Basics in Cyber Security

Griffith University

Griffith UNIVERSITY
Queensland, Australia

Basics in Cyber Security

- CIA model

Basics in cyber security

Core Goals of Security

- Confidentiality
- Integrity
- Availability

Authenticity

Non-repudiation

CIA model

Saltzer J. and ***Schroeder*** M., "The Protection of Information in Computer Systems," *Communications of the ACM*, 17(7), July 1974.

Saltzer

Schroeder

Basics in cyber security

Confidentiality

- Relates to data/information security
  - ✓ Mitigating unauthorized access to sensitive network assets
- Accomplish through various levels of
  - ✓ Encryption
  - ✓ Authentication
  - ✓ Access controls

Common Confidentiality Classifications

- Private sector:
  - ✓ Public
  - ✓ Internal
  - ✓ Confidential
- Government agencies:
  - ✓ Unclassified
  - ✓ Restricted
  - ✓ Secret
  - ✓ Top secret

Basics in cyber security

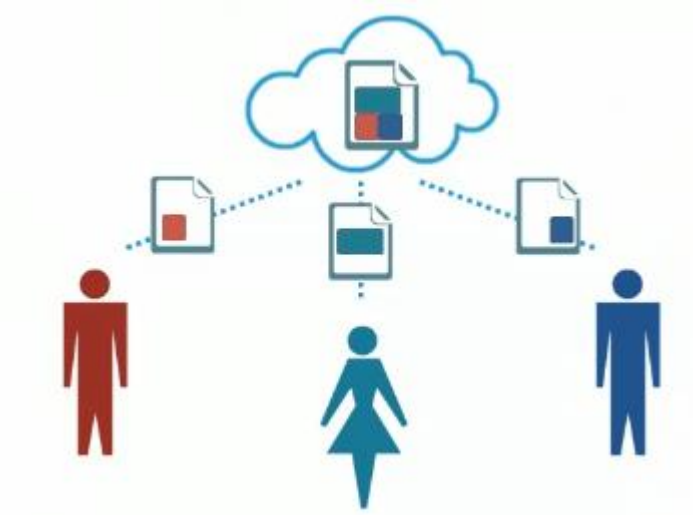
Integrity

- Relates to data/information security
  - ✓ To protect data/info. against unauthorized or accidental change
- Encompasses data/info:
  - ✓ Consistency
  - ✓ Accuracy
  - ✓ Validity
- Accomplished through:
  - ✓ Security programs which manage and detect change
  - ✓ Permission to control access to assets
  - ✓ Auditing and accounting processes to record changes

Basics in cyber security

Availability

- Relates to data/information security
- Generally unfettered accessibility of resources to users, systems and applications
- Two common threats to availability
  - Accidental
    - ✓ Natural disasters
    - ✓ Equipment failure
    - ✓ Unplanned outages
  - Deliberate
    - ✓ DoS attacks
    - ✓ Network worms



Basics in cyber security

Authenticity

- Authenticate who sent/created the data
- Accomplished through:
  - ✓ Message Authenticate Code
  - ✓ Time stamp
  - ✓ Authentication Protocols

Non-Repudiation

- Assure that the author/sender cannot deny an action
- Accomplished through:
  - ✓ Digital Signature

Basics in Cyber Security

What is the security goal in following scenarios?

1. Software providers wish to guarantee no malicious code is attached to their original clean code.
2. Service providers wish to provide service to users all the time.
3. The financial department wishes to let the receivers trust the email is from this department.
4. A university cannot deny a degree certificate has been issued after many years.
5. The Canvas system needs to protect the exam papers/answers not to be accessed by students in a wrong time.

Basics in Cyber Security

What is the security goal in following scenarios?

1. Software providers wish to guarantee no malicious code is attached to their original clean code. Integrity
2. Service providers wish to provide service to users all the time. Availability
3. The financial department wishes to let the receivers trust the email is from this department. Authenticity
4. A university cannot deny a degree certificate has been issued after many years. Non-repudiation
5. The Canvas system needs to protect the exam papers/answers not to be accessed by students in a wrong time. Confidentiality

Basics in Cyber Security

– Risks, threats, vulnerabilities, exploits

Basics in cyber security

Risks, Threats, Vulnerabilities, and Exploits

- Often confused
- Distinction is important
  - Documentation
  - Organizational security policies

Questions: Does the following description mean a threat, vulnerability or an exploit?

- Lack of user awareness and training
- A hacker may hack the user by social engineering
- Trick the user to open file attachments that includes malware

Basics in cyber security

Threats

"A potential violation of security" - ISO 7498-2

- Asset inventory
- Threat analysis
- Negative impact analysis against an asset
- Assets and threats must be prioritized

Threats have a negative effect on business operations:

- Loss of revenue
- Loss of reputation
- Loss of consumer confidence

Sources of threats

- Malware
- Social engineer
- Security breach
- Natural disasters
- War

Basics in cyber security

Asset identification

- What has value to the organization?
  - IT systems
  - Customer data
- What type of data is the most valuable?
  - Personally identifiable information (PII)
  - Confidential corporate data
    - Accounting data
    - Trade secrets
  - Intellectual property (IP)
    - Industrial or artistic
  - Payment card information

Threats classification

Known threats

- Unique virus signature

Unknown threats

- 0-day
- Weakness in OS unknow to vendor

APT (Advanced Persistent Threats)

- Backdoors
- Use a compromised system for a long period of time

Basics in cyber security

Vulnerabilities

- Hardware
  - Out of date firmware
  - Lack of physical security controls
  - Unused open ports left running
    - Telnet, SSH, HTTP
- Software
  - Updates not applied
  - Misconfiguration
  - Default settings
  - Design errors
- Policy flaws
- Human errors

Exploits

- Takes advantage of a vulnerability by malicious users
- 0-day exploit: unknown to manufacturer, known but not patched

Risks

Relates to:

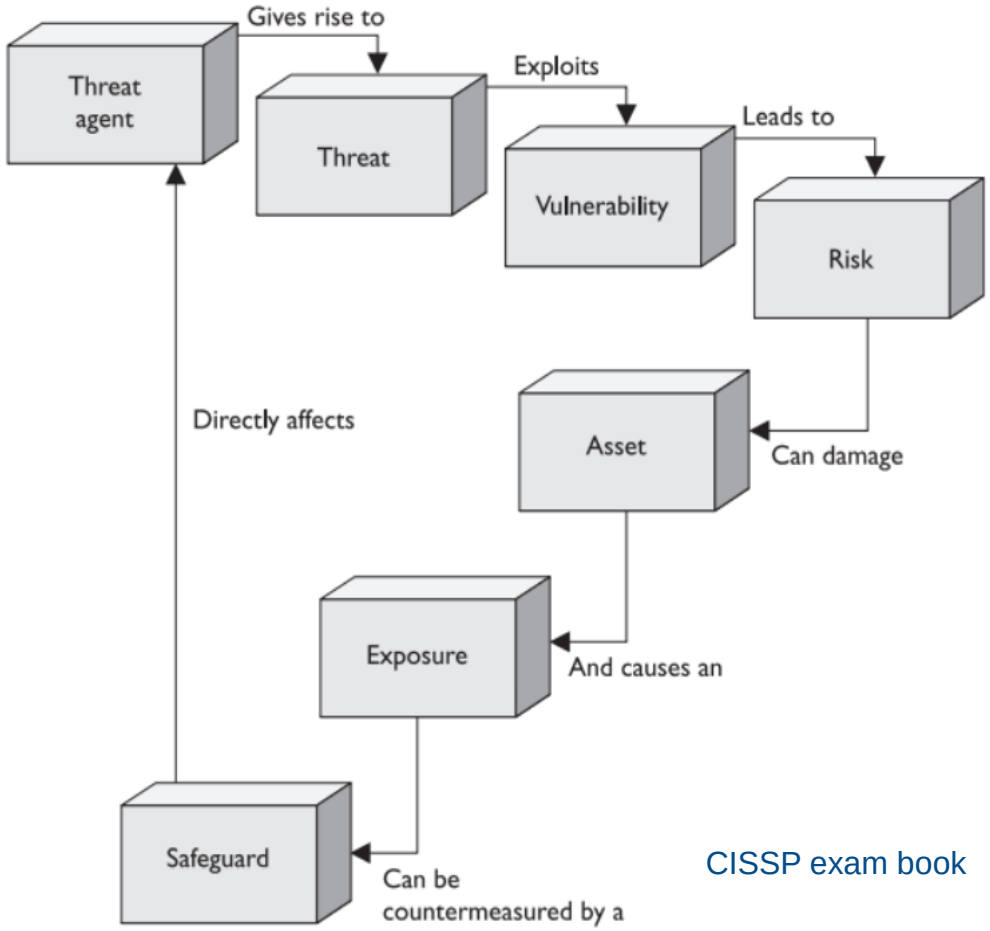
* the probability that a particular threat using a specific exploit will take advantage of a specific vulnerability

* the impact of this exploit.

Basics in cyber security

Risk = Likelihood x Impact of Threats Exploiting Vulnerabilities

= Vulnerabilities x Threats x Impact of Threats Exploiting Vulnerabilities



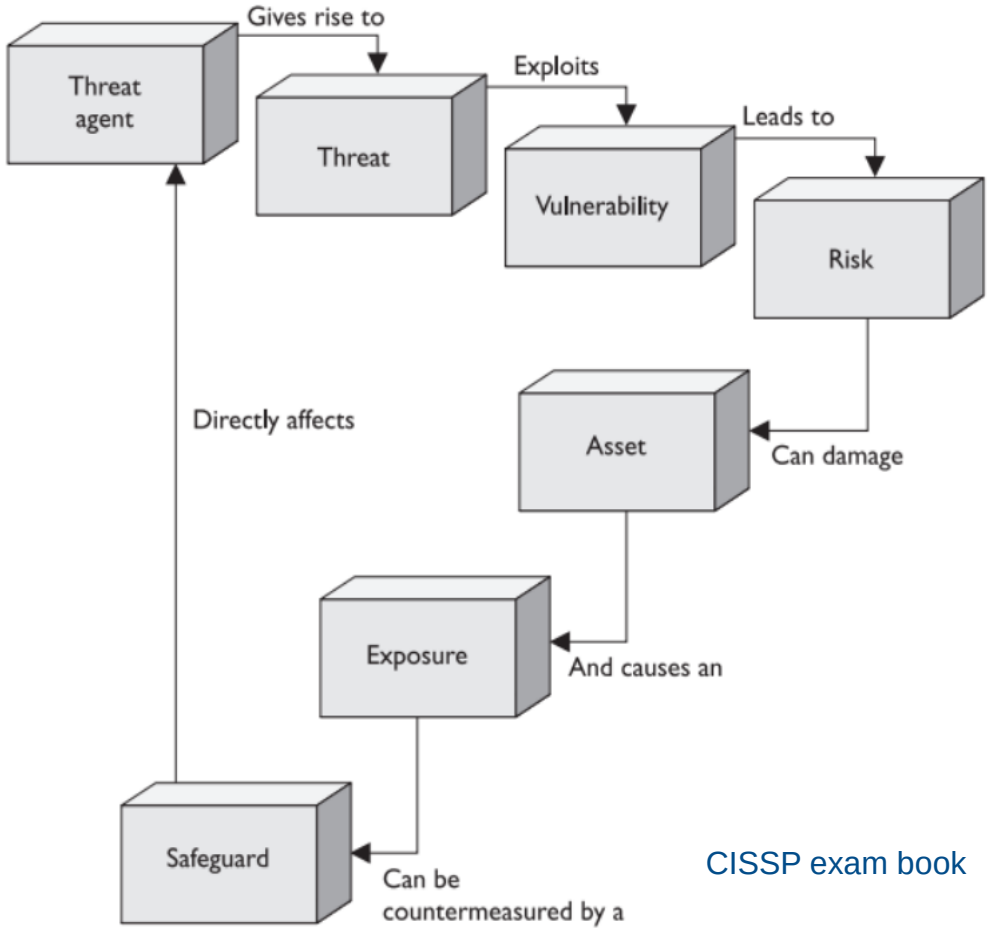
CISSP exam book

- Lack of user awareness and training
- A hacker may hack the user by social engineering
- Trick users to opening file attachments that includes malware

Basics in cyber security

Risk = Likelihood x Impact of Threats Exploiting Vulnerabilities

= Vulnerabilities x Threats x Impact of Threats Exploiting Vulnerabilities



CISSP exam book

- Lack of user awareness and training **--- Vulnerability**
- A hacker may hack the user by social engineering **--- Threat**
- Trick users to opening file attachments that includes malware **--- Exploit**

Basics in cyber security

Risks, Threats, Vulnerabilities, and Exploits

Motivation

Threat Actors

- Hacktivist
- Industrial spies
- Nation/state
- Hobbyist

Ability

Exploits

- Hacking using tools
- Social engineering

Opportunity

Vulnerabilities

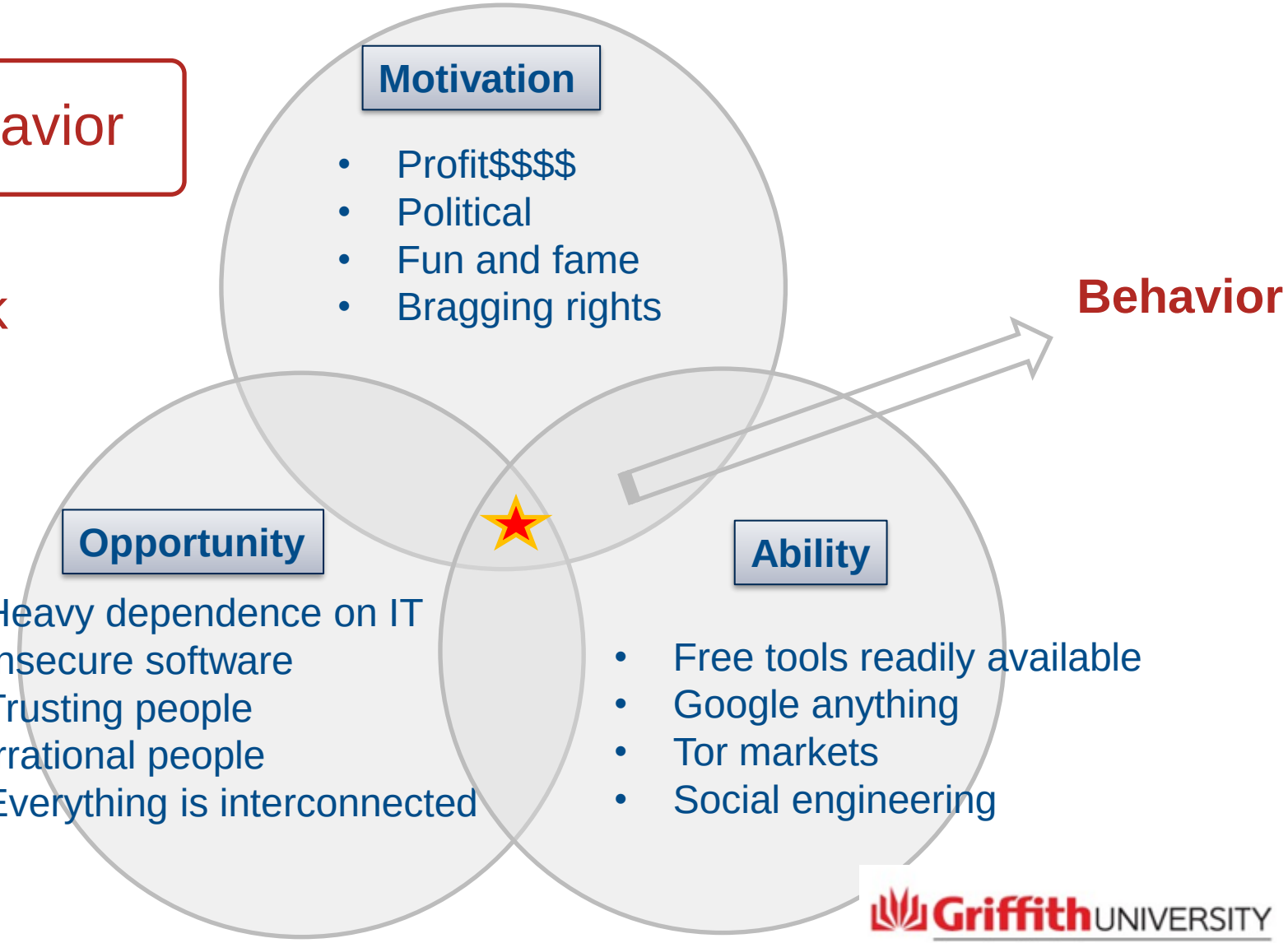
- Trusting human
- Vulnerable software
- Misconfigured systems
- Vulnerable wireless AP

Risks

Why does Cybercrime exist?

Motivation → Behavior

MAO Framework



Griffith UNIVERSITY
Queensland, Australia