INDUSTRIAL TRAINING REPORT ON CYBER SECURITY

OSENI OLUWTOSIN MARIAM

U/22/CS/0019

COMPUTER SCIENCE 300L

NAME OF INDUSTRY:

SUPERVISOR: PROFESSOR B.O. AKINYEMI

ADDRESSS: AFRICAN CENTRE OF EXCELLENCY ICT, OAU ILE-IFE OSUN STATE

OCTOBER, 2024

Table of Contents

[**INTRODUCTION TO CYBER SECURITY** 3](#_Toc180433472)

[**CONCEPTS OF CYBER SECURITY** 3](#_Toc180433473)

[**AREAS OF CYBER SECURITY** 5](#_Toc180433474)

[**LINUX** 6](#_Toc180433475)

# **INTRODUCTION TO CYBER SECURITY**

Cyber security is the practice of protecting computer systems, networks, and digital information from unauthorized access, data breaches, and cyber threats. It encompasses a wide range of strategies, technologies, and practices aimed at safeguarding sensitive data, ensuring the confidentiality, integrity, and availability (CIA TRIAD) of digital assets, and mitigating risk associated with the digital landscape.

Cyber security measures include the use of firewalls, encryption, access controls, and regular system updates, along with user education and awareness to defend against evolving cyber threats such as malware, phishing attacks, and hacking attempts.

In an increasingly interconnected and technology-dependent world, cyber security plays a critical role in preserving the privacy and security of individuals, organization, and nations.

# **CONCEPTS OF CYBER SECURITY**

Here are the core concepts of cybersecurity:

1. **Confidentiality**: Ensuring that sensitive information is accessed only by authorized users. This is often achieved through encryption and access controls.
2. **Integrity**: Protecting information from being altered or tampered with by unauthorized users. This includes using checksums, hashing, and validation processes.
3. **Availability**: Ensuring that systems and data are accessible when needed. This involves protecting against attacks like denial-of-service (DoS) and implementing backup solutions.
4. **Authentication**: Verifying the identity of users and systems. This can involve passwords, biometrics, or multi-factor authentication (MFA).
5. **Authorization**: Granting users the right to access specific resources based on their identity. This ensures that users can only perform actions they are permitted to.
6. **Non-repudiation**: Ensuring that a user cannot deny having performed an action. This is often achieved through logging and digital signatures.
7. **Threat and Vulnerability Management**: Identifying, assessing, and mitigating potential threats and vulnerabilities in systems and networks.
8. **Incident Response**: Developing a structured approach to manage and respond to cybersecurity incidents effectively. This includes preparation, detection, containment, eradication, recovery, and lessons learned.
9. **Risk Management**: Evaluating and prioritizing risks to determine appropriate measures to protect assets. This involves assessing threats, vulnerabilities, and impacts.
10. **Security Policies and Procedures**: Establishing guidelines and protocols for how security measures are implemented and maintained within an organization.
11. **Compliance and Legal Issues**: Understanding and adhering to relevant laws, regulations, and industry standards that govern data protection and cybersecurity practices.
12. **User Education and Awareness**: Training users on security best practices to reduce human-related vulnerabilities, such as phishing and social engineering attacks.

# **AREAS OF CYBER SECURITY**

Cybersecurity encompasses several areas, each focusing on different aspects of protection and risk management. Here are the key areas:

1. **Network Security**: Protecting the integrity, confidentiality, and availability of data and services in networks. This includes firewalls, intrusion detection systems (IDS), and secure network architecture.
2. **Application Security**: Ensuring software applications are secure from threats throughout their lifecycle, including secure coding practices, vulnerability assessments, and penetration testing.
3. **Endpoint Security**: Protecting end-user devices such as computers, smartphones, and tablets from threats. This often involves antivirus software, endpoint detection and response (EDR), and mobile device management (MDM).
4. **Data Security**: Safeguarding data through encryption, access controls, and data masking. This area focuses on protecting data at rest, in transit, and during processing.
5. **Cloud Security**: Securing cloud environments and services, including data protection, access management, and compliance with regulatory requirements for cloud-based applications.
6. **Identity and Access Management (IAM)**: Managing user identities and controlling access to systems and data. This includes authentication, authorization, and user provisioning processes.
7. **Incident Response and Management**: Preparing for, detecting, and responding to security incidents. This includes developing incident response plans, conducting drills, and post-incident analysis.
8. **Security Operations**: Monitoring, detecting, and responding to threats in real-time, often through security information and event management (SIEM) systems and security operations centres (SOCs).
9. **Governance, Risk Management, and Compliance (GRC)**: Establishing policies and processes to manage risk and ensure compliance with laws, regulations, and industry standards.
10. **Physical Security**: Protecting physical assets and infrastructure from physical threats, including unauthorized access to facilities and equipment.
11. **Cybersecurity Awareness and Training**: Educating employees and users about security best practices, threat recognition, and safe behaviours to reduce human error and insider threats.
12. **IoT Security**: Addressing security concerns related to Internet of Things (IoT) devices, including securing data, managing device identities, and ensuring secure communications.

# **LINUX**

Linux is an open-source operating system kernel that serves as the foundation for various operating systems, collectively known as Linux distributions (distros). Created by Linus Torvalds in 1991, Linux is known for its stability, security, and flexibility. Here are some key features and aspects of Linux:

1. **Open Source**: Linux is free to use, modify, and distribute. Its source code is accessible to anyone, fostering collaboration and innovation.
2. **Distributions**: There are many Linux distributions, each tailored for specific needs. Popular examples include Ubuntu, CentOS, Fedora, and Debian.
3. **Multitasking and Multiuser**: Linux supports multiple users and processes running simultaneously, making it suitable for servers and personal computers alike.
4. **Security**: Linux is known for its robust security features, including user permissions, access controls, and a strong community that actively addresses vulnerabilities.
5. **Command-Line Interface**: While many distros offer graphical user interfaces (GUIs), Linux is often used through the command line, providing powerful control over the system.
6. **Compatibility**: Linux can run on a wide variety of hardware, from servers and desktops to embedded systems and mobile devices.
7. **Community Support**: A large community of developers and users contributes to Linux, providing extensive documentation, forums, and resources for troubleshooting and support.
8. **Software Management**: Linux uses package management systems (like APT, YUM, or Pacman) to install, update, and manage software easily.

Linux is widely used in various environments, including web servers, supercomputers, and as an operating system for personal computers, due to its versatility and reliability.