**Introduction to Cybersecurity**

**Cybersecurity Fundamentals**

**Learning Objectives**

****

By the end of lessons you will be able to:

Explain the fundamentals of cybersecurity Identify threat actors, attacks, and mitigation

Describe security policies, procedures, standards, and baseline 

Elaborate the cybersecurity mitigation methods

**Fundamentals of Cybersecurity**

**What Is Cybersecurity?**

****

A set of technologies used for protecting systems, networks, and programs from digital attacks, damage, and unauthorized access.

**Unauthorized**

**Attack** 

**Address Threats**

**Access**

**Damage**

**Why Cybersecurity?**

****

Presence of crime

syndicates

Increased demand

to protect data

Increased rate

of cyber crime

The world relies on technology more

than ever before, and as a result digital

data creation has surged.

Presence of cyber

armies

Presence of

financial frauds

**Information Security and Cybersecurity**

****

**Information Security**

Refers to processes and tools designed to protect sensitive information

Encompasses paper documents and digital and intellectual property

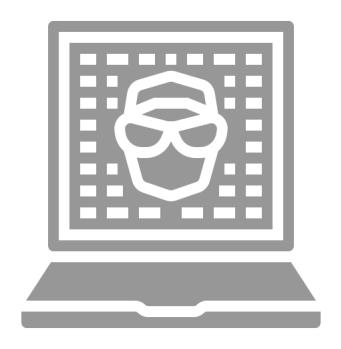
**Cybersecurity**

Is a set of techniques used to protect the integrity of networks, programs, and data

Is a component of information security

**Cyber Crime Statistics**

****

25+ million records 

exposed everyday in

2018

Cyber Crime to cost

$6 trillion in 2021

Healthcare:

Ransomware attacks

will quadruple

300 billion passwords exist worldwide in 2020

24,000 malicious

mobile apps blocked daily

60% of fraud

originates from

mobile devices

**Factors Affecting Cybersecurity**

****

**Technology Business Plans**

**1**

Platforms and tools

Network connectivity

**2**

Level of IT complexity

**3**

**4**

New or emerging security tools Operational support for security **5**

Nature of business

Risk tolerance

Industry trends

Mergers and acquisitions and partnerships Outsourcing service providers

**CIA Triad**

****

Information must be available

on demand

**CIA Triad**

****

Authorized parties can 

access the information

**CIA Triad**

****

Authorized people can add, 

remove, or alter information

**Governance, Risk Management, and Compliance (GRC)**

**Scope of GRC**

****

Governance, Risk Management, and Compliance of every organization is different and varies based on the type of organization.

It depends on organization mission, size, industry, culture, and legal regulations.



Mission Regulations Size



Culture Industry

**Responsibility of GRC**

****

The ultimate responsibility of the GRC program is to protect their assets and operations IT, including their infrastructure and information.



**Governance**

Risk Management Compliance

**GRC**

****

The board of directors and senior management of an organization are responsible for Governance.

Provides strategic direction 

Ensures that the objectives are achieved

Ascertains whether **risk** is being managed

appropriately

Verifies that the organization's resources are being

used responsibly

**GRC**

****

It is the process by which the organization manages risks to acceptable

levels. These risks may include investment risk, physical risk, and cyber risk.

Governance

**Risk Management** 

Compliance

**GRC**

****

It is the act of adhering to mandated requirements defined by laws and

regulations.

Governance 

Risk Management

**Compliance**

**Roles of Cybersecurity**

**Cybersecurity Roles**

****

The success of a cybersecurity role is ultimately the responsibility of the board of directors.

Board of Directors

Executive

Committee



Security

Management

Cybersecurity Practitioners

**Approaches to Cybersecurity**

****

****

**Compliance-based security Risk-based security Ad-hoc approach**

**Cybersecurity: Key Terms**

****

**Cybersecurity: Key Terms**

****Inherent risk 

Residual risk

**Illustration: Basics of Cybersecurity**

****

****

**Threat Actors, Attacks, and Mitigation**

**Threat Actor**

****

A threat actor or malicious actor is a person or entity that is responsible for an event or incident that impacts or has the potential to impact the safety or security of another entity.



**Threat Actor Categories**

****

Script kiddies Hactivist 

**Threat Actor categories are:**

****Nation states APT Insiders

Organized crime Competitors

**Threats to a System**

****Main threats to an organization should be considered.

Natural

environmental threats

Supply system threats

Man-made threats

Sociopolitical threats



**Malware**

****

Malware is any software that is intentionally designed to cause damage to a computer, server, client, or computer network.



Worms Viruses Trojans Spyware

Adware

**Types of Malware**

****

Rootkit

Backdoor

Logic bombs

Ransomware

**Worms**

****

Worms are self-replicating codes designed to penetrate computer systems.

**Virus**

****

Virus is a malicious code that replicates by attaching to an executable code.

**Trojans**

****

Trojans are programs that claim to perform one function but does another, typically malicious.



**Spyware**

****

Spyware is a software aimed to steal personal or organizational information.

**Adware**

****

Adware is a software that displays endless ads and pop-up windows.

**Rootkit**

****

Rootkits are designed to modify the operating systems’ operations to facilitate non-standard functionality. 

**Backdoor**

****

Backdoor provides the attacker with unauthorized remote access to a system by exploiting security vulnerabilities.



**Logic Bombs**

****

Logic bombs infect a system and lie dormant until they are triggered by a specific condition.

**Ransomware**

****

Ransomware attempts to extort money from the user by infecting and taking control of a victim's machine.

**Malware Attacks**

****

****Kovter WannaCry Zeus or Zbot



Ghost Mirai

**Denial-of-Service Attack**

****

The purpose of DoS is to prevent access to the target system.



**Distributed Denial-of-Service**

****

It is a denial-of-service attack employing multiple attacking systems.



**Distributed Denial-of-Service**

****

The goal of DDoS is to prevent access to a specific system.



**DoS/DDoS Attacks**

****

**GitHub: 1.35 Tbps**

****GitHub was hit with 1.35 terabits per

second of traffic.

**DoS/DDoS Attacks**

****

**Cloudflare: 400 Gbps**

****The attack was directed at a single computer with vulnerability.

**Application Layer Attacks**

****

They target computers by causing a fault in the operating system or applications.

**Application Layer Attacks**

****

They refer to a type of malicious behavior designed to target the top layer in the OSI model.

**Application Layer Attacks**

****

****Cross-site scripting Buffer overflow Domain hijacking

DNS spoofing SQL injection DoS/DDoS

**Software Codes and Security**

****Programmers are responsible to write safe and high quality codes.



**Software Codes and Security**

****Source codes are statements written using a computer programming language.



**Software Codes and Security**

****

Code review is a systematic examination or peer review of source code. Find mistakes Improve software quality

**Software Testing Methods**

****

Evaluates the security of

software in a runtime

environment

**Static Testing**

**Dynamic Testing**

Evaluates the security of

software without running it

**Software Testing Methods**

****

In March 2018, hackers hit Saks Fifth Avenue and Lord & Taylor, stealing debit and credit cards. 5 million records breached

**Software Testing Methods**

****

In May 2018, the concert and sporting event ticketing website, **ticketfly** was vandalized, taken down, and disrupted for a week.



**Security Attacks**

****

In August 2018, Russian hackers made millions selling credit card details stolen from almost 245,000 British Airways customers.



**Social Engineering**

****

It is the art of manipulating people, so they give up their confidential information violating the security principle.



**Social Engineering Attack Categories**

****There are several attack categories of social engineering.

Spear Phishing

Phishing Whaling Phishing

**Social Engineering Attack Categories**

****

**Phishing Spear Phishing Whaling Phishing**

It is a fraudulent attempt to obtain sensitive information.

It is targeted to a specific group or an individual.

It targets wealthy and prominent individuals.

**Social Engineering Attack: Ethereum Classic**

****

In 2017, Ethereum Classic website was hacked resulting in the loss of thousands of dollars in cryptocurrency.



**Social Engineering Attack: Ethereum Classic**

****

Impersonated Ethereum owner

Redirected the domain to their server



Gained access to domain registry

Extracted cryptocurrency from the victims

**Security Policies and Procedures**

Initiates and defines

policies

Releases standards and

**Security Management Plan**

****Senior Management

policy guidelines

Implements the controls

and policies

Middle Management

Operations Management/IT Team

End Users

Must comply with the

organization’s functions

**Types of Security Management Plan**

****

****Strategic Plan Tactical Plan Operational Plan

**Types of Security Management Plan**

****

****Strategic Plan Tactical Plan Operational Plan

● Is a long-term plan

● Defines security posture

● Is valid for five years and is

renewed annually

● Helps understand security

functions

● Helps in risk assessment

**Types of Security Management Plan**

****

****Strategic Plan Tactical Plan Operational Plan

● Is a mid-term plan

● Provides detailed goals

● Is updated every year or two

● Is technology oriented

**Types of Security Management Plan**

****

****Strategic Plan Tactical Plan Operational Plan

● Is a short-term plan

● Is highly detailed

● Is updated monthly or

quarterly

● Spells out how to accomplish

goals

**Security Policy**

****

• Is a strategic plan

• Defines the scope of security 

• Outlines security objectives

and framework

• Identifies the functional areas

• Outlines security goals and

practices

• Assigns responsibilities and requirements

• Defines risk levels

**Types of Security Policy**

****

Focuses on issues relevant to every

aspect of the organization

Organizational

policy

Issue-specific policy

System-specific

policy

Focuses on individual

systems Focuses on a specific service, department, or function

**Security Policy Framework**

****

**Standard** 

**Procedure**

**Guideline Baseline**

● Defines the minimum level of security

● Is system specific

● Establishes the common secure state

**Security Policy Framework**

****

**Standard** 

**Procedure** ● Offers recommendations on implementation

● Serves as an operating guide

**Guideline Baseline**

● Is customized for each unique system

**Security Policy Framework**

****

**Standard**

● Is the final element of formalized

security policy structure

**Procedure Guideline Baseline** 

● Describes actions for implementing the security mandates

● Is system and software specific

● Ensures integrity of the business process

**Security Policy Framework**

****● Defines the compulsory

**Standard Procedure Guideline Baseline** 

requirements

● Provides a course of action ● Is a tactical document

**Due Care and Due Diligence**

**Due Care Due Diligence**

● Reasonable care is taken in protecting the organization

● Pertains to the legal duty of the organization

● Lack of due care is considered negligence

● Is about practicing the activities that maintain the due care effort

● Pertains to best practices that a company should follow

● Might not be legally liable

**Cybersecurity Mitigation Methods**

**Information Technology Control**

****An IT control is a procedure or policy that provides a reasonable assurance that:

IT used by an organization is operating as intended

The organization is in 

compliance with laws

and regulations

Data is reliable

**Countermeasure**

****

It is an action or method that is applied to prevent, avert, or reduce potential threats to:



Computers Networks Operating

Servers Information

systems

systems

**Countermeasure**

****

****It helps to mitigate or reduce the potential risk.

**Control Categories**

****

****

Administrative controls

Technical controls

Physical controls

**Administrative Controls**

****

These are procedures and policies used to define employee actions toward sensitive information.

**Technical Controls**

****

These are procedures and policies used to define employee actions toward sensitive information.

