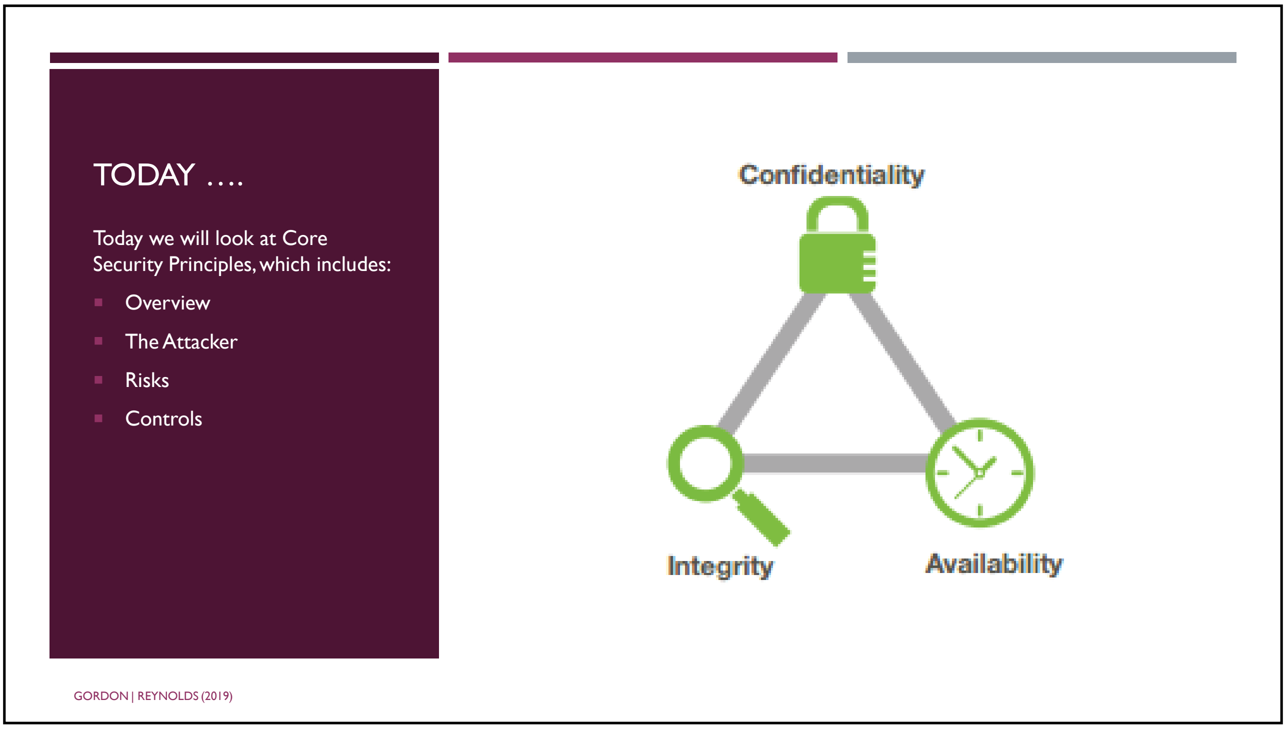
FOUNDATIONS IN IT SECURITY: CIA TRIAD & INFORMATION ASSURANCE

COMPUTER SYSTEMS SECURITY

GORDON | REYNOLDS (2019)



TODAY ….

Today we will look at Core Security Principles, which includes:

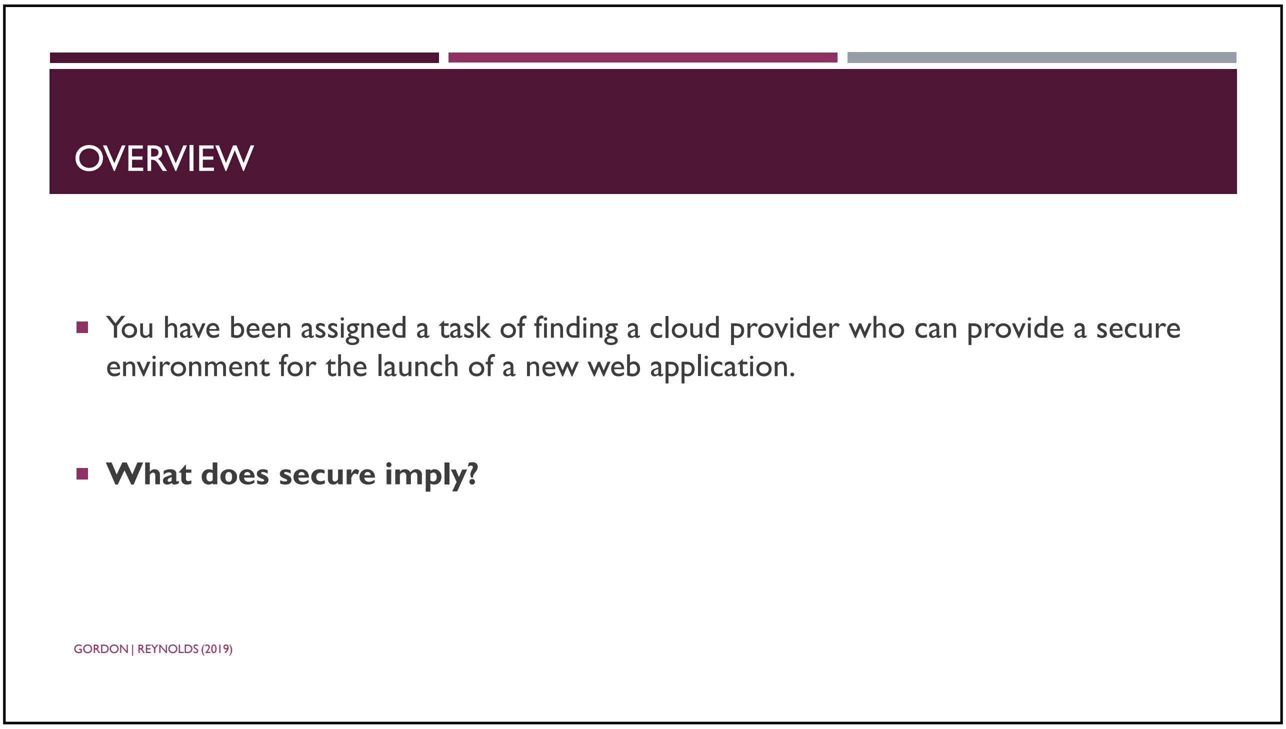
- Overview
- The Attacker
- Risks
- Controls

GORDON | REYNOLDS (2019)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: OVERVIEW

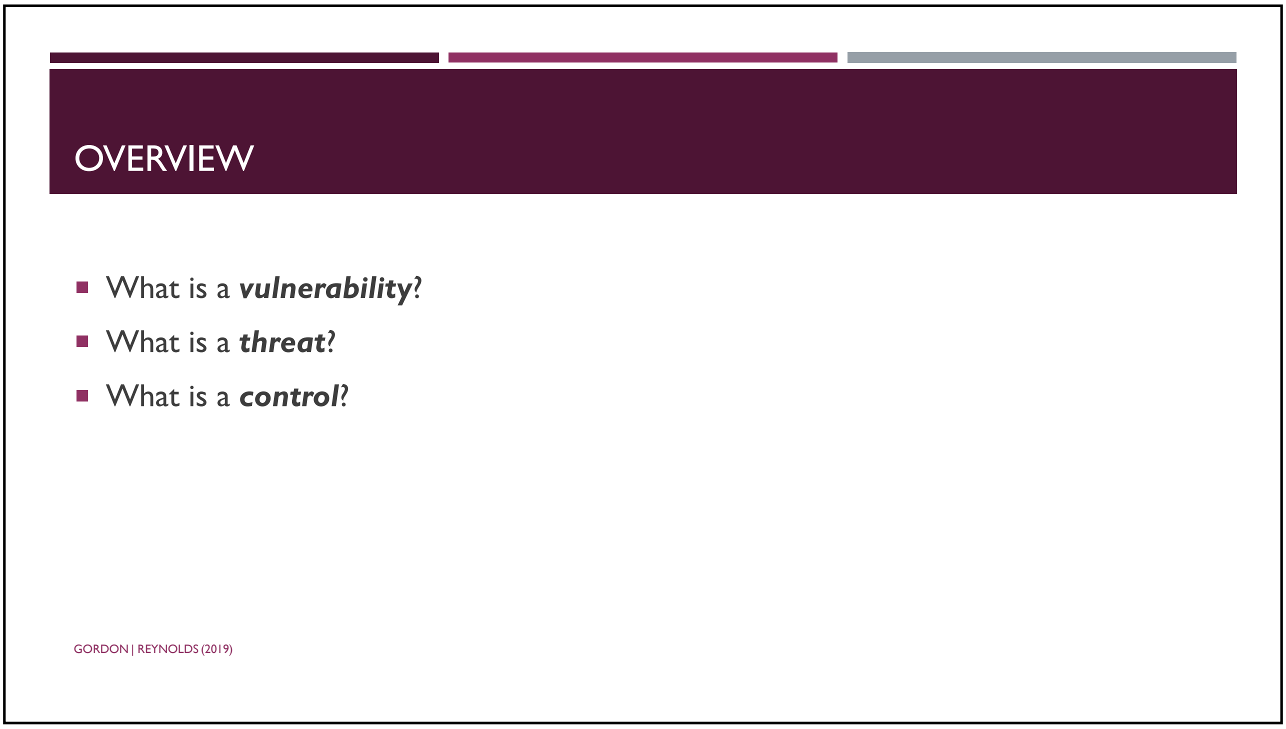
GORDON | REYNOLDS (2018)



OVERVIEW

- You have been assigned a task of finding a cloud provider who can provide a secure environment for the launch of a new web application.
- **What does secure imply?**

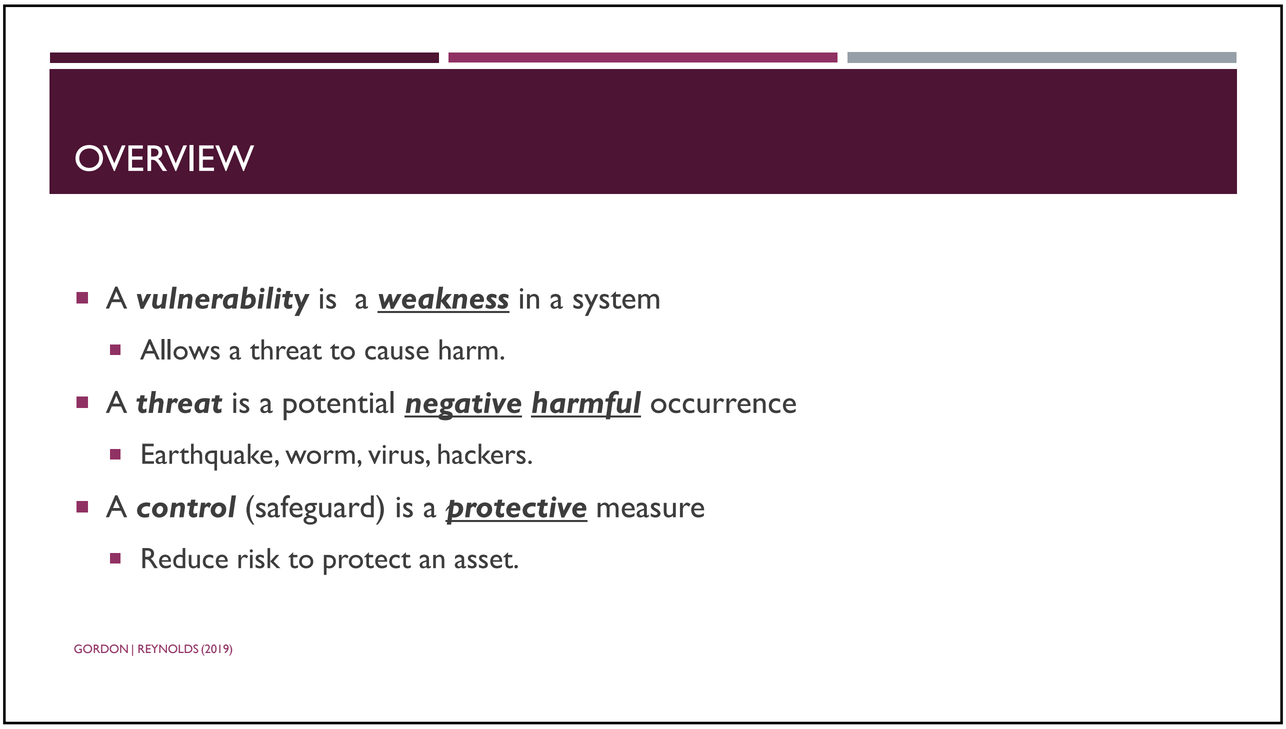
GORDON | REYNOLDS (2019)



OVERVIEW

- What is a ***vulnerability***?
- What is a ***threat***?
- What is a ***control***?

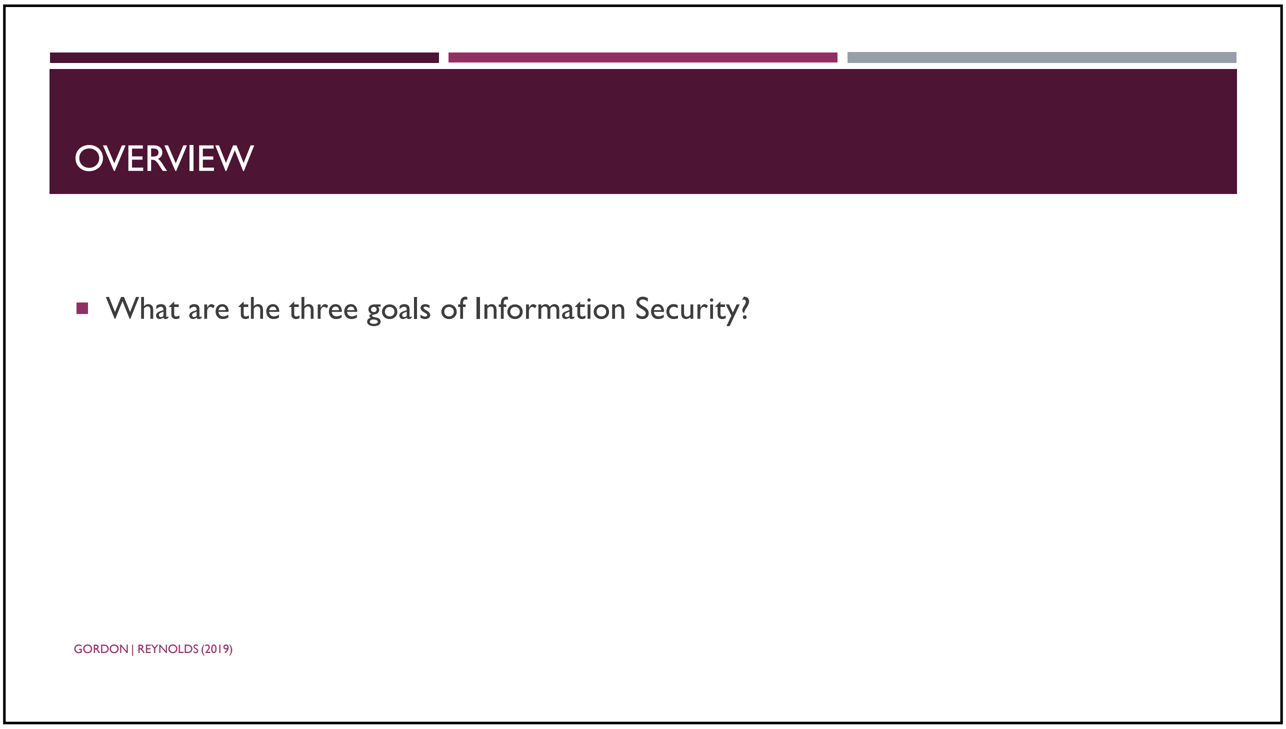
GORDON | REYNOLDS (2019)



OVERVIEW

- A ***vulnerability*** is a ***weakness*** in a system
  - Allows a threat to cause harm.
- A ***threat*** is a potential ***negative*** ***harmful*** occurrence
  - Earthquake, worm, virus, hackers.
- A ***control*** (safeguard) is a ***protective*** measure
  - Reduce risk to protect an asset.

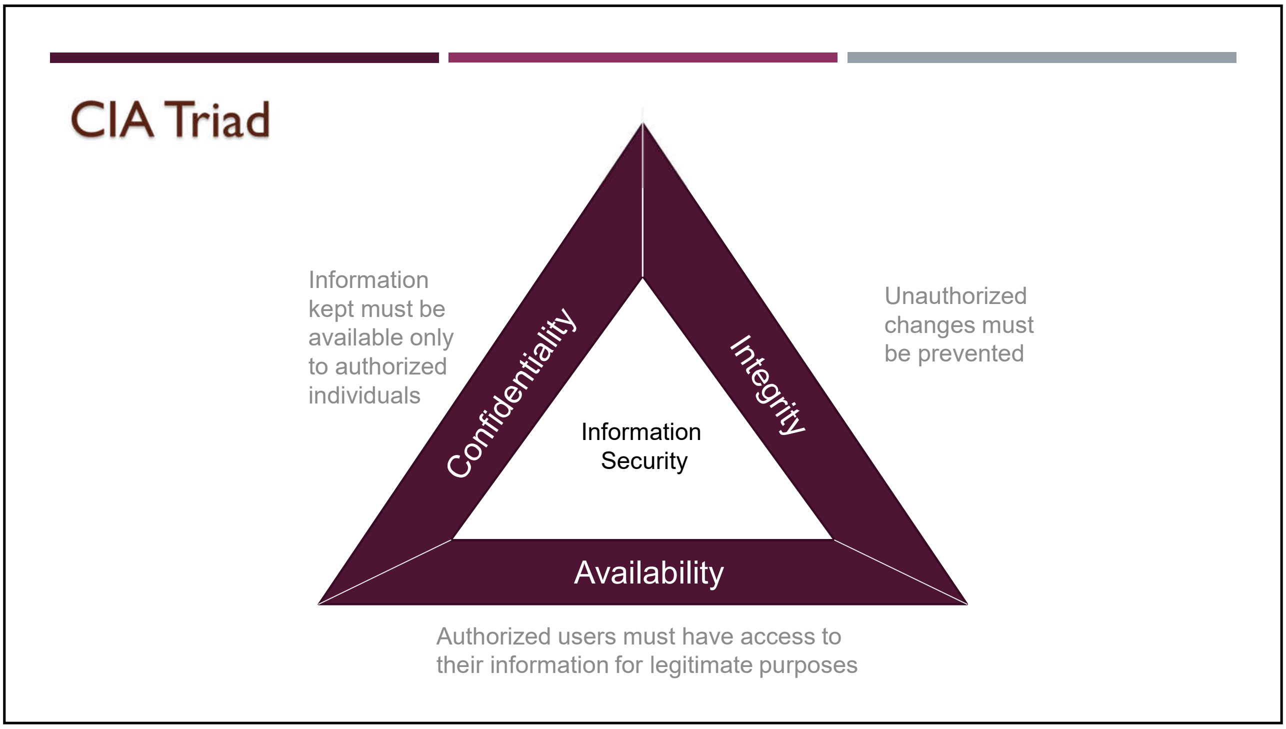
GORDON | REYNOLDS (2019)



OVERVIEW

- What are the three goals of Information Security?

GORDON | REYNOLDS (2019)



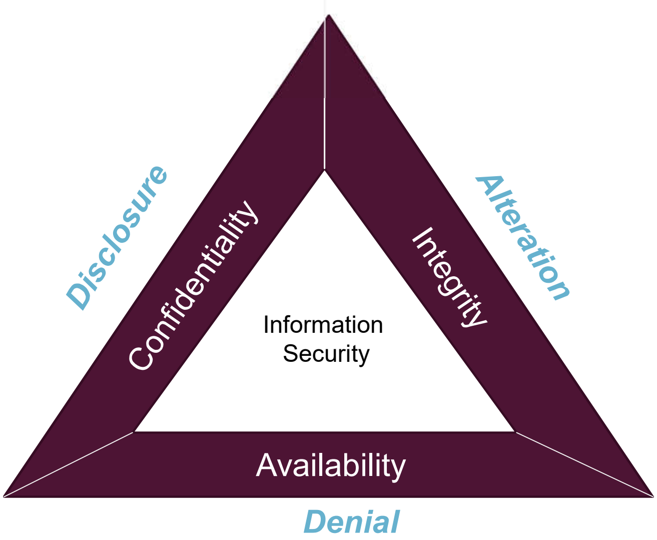
CIA Triad

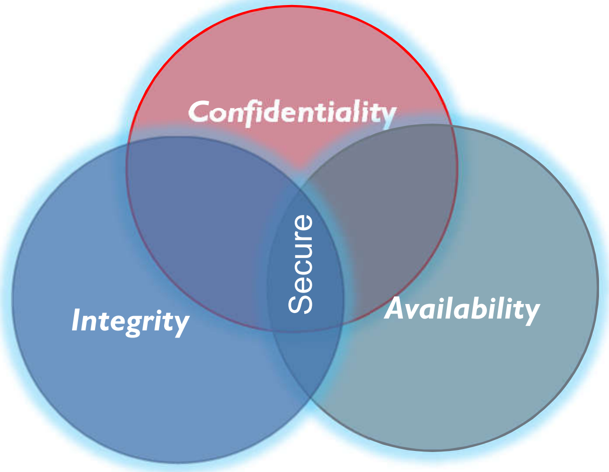
Information kept must be available only to authorized individuals

Unauthorized changes must be prevented

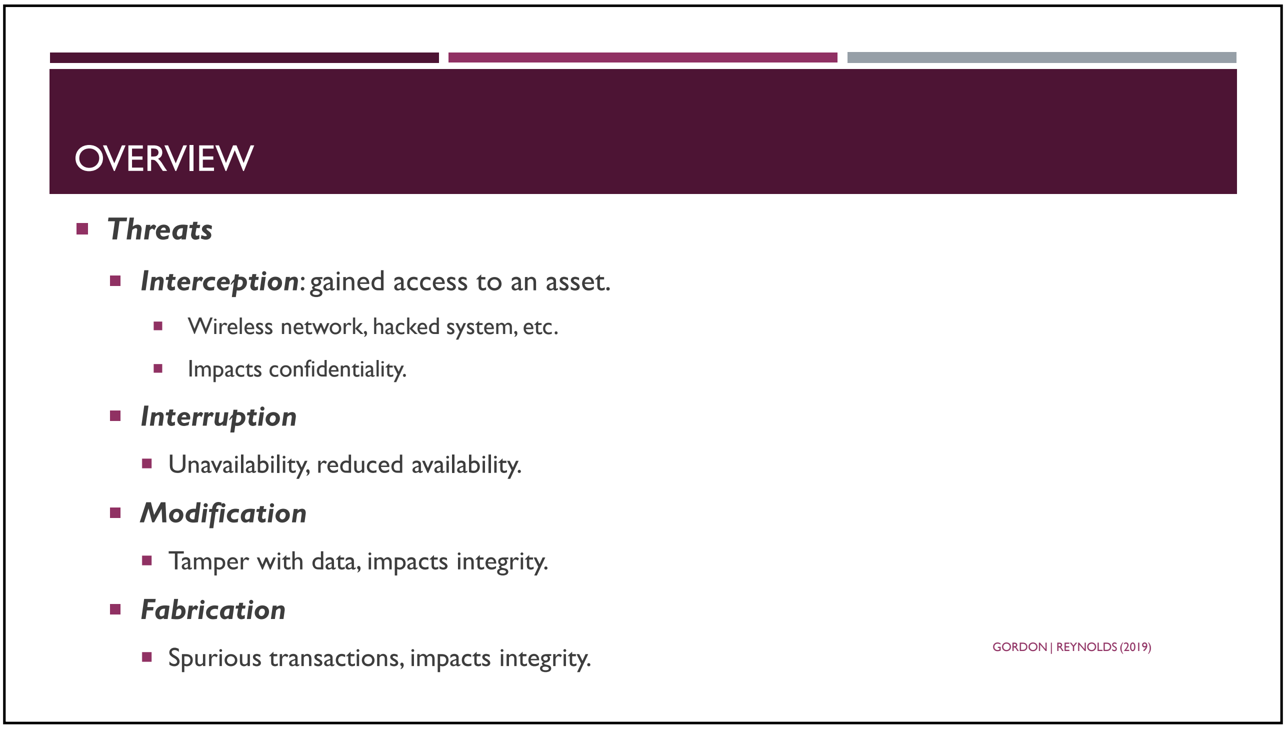
Authorized users must have access to their information for legitimate purposes

Threats





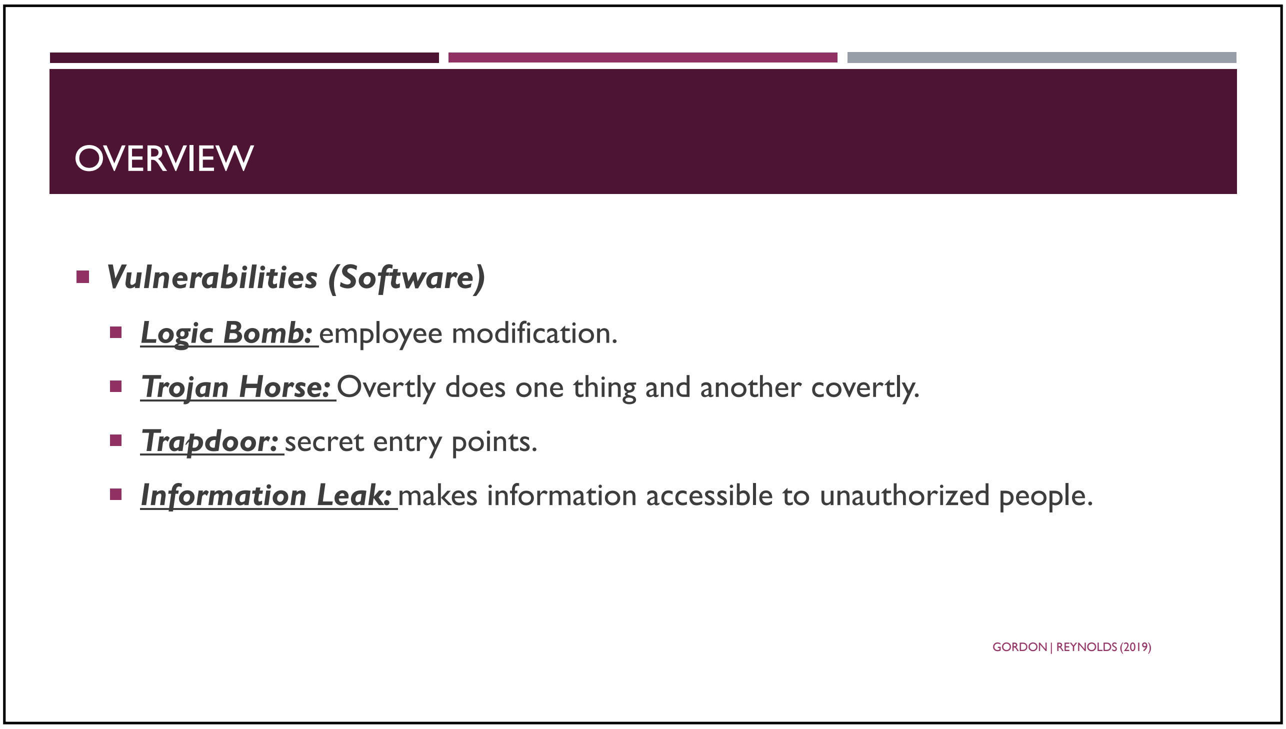
The Relationship Between Confidentiality, Integrity, and Availability.



OVERVIEW

- ***Threats***
  - ***Interception***: gained access to an asset.
    - Wireless network, hacked system, etc.
    - Impacts confidentiality.
  - ***Interruption***
    - Unavailability, reduced availability.
  - ***Modification***
    - Tamper with data, impacts integrity.
  - ***Fabrication***
    - Spurious transactions, impacts integrity.

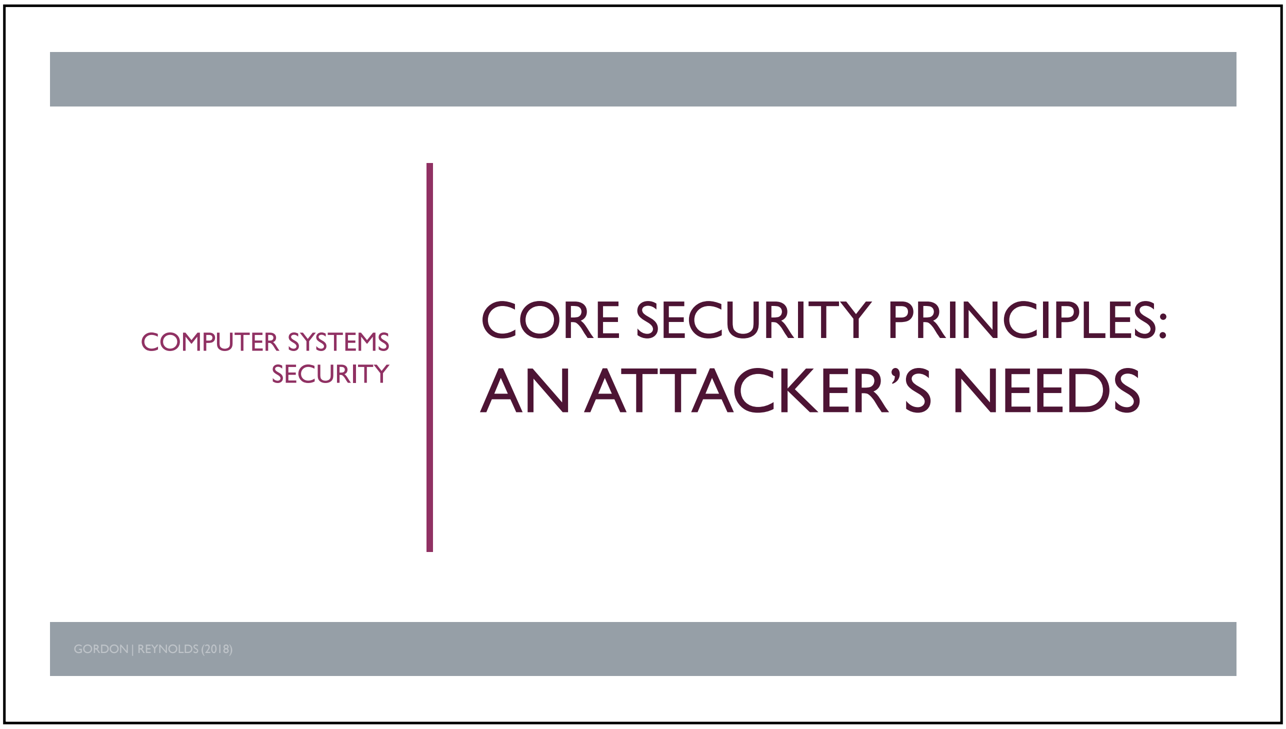
GORDON | REYNOLDS (2019)



OVERVIEW

- ***Vulnerabilities (Software)***
  - ***Logic Bomb:*** employee modification.
  - ***Trojan Horse:*** Overtly does one thing and another covertly.
  - ***Trapdoor:*** secret entry points.
  - ***Information Leak:*** makes information accessible to unauthorized people.

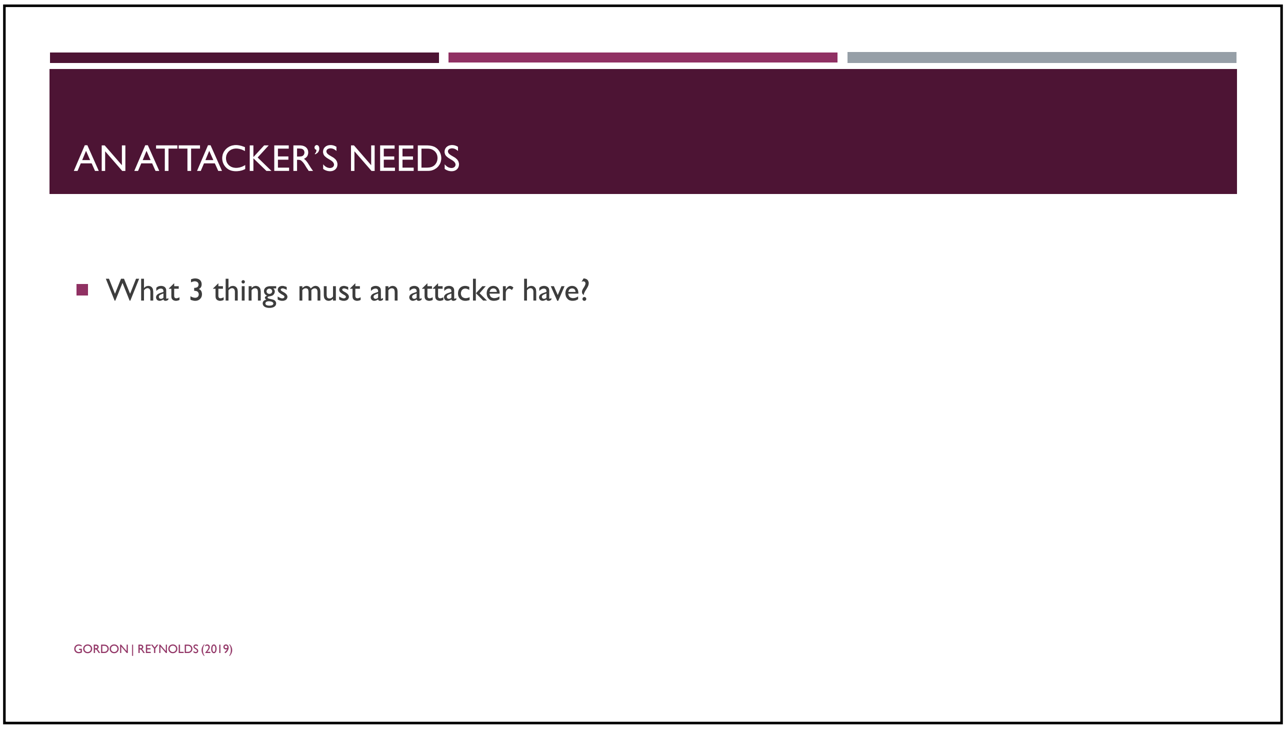
GORDON | REYNOLDS (2019)



COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: AN ATTACKER'S NEEDS

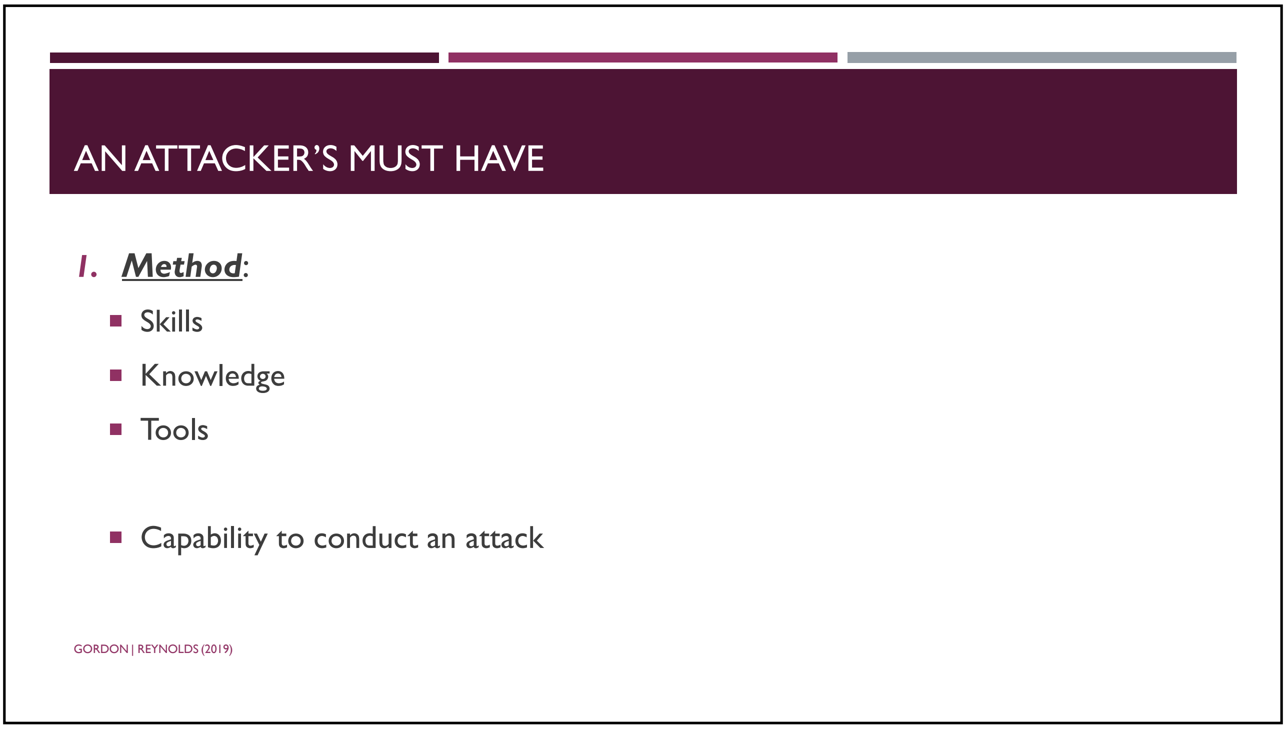
GORDON | REYNOLDS (2018)



AN ATTACKER'S NEEDS

- What 3 things must an attacker have?

GORDON | REYNOLDS (2019)

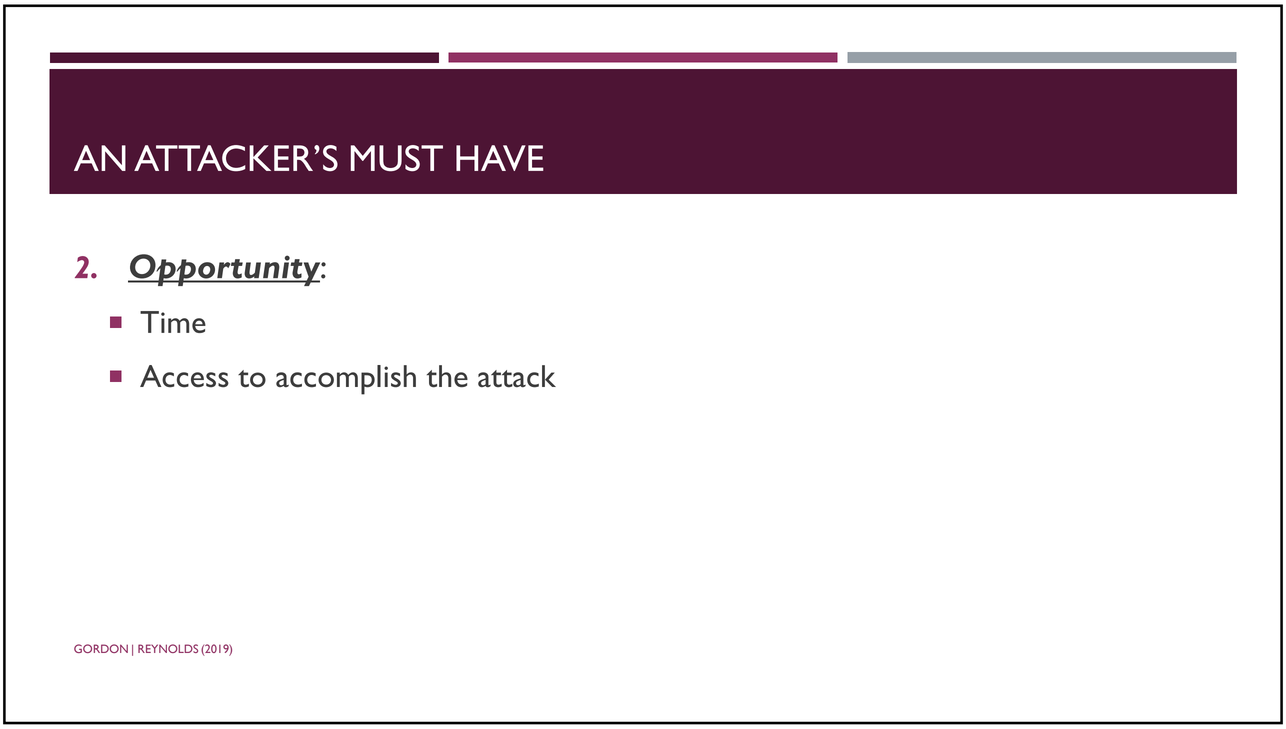


AN ATTACKER'S MUST HAVE

1. ***Method***:
   - Skills
   - Knowledge
   - Tools

   - Capability to conduct an attack

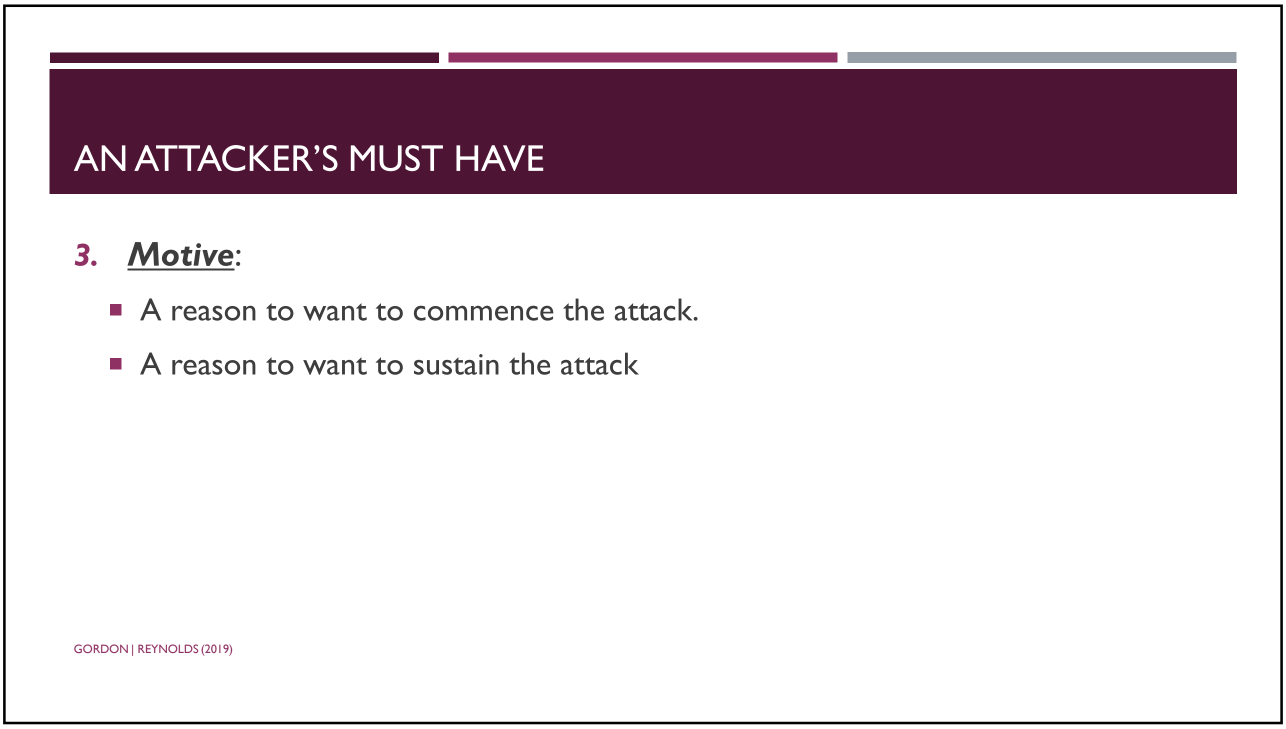
GORDON | REYNOLDS (2019)



AN ATTACKER'S MUST HAVE

2. ***Opportunity***:
   - Time
   - Access to accomplish the attack

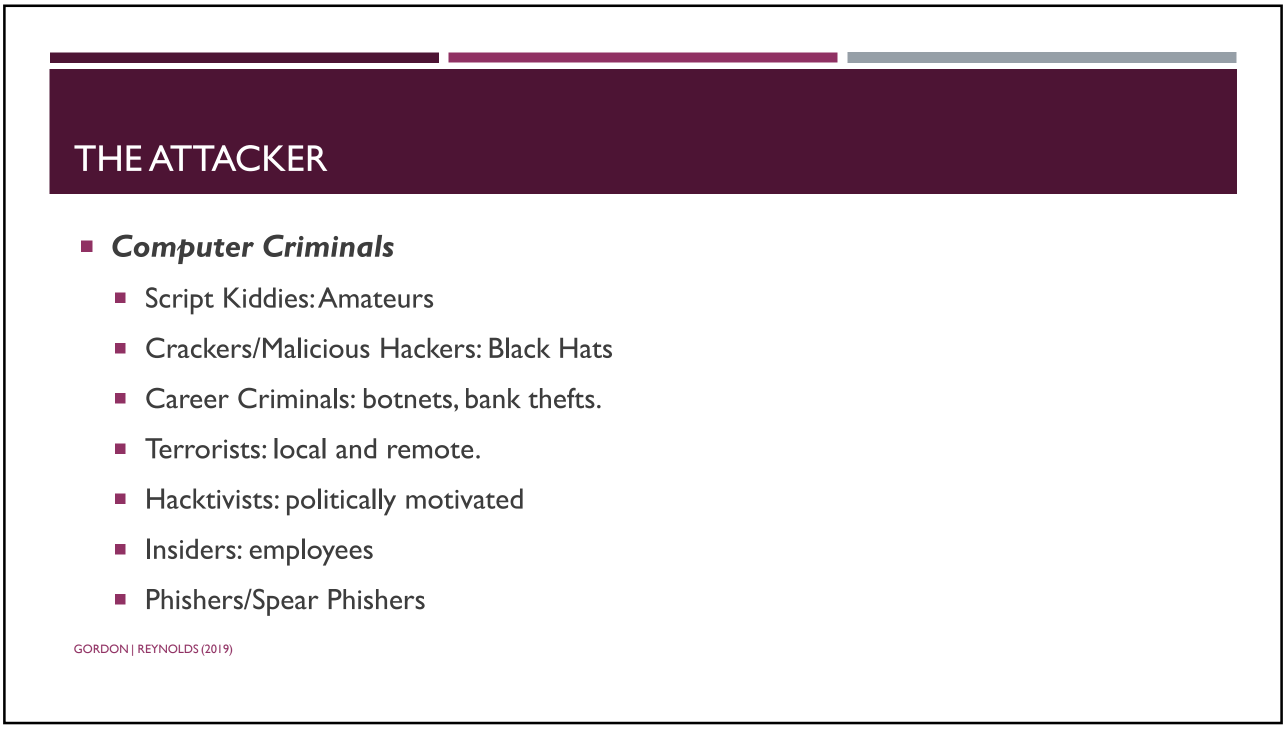
GORDON | REYNOLDS (2019)



AN ATTACKER'S MUST HAVE

3. ***Motive***:
   - A reason to want to commence the attack.
   - A reason to want to sustain the attack

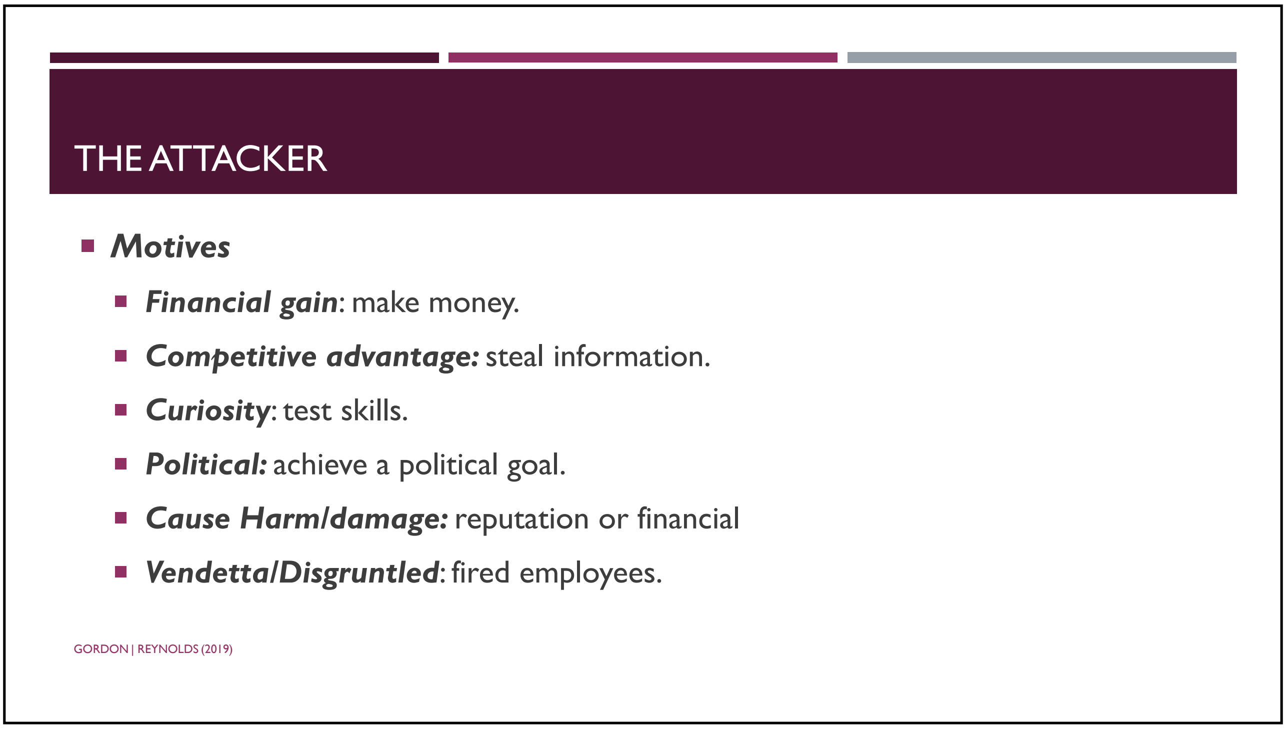
GORDON | REYNOLDS (2019)



THE ATTACKER

- ***Computer Criminals***
  - Script Kiddies: Amateurs
  - Crackers/Malicious Hackers: Black Hats
  - Career Criminals: botnets, bank thefts.
  - Terrorists: local and remote.
  - Hacktivists: politically motivated
  - Insiders: employees
  - Phishers/Spear Phishers

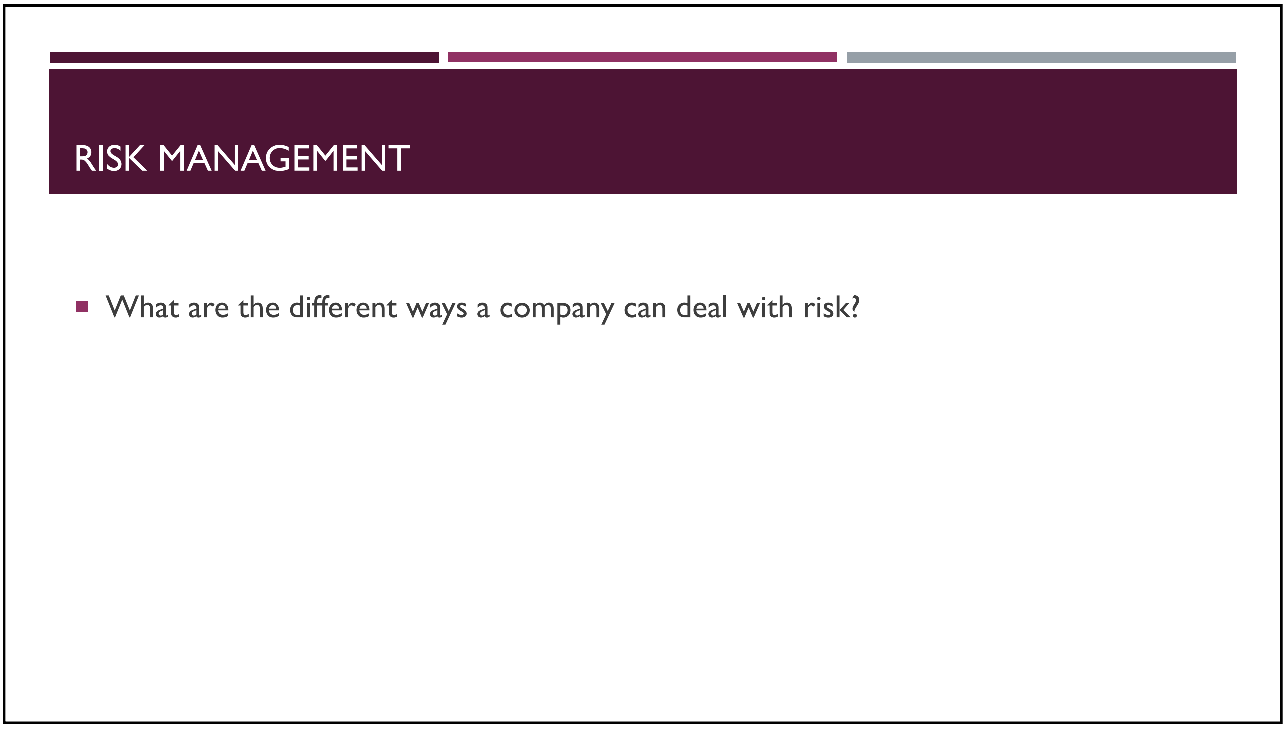
GORDON | REYNOLDS (2019)



THE ATTACKER

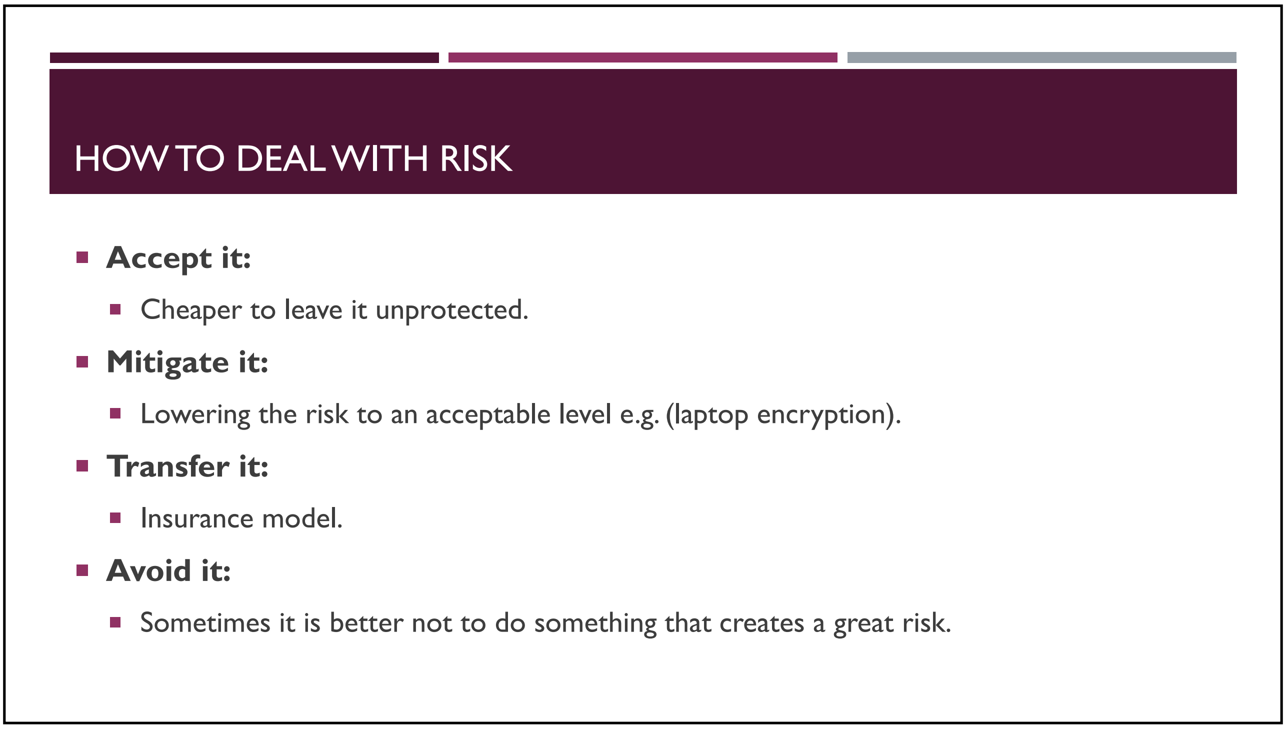
- ***Motives***
  - ***Financial gain***: make money.
  - ***Competitive advantage:*** steal information.
  - ***Curiosity***: test skills.
  - ***Political:*** achieve a political goal.
  - ***Cause Harm/damage:*** reputation or financial
  - ***Vendetta/Disgruntled***: fired employees.

GORDON | REYNOLDS (2019)



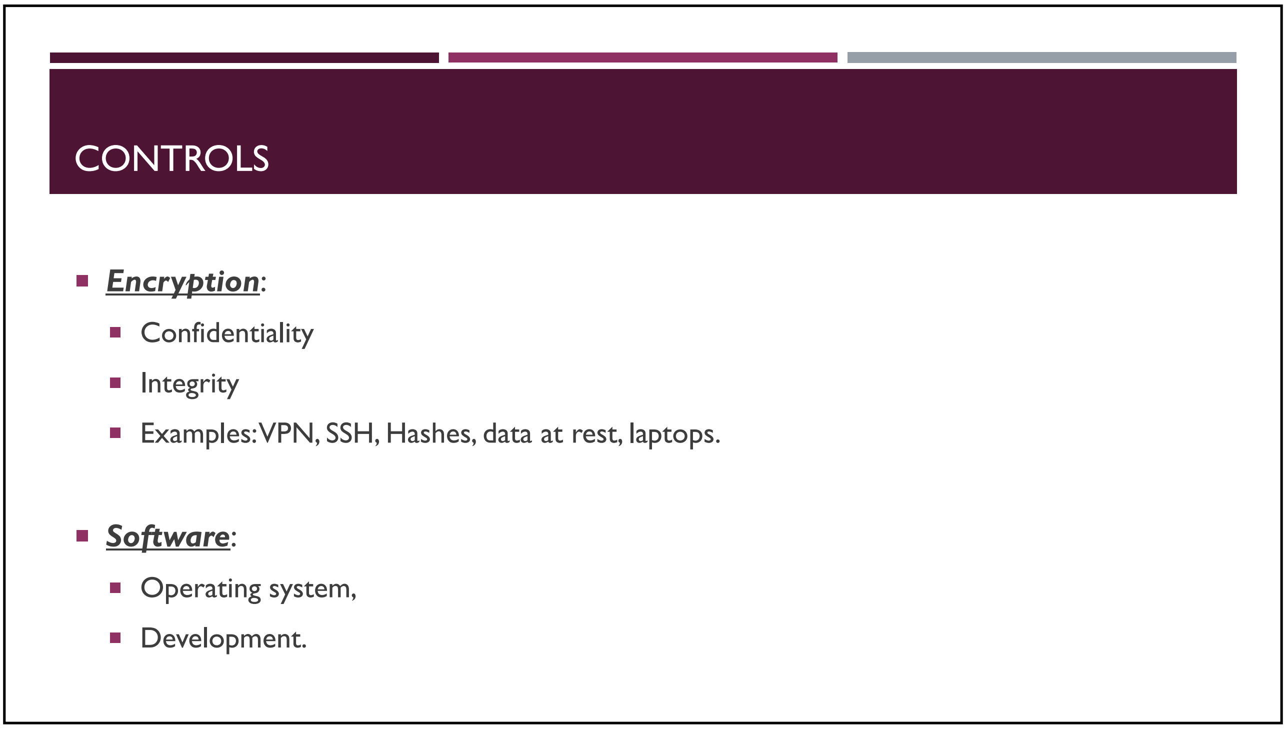
RISK MANAGEMENT

- What are the different ways a company can deal with risk?



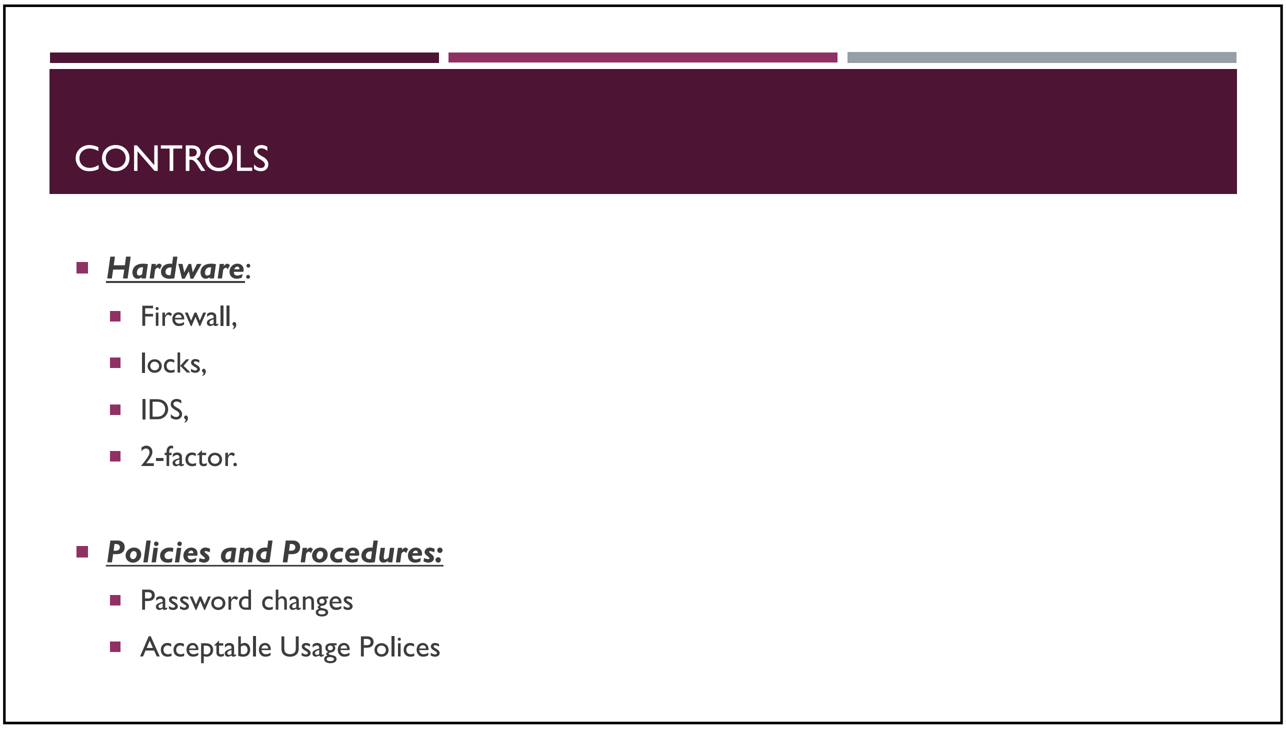
HOW TO DEAL WITH RISK

- **Accept it:**
  - Cheaper to leave it unprotected.
- **Mitigate it:**
  - Lowering the risk to an acceptable level e.g. (laptop encryption).
- **Transfer it:**
  - Insurance model.
- **Avoid it:**
  - Sometimes it is better not to do something that creates a great risk.



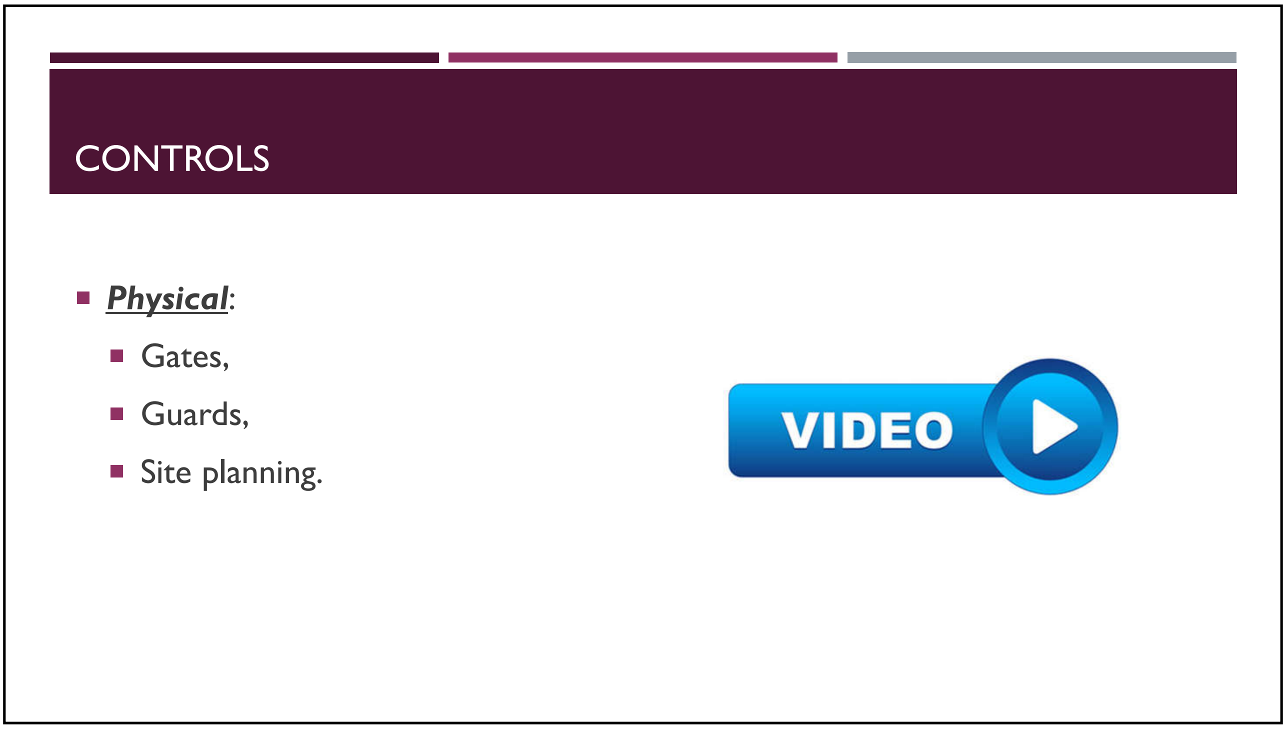
CONTROLS

- ***Encryption***:
  - Confidentiality
  - Integrity
  - Examples:VPN, SSH, Hashes, data at rest, laptops.
- ***Software***:
  - Operating system,
  - Development.



CONTROLS

- ***Hardware***:
  - Firewall,
  - locks,
  - IDS,
  - 2-factor.
- ***Policies and Procedures:***
  - Password changes
  - Acceptable Usage Polices



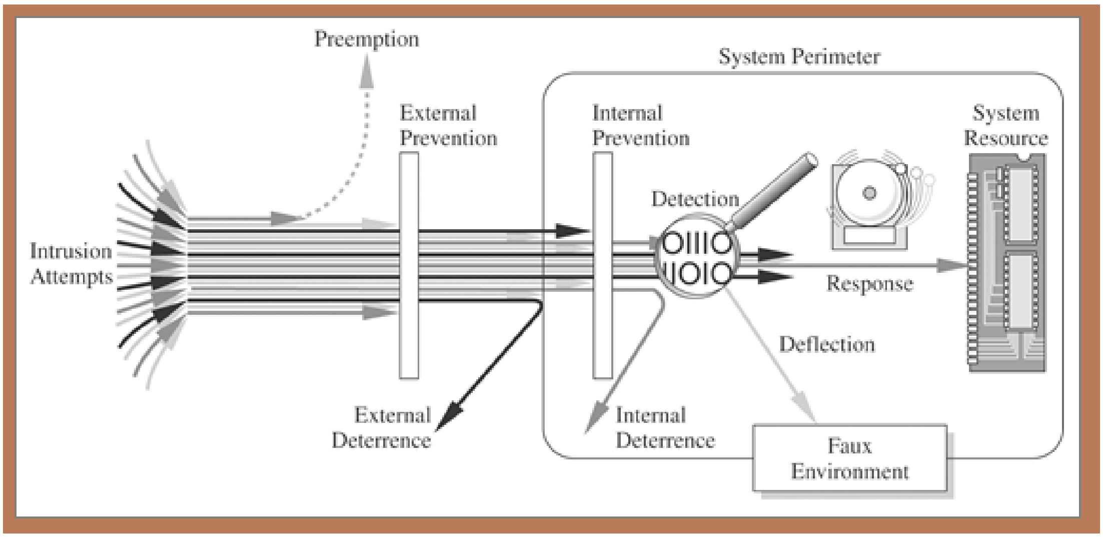
CONTROLS

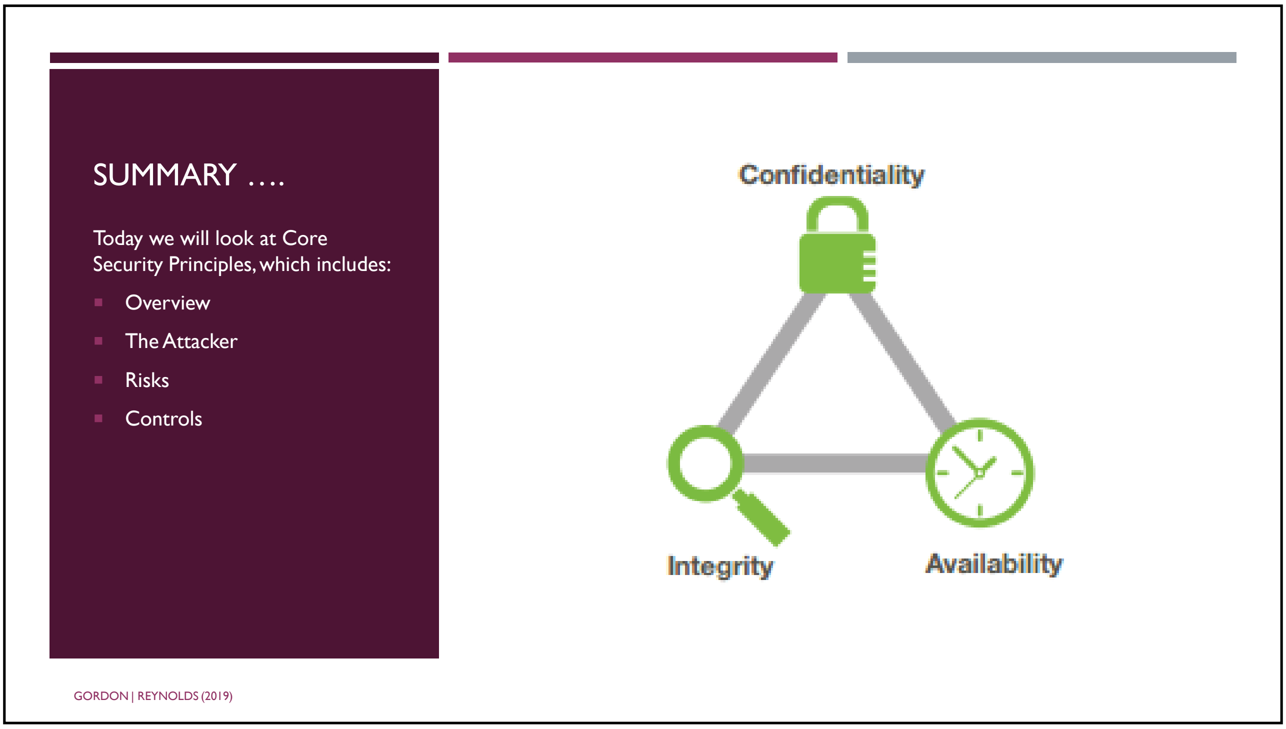
- ***Physical***:
  - Gates,
  - Guards,
  - Site planning.

VIDEO

TYPES OF CONTROLS

- ***Preventive***: prevent actions.
- ***Detective***: notice & alert.
- ***Corrective***: correcting a damaged system.
- ***Recovery***: restore functionality after incident.
- ***Deterrent***: deter users from performing actions.
- ***Compensating***: compensate for weakness in another control.





SUMMARY ….

Today we will look at Core Security Principles, which includes:

- Overview
- The Attacker
- Risks
- Controls

Confidentiality
Integrity
Availability

GORDON | REYNOLDS (2019)