CEG 3400 : Risk

*Not the board game

Risk

Today we are going to cover the following:

- Risk Profile
  - Risk Appetite
  - Risk Tolerance
  - Risk Capacity
- Risk Management
- Threat Modeling
- Risk Assessment tools

What is Risk?

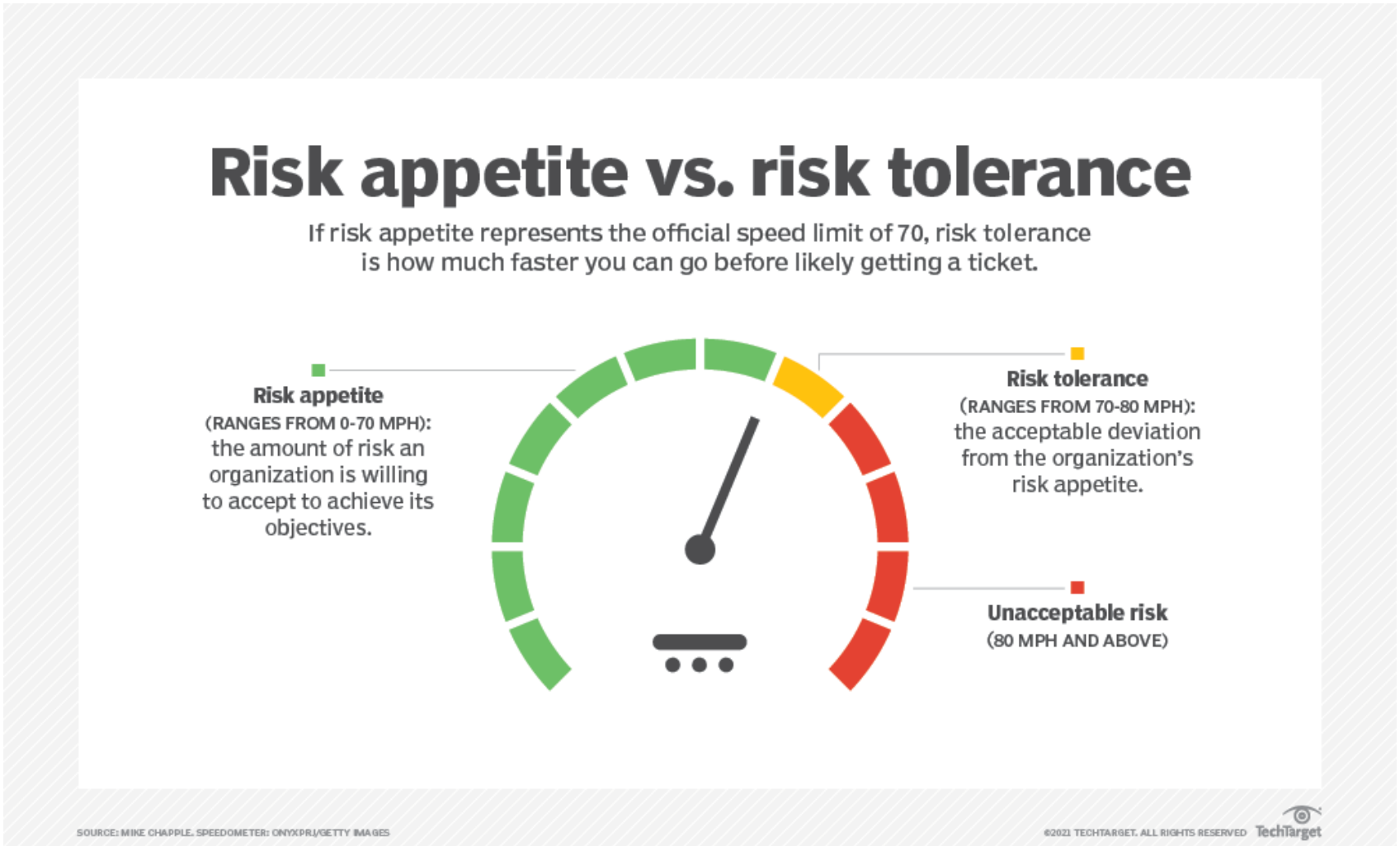
Figure 1: again, not this

noun a situation involving exposure to danger.

verb expose to danger, harm, or loss.

Risk Profile

- **Risk Appetite** the risk *NEEDED* to achieve goals
- **Risk Tolerance** how comfortable you feel about this risk AKA, the risk you *PREFER* to take
- **Risk Capacity** the risk you can *AFFORD* to take



Lets practice

NIST Special Puplication 800-30 : Guide for Conducting Risk Assessment

Lab 6 is all about risk assessment.

Step 1: Prepare for Risk Assessment	
TASK 1-1 IDENTIFY PURPOSE **Section 3.1**	Identify the purpose of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.
TASK 1-2 IDENTIFY SCOPE **Section 3.1**	Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations.
TASK 1-3 IDENTIFY ASSUMPTIONS AND CONSTRAINTS **Section 3.1**	Identify the specific assumptions and constraints under which the risk assessment is conducted.
TASK 1-4 IDENTIFY INFORMATION SOURCES **Section 3.1**	Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.
TASK 1-5 IDENTIFY RISK MODEL AND ANALYTIC APPROACH **Section 3.1**	Identify the risk model and analytic approach to be used in the risk assessment.

Figure 3: task1

Lab 6

- You alone are the entire C-suite of a new startup ***Your Name Inc.***.
- The business purpose of this startup is to facilitate you graduating and getting an awesome job while maintaining some semblence of sanity (this is a joke, stay healthy kids).
- Insiders in your organization are anyone currently living with you or sharing an account.
- Purpose of this assessment: familiarize the board of ***Your Name Inc.*** with basic risk assessment practices and identify any high risk items that might impede your organizations objectives.

Risk Management

Understand, analyze, and address risk to make sure the organization achieves its goals.

- Continuing process (repeats)
- Before you understand your risk you need to identify them
- Your entire organization will get this wrong (everyone does)
- Your organization will perform this better than some multi-million $ companies (see last point)
- Humans (and Mark Zuckerberg) perform risk managment every day

Matt Hanon

Matt Hanon

- Wired.com author
- Twitter nerd
- apple fanboy
- used apple's me.com
- Gmail user
- also bought items on amazon.com

The Hack

Figure 4: twitter

Figure 5: gmail

Figure 6: amazon.com

Lab 6: Scope

- `nmap` scan of your home network (with permission)
- all other networked and non-networked electronic devices
- all online accounts with non-directory information
- all pertinent data about you that might cause harm
- time frame is from today until after your first month of a CS/Cyber/IT job

What are we doing?

- Policies: Confidentiality, Integrity, Availabilty
- Threat Model: assumptions about our adversaries
- Mechanisms (SW, HW, procedure etc.) that achieve org goals and maintain our policies

But you did not have the word risk in that last slide...

Well before we can assess risk we need to understand the threats we may be facing.

2 types of threats we are going to focus on:

- Non-adversarial
- Adversarial

Non adversarial

- Accident
- Human Error
- Structural failure
- Environmental

See NIST 800-30 Table E-3.

Adversarial

Deliberate actaions of a third party with ***intent*** to cause organizational disruption or loss.

Who are our adversaries and what are their capabilities?

- Hackers
- Script Kiddie
- Cyber Criminals
- Cyber Terrorists
- Hacktivists
- State-Sponsored attackers
- That one cousin who cant stand to see you succeed and is actively sabotaging your graduation
- That one person from ITinder that you swiped right on, had dinner with, then ghosted

What can our adversaries do?

Nist 800 30 Table E-2

Threat Events (Characterized by TTPs)	Description
Perform reconnaissance and gather information.	
Perform perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections.
Gather information using open source discovery of organizational information.	Adversary mines publically accessible information to gather information about organizational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
Perform reconnaissance and surveillance of targeted organizations.	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organizations and ascertain points of vulnerability.
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
Craft or create attack tools.	
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.

Figure 7: adversarial threat events

Where are we weakest

Identify all vulnerabilities and predisposing conditions that affect the likelihood of a threat event causing adverse impact.

Determine Likelihood

What are the chances of a threat event occuring that results in adverse impact.

Consider the following:

- charactersistics of threat source
- vulnerabilities identified
- susceptibility given the safegaurds/countermeasures the org has in place to prevent or impede such an event

Determine impact of event

Assuming the event occurs, what is the impact of that event.

Determine Risk

Based on the likelihood of an event occuring and the impact from that event should it occur.

What do we get out of all this

Hopefully two things.

1. A better understanding of your overall risk profile, which can inform decision making around better mechanisms to protect the organization.
2. A priority ranking of threats as they would impact your organization, given limited resources this will focus your organizational spending on security mechanisms for a higher Return On Investment