**Computer Security**

* Processes and mechanisms by which computer based equip-

ment, information, and services are protected from unintended

or unauthorized access, change or destruction.

* Computer security also includes protection from unplanned events

and natural disasters.

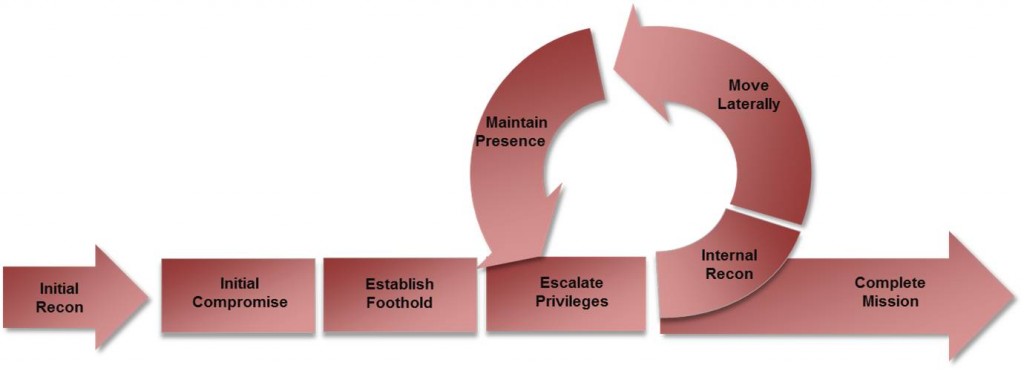
* Cyber Security refers to the technologies, processes, and prac-

tices designed to protect networks, devices, applications, and

data from any cyber-attacks. Cyber security may also be known

as information technology (IT) security.

**Attack Life Cycle**



**Cybersecurity Framework**

A baseline of network operations and expected data flows for

users and systerns is established and managed

Detected events are analyzed to understand attack targets and

Methods. Event data are aggregated and correlated from multiple sources

and sensors. Impact of events is determined. Incident alert thresholds are established

**Causes of Security Related Issue**

* Protocol Error: No one gets it right the first time.
* Software Bugs: Is it a bug or feature?
* Active Attack: Targeting specific devices, BotNets, DDoS (amplification attacks).
* Configuration Mistakes: Very common form of problem.

**Passive VS Active Attacks**

* Passive Attacks
  + Eavesdropping.
  + Offline cryptographic attacks.
* Active Attacks
  + Replay
  + Man-In-The-Middle.
  + Message Insertion.
  + Spoofing (device or user).
  + Denial of Service.
  + Protocol specific attacks.

**What are we trying to protect?**

* Infrastructure: Routers, switches, and associated data
* Hosts, services, Mail, DNS, ...
* Data: Files, databases, .. .
* Users: Passwords, privileged accesses

**The CIA Triad**

Chart, radar chart

Description automatically generated

* Confidentiality: Access to information is restricted to those who are privileged to see it.
* Integrity: Having trust that information has not been altered during its transit from sender to intended recipient.
* Availability: Information or resources are accessible when required.

**Security Services**

* Authentication: Process of verifying the claimed identity of a device, user/application.
* Authorization: Rights and permissions granted to a user, device or application that enables access to resources.
* Access Control: Means by which authorized user has access to resources.
* Encryption: Mechanism by which information is kept confidential.
* Auditing: Process that keeps track of networked activity.

**Policy Framework**

* Typical policy framework for a University is an "Acceptable Use Policy"
* AUP: Allowed Activity, Disallowed Activity, Monitoring, Conse-
* quence, Processs.
* Typical: Computing and network for University-related use only.
* Typical: Shall not interfere with use of computing, network of others. Copyright must be respected, Violators be denied access. Use of computing and network is not private and can be monitored by IT Staff.
* Policy is important as it is a question of behaviour and discipline, not technology.

**The Age of Artificial Intelligence and Machine Learning**

* The goal of ML is to identify and exploit hidden patterns in "training" data.The patterns learnt are used to analyse unknown data, such that it can be grouped together or mapped to the known groups.