Introduction to Cybersecurity

©Simplilearn. All rights reserved.

Cybersecurity Fundamentals

©Simplilearn. All rights reserved.

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

©Simplilearn. All rights reserved.

Fundamentals of Cybersecurity

©Simplilearn. All rights reserved.

What Is Cybersecurity?

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

Attack

Unauthorized Access

Address Threats

Damage

©Simplilearn. All rights reserved.

Why Cybersecurity?

©Simplilearn. All rights reserved.

Information Security and Cybersecurity

Information Security	Cybersecurity
Refers to processes and tools designed to protect sensitive information	Is a set of techniques used to protect the integrity of networks, programs, and data
Encompasses paper documents and digital and intellectual property	Is a component of information security

©Simplilearn. All rights reserved.

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

©Simplilearn. All rights reserved.

Factors Affecting Cybersecurity

Technology		Business Plans
Platforms and tools	1	Nature of business
Network connectivity	2	Risk tolerance
Level of IT complexity	3	Industry trends
New or emerging security tools	4	Mergers and acquisitions and partnerships
Operational support for security	5	Outsourcing service providers

©Simplilearn. All rights reserved.

CIA Triad

Information must be available on demand

©Simplilearn. All rights reserved.

CIA Triad

Authorized parties can access the information

©Simplilearn. All rights reserved.

CIA Triad

Authorized people can add, remove, or alter information

©Simplilearn. All rights reserved.

Governance, Risk Management, and Compliance (GRC)

©Simplilearn. All rights reserved.

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

©Simplilearn. All rights reserved.

Responsibility of GRC

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

©Simplilearn. All rights reserved.

GRC

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

Governance

Risk Management

Compliance

- 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

©Simplilearn. All rights reserved.

GRC

Governance

Risk Management

Compliance

It is the process by which the organization manages risks to acceptable levels. These risks may include investment risk, physical risk, and cyber risk.

©Simplilearn. All rights reserved.

GRC

Governance

Risk Management

Compliance

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

©Simplilearn. All rights reserved.

Roles of Cybersecurity

©Simplilearn. All rights reserved.

Cybersecurity Roles

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

©Simplilearn. All rights reserved.

Approaches to Cybersecurity

Compliance-based security

Risk-based security

Ad-hoc approach

©Simplilearn. All rights reserved.

Cybersecurity: Key Terms

©Simplilearn. All rights reserved.

Cybersecurity: Key Terms

Inherent risk

Residual risk

©Simplilearn. All rights reserved.

Illustration: Basics of Cybersecurity

©Simplilearn. All rights reserved.

Threat Actors, Attacks, and Mitigation

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

Threat Actor Categories

©Simplilearn. All rights reserved.

Threats to a System

Main threats to an organization should be considered.

Natural environmental threats

Supply system threats

Man-made threats

Sociopolitical threats

©Simplilearn. All rights reserved.

Malware

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

©Simplilearn. All rights reserved.

Types of Malware

- Worms
- Viruses
- Trojans
- Spyware
- Adware
- Rootkit
- Backdoor
- Logic bombs
- Ransomware

©Simplilearn. All rights reserved.

Worms

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

©Simplilearn. All rights reserved.

Virus

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

©Simplilearn. All rights reserved.

Trojans

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

©Simplilearn. All rights reserved.

Spyware

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

©Simplilearn. All rights reserved.

Adware

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

©Simplilearn. All rights reserved.

Rootkit

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

Rootkit

©Simplilearn. All rights reserved.

Backdoor

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

©Simplilearn. All rights reserved.

Logic Bombs

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

©Simplilearn. All rights reserved.

Ransomware

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

©Simplilearn. All rights reserved.

Malware Attacks

Kovter

WannaCry

Zeus or Zbot

Ghost

Mirai

©Simplilearn. All rights reserved.

Denial-of-Service Attack

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

©Simplilearn. All rights reserved.

Distributed Denial-of-Service

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

©Simplilearn. All rights reserved.

Distributed Denial-of-Service

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

©Simplilearn. All rights reserved.

DoS/DDoS Attacks

GitHub: 1.35 Tbps

GitHub was hit with 1.35 terabits per second of traffic.

©Simplilearn. All rights reserved.

DoS/DDoS Attacks

Cloudflare: 400 Gbps

The attack was directed at a single computer with vulnerability.

©Simplilearn. All rights reserved.

Application Layer Attacks

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

©Simplilearn. All rights reserved.

Application Layer Attacks

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

©Simplilearn. All rights reserved.

Application Layer Attacks

Cross-site scripting

Buffer overflow

Domain hijacking

DNS spoofing

SQL injection

DoS/DDoS

©Simplilearn. All rights reserved.

Software Codes and Security

Programmers are responsible to write safe and high quality codes.

©Simplilearn. All rights reserved.

Software Codes and Security

Source codes are statements written using a computer programming language.

©Simplilearn. All rights reserved.

Software Codes and Security

Code review is a systematic examination or peer review of source code.

Find mistakes

Improve software quality

©Simplilearn. All rights reserved.

Software Testing Methods

Evaluates the security of software in a runtime environment

Evaluates the security of software without running it

©Simplilearn. All rights reserved.

Software Testing Methods

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

5 million records breached

©Simplilearn. All rights reserved.

Software Testing Methods

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

©Simplilearn. All rights reserved.

Security Attacks

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

BRITISH AIRWAYS

©Simplilearn. All rights reserved.

Social Engineering

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

©Simplilearn. All rights reserved.

Social Engineering Attack Categories

There are several attack categories of social engineering.

©Simplilearn. All rights reserved.

Social Engineering Attack Categories

Phishing

It is a fraudulent attempt to obtain sensitive information.

Spear Phishing

It is targeted to a specific group or an individual.

Whaling Phishing

It targets wealthy and prominent individuals.

©Simplilearn. All rights reserved.

Social Engineering Attack: Ethereum Classic

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

©Simplilearn. All rights reserved.

Social Engineering Attack: Ethereum Classic

Impersonated Ethereum owner

Redirected the domain to their server

Gained access to domain registry

Extracted cryptocurrency from the victims

©Simplilearn. All rights reserved.

Security Policies and Procedures

©Simplilearn. All rights reserved.

Security Management Plan

©Simplilearn. All rights reserved.

Types of Security Management Plan

Strategic Plan

Tactical Plan

Operational Plan

©Simplilearn. All rights reserved.

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

©Simplilearn. All rights reserved.

Types of Security Management Plan

Strategic Plan

Tactical Plan

- Is a mid-term plan
- Provides detailed goals
- Is updated every year or two
- Is technology oriented

Operational Plan

©Simplilearn. All rights reserved.

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

©Simplilearn. All rights reserved.

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

©Simplilearn. All rights reserved.

Types of Security Policy

Focuses on issues relevant to every aspect of the organization

Organizational policy

Issue-specific policy

System-specific policy

Focuses on a specific service, department, or function

Focuses on individual systems

©Simplilearn. All rights reserved.

simplilearn

Security Policy Framework

- Defines the minimum level of security
- Is system specific
- Establishes the common secure state

©Simplilearn. All rights reserved.

Security Policy Framework

- Offers recommendations on implementation
- Serves as an operating guide
- Is customized for each unique system

©Simplilearn. All rights reserved.

Security Policy Framework

- Is the final element of formalized security policy structure
- Describes actions for implementing the security mandates
- Is system and software specific
- Ensures integrity of the business process

©Simplilearn. All rights reserved.

Security Policy Framework

- Defines the compulsory requirements
- Provides a course of action
- Is a tactical document

©Simplilearn. All rights reserved.

Due Care and Due Diligence

Due Care

- Reasonable care is taken in protecting the organization
- Pertains to the legal duty of the organization
- Lack of due care is considered negligence

Due Diligence

- 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

©Simplilearn. All rights reserved.

Cybersecurity Mitigation Methods

©Simplilearn. All rights reserved.

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

©Simplilearn. All rights reserved.

Countermeasure

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

Computers

Networks

Servers

Operating systems

Information systems

©Simplilearn. All rights reserved.

Countermeasure

It helps to mitigate or reduce the potential risk.

©Simplilearn. All rights reserved.

Control Categories

Administrative controls

Technical controls

Physical controls

©Simplilearn. All rights reserved.

Administrative Controls

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

©Simplilearn. All rights reserved.

Technical Controls

These are hardware or software mechanisms used to protect important and confidential assets.

©Simplilearn. All rights reserved.

Physical Controls

These are security measures designed to deny unauthorized access.

©Simplilearn. All rights reserved.

Physical Controls

Deterrent

Preventive

Corrective

Recovery

Detective

Compensating

©Simplilearn. All rights reserved.

Defense in Depth or Layered Approach

It is the act of using multiple layers of security controls to protect the integrity of information.

©Simplilearn. All rights reserved.

Defense in Depth or Layered Approach

Its intent is to provide increased security through intentional redundancy based on multi-layered security approach.

©Simplilearn. All rights reserved.

Defense in Depth or Layered Approach

©Simplilearn. All rights reserved.

Identity Management

It is an organizational process for identifying, authenticating, and authorizing individuals or groups of people.

Identified

Authenticated

Authorized

©Simplilearn. All rights reserved.

Identity Management

It enables the right users to access the right resources at the right time for the right reasons.

©Simplilearn. All rights reserved.

IAM Components

©Simplilearn. All rights reserved.

Identification and **Authentication**

Identification

Identify a user or an application in the system

Authentication

Prove that a user or an application is genuine

©Simplilearn. All rights reserved.

Identification and **Authentication**

Password

Something you know

Something you have

Token card

Biometric

Something you are or do

Where you are

Location

©Simplilearn. All rights reserved.

Multi-Factor Authentication

It is an authentication method where a user is granted access after presenting two or more evidences.

©Simplilearn. All rights reserved.

Two-Factor Authentication

It is a subset of multi-factor authentication, confirming that users are granted access with a combination of two different factors.

©Simplilearn. All rights reserved.

Multi-Factor Authentication

It is an authentication method where a user is granted access after presenting two or more evidences.

©Simplilearn. All rights reserved.

Authorization

It is the process of determining what types of activities, resources, or services a user is permitted.

©Simplilearn. All rights reserved.

Authorization

A user may be authorized for different types of activity once authenticated.

©Simplilearn. All rights reserved.

Accountability

It is the traceability of actions performed on a system to a specific system entity.

©Simplilearn. All rights reserved.

Accountability

User identification and authentication support accountability

User ID and password destroy accountability

©Simplilearn. All rights reserved.

Auditing

It is a manual or a systematic measurable technical assessment of a system or application.

©Simplilearn. All rights reserved.

Monitoring

It is a manual or a systematic measurable technical assessment of a system or application.

Defining the behavior types to trigger alerts

Taking actions on alerts as needed

©Simplilearn. All rights reserved.

Patch Management

It involves acquiring, testing, and installing multiple patches to an administered computer system.

©Simplilearn. All rights reserved.

Patch Management Tasks

Maintain knowledge of available patches

Decide appropriate patches for particular systems

Ensure that patches are installed properly

Test systems after installation

Document all associated procedures

©Simplilearn. All rights reserved.

Patch Management: Example

The outbreak of WannaCry ransomware became large and intense because of a missing security patch.

©Simplilearn. All rights reserved.

System Hardening

It is a collection of tools, techniques, and best practices to reduce vulnerability.

Technology applications

Systems

Infrastructure

Firmware

©Simplilearn. All rights reserved.

System Hardening: Purpose

It eliminates security risks and secures a system by reducing its attack surface.

©Simplilearn. All rights reserved.

System Hardening Activities

©Simplilearn. All rights reserved.

Change Control

It is a systematic approach to manage all changes made to a product or system.

©Simplilearn. All rights reserved.

Change Control: Purpose

All changes are documented

No unnecessary changes are made

Services are not disrupted

Resources are used efficiently

©Simplilearn. All rights reserved.

Change Control: Purpose

©Simplilearn. All rights reserved.

Asset Management

It is the systematic process of developing, operating, maintaining, upgrading, and disposing of assets cost-effectively.

©Simplilearn. All rights reserved.

Asset Management Lifecycle

©Simplilearn. All rights reserved.

Data Management

Data is the smallest piece of information in any form.

©Simplilearn. All rights reserved.

Data Management

It is an administrative process to ensure the accessibility, reliability, and timeliness of the data for its users.

©Simplilearn. All rights reserved.

States of Data

They describe the different modes whereby data is used by a computing equipment.

©Simplilearn. All rights reserved.

Three Basic States of Data

Data at rest

Data in transit

Data in use

©Simplilearn. All rights reserved.

Information Lifecycle

Acquisition: Indexed system data

Disposal: Stored data for destruction

Archival: Backup, protection, and retention

Use: Challenges in protection

©Simplilearn. All rights reserved.

Information Lifecycle

It is an ongoing process

It helps ensure data is protected

Metadata must be at the right classification level

It helps indicate the level of data protection

Classification level must be attached to the information lifecycle

©Simplilearn. All rights reserved.

Encryption

It describes the different modes whereby data is used by a computing equipment.

©Simplilearn. All rights reserved.

Encryption

©Simplilearn. All rights reserved.

Encryption

Protects data in transit over networks

Protects information stored on computers

Deters and detects alterations of data

Verifies the authenticity of a transaction

©Simplilearn. All rights reserved.

Cryptography

Cryptography is the science of protecting information by encoding it into an unreadable format.

©Simplilearn. All rights reserved.

Cryptography

©Simplilearn. All rights reserved.

Factors Influencing Effective Encryption

The non-existence of back doors

Algorithm strength, secrecy, and difficulty of compromising a key

The inability to decrypt an entire cipher text

©Simplilearn. All rights reserved.

Types of Encryption

Symmetric Encryption

Asymmetric Encryption

©Simplilearn. All rights reserved.

Symmetric Encryption

Symmetric encryption is based on the same key or private key to encrypt plain text and decrypt ciphertext.

- Uses one key to encrypt and decrypt
- Uses less processing power

- Shares the key with the receiver

©Simplilearn. All rights reserved.

Symmetric Encryption

Common private key cryptography systems:

Data Encryption Standard (DES)

64-bit

Advanced Encryption Standard (AES)

128-bit to 256-bit

©Simplilearn. All rights reserved.

Asymmetric Encryption

Solves the problem of sharing the key with the receiver

©Simplilearn. All rights reserved.

Asymmetric Encryption

Services of cryptography:

Authentication

Validates the sender's identity

Non-repudiation

Prevents denial of action

Confidentiality

Controls who reads the data

©Simplilearn. All rights reserved.

Incident Response

It is an organized approach to address and manage the aftermath of a security breach.

©Simplilearn. All rights reserved.

Incident Response: Goals

Reduces damage, recovery time, and costs

Manages potential disruption to IT service

Has normal service operations within SLAs

Minimizes the adverse impact on business operations

©Simplilearn. All rights reserved.

Security Training

It is an organized approach to addressing and managing the aftermath of a security breach or cyber attack.

©Simplilearn. All rights reserved.

Security Awareness

It is the process of exposing people to security issues so that they may be able to recognize them and better respond to them.

©Simplilearn. All rights reserved.

Key Takeaways

- Cybersecurity refers to a set of techniques used to protect the integrity of network programs and data from attack, damage, and unauthorized access.
- Malware is a software that is designed to cause damage to a computer, server, client, or network. The types of malware include worm, spyware, virus, trojan, and logic bomb.
- Strategic plan, tactical plan, and operational plan are the types of security management plans.
- Change control is a systematic approach for managing all changes made to a product or system.

©Simplilearn. All rights reserved.