No. of affected Components
Degree of Mitigation
Discoverability
Exploitability
Reproducability

Risks

Anything, anywhere, anytime

Alright not really.

Limited by processing power and storage

“I got some oceanfront property in Utah”

Mitigations

Don’t use the internet

Alright, not really

- Be American/ don’t talk to terrorists
- Use quantum proof cryptography
- Don’t use the internet

Intro to OPSEC

aka, how to not get caught

How Do Hackers Get Caught

80% Hacking from mom's basement

Failure to Mask Location

10% Hacking using reused usernames/ personal life bleed over

Failure to Compartmentalize

5% Develop friendships with friend who does one of the above, get snitched on

5% HAXXORREDDDD

99% Known vulnerabilities, phishing, backdoored executables

1% 0 Day

Let’s Address One at a Time

Hacking From Mom’s Basement

DON’T USE LOIC!

VPN

TOR

ProxyChains

Use public wifi

- Untraceable laptop
- No cameras!

Reused Usernames/ Personal Life Bleed Over

Don’t use a username that you have used anywhere else, or means anything to you

New username for each persona, new persona for each activity

Don’t use easily identifiable greetings or styles of speech (“Hiya!”)

Don’t acknowledge your personal life with anyone, no PII, no pictures

Assume all chat logs are saved

Assume everything posted is saved

Snitches

If you don’t break any rules in the first two slides, you should be good

Never let anyone know your actual identity

HAXXORRED

Follow all rules from the security section, and you will be good against most things

Don’t run ~~backdoored versions of~~ LOIC

Don’t run backdoored Metasploit Pro

Don’t try to run any source code you find on HackForums

Unless you know how to read

So you got caught… how do you not get prosecuted?

Beat the case!

Encrypt your hard drive (full disk encryption) and refuse to incriminate yourself!

Encrypt a virtual machine with TrueCrypt, in the hidden partition

Plausible deniability? Not really, but it slows them down

DELETE VMs ON REGULAR BASIS

Destroy hacking infrastructure on regular basis - https://i.imgur.com/WmRwjI3.gifv

REFUSE TO INCRIMINATE YOURSELF!!!!!

Resources

https://grugq.github.io/resources/some_elements_of_intelligence_work-dulles.txt

http://www.slideshare.net/grugq/opsec-for-hackers