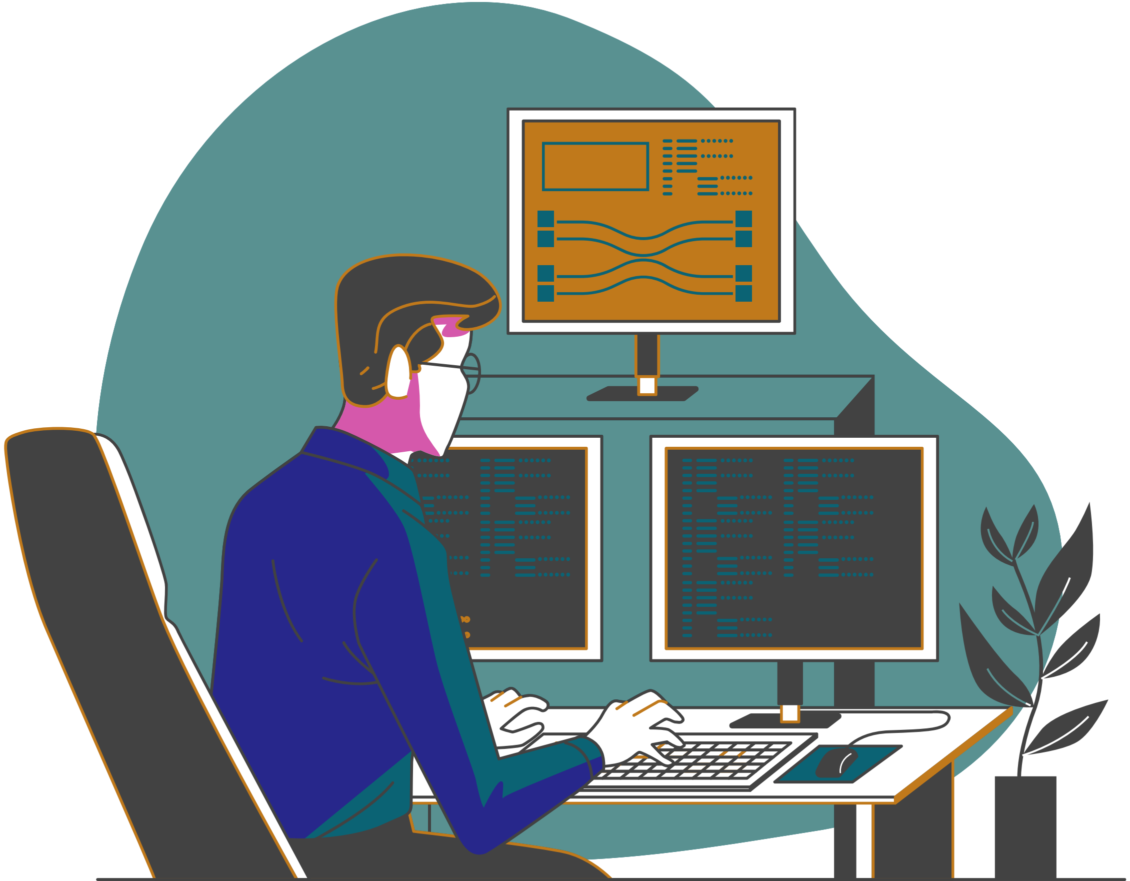

4NONYMOU5 CYSE200T Presentation

Jaivon Doniel, William Albert,Clifford Osei, Goodluck Ahusimiro,

Introduction

- Cybersecurity relies on CIA Triad to protect data amid rising cyber attacks.
- In sector like healthcare and workplace, balancing innovation with ethical use is crucial.
- Future cyber policies must ensure responsibility and security in an increasingly digital world.

CIA Triad

- **Confidentiality**: ensures that sensitive information is accessible only to authorized individuals and is protected from unauthorized access.
- Encryption, Access-Control, Secure Communication

- **Integrity**: ensures that information remains accurate, consistent, and unaltered, maintaining its trustworthiness.
- Hash Functions, Digital Signatures, Version Control

- **Availability**: ensures that information and resources are accessible to authorized users whenever needed.
- Redundant systems, Backups, Disaster Recovery Plan

Authentication vs. Authorization

- **Authentication**: ensures that only legitimate users or systems can access the network or system, preventing unauthorized access.

- Two-factor authentication, Biometric authentication, Username-Password Login

- **Authorization**: ensures that even authenticated users or systems can only perform actions they are permitted to, protecting sensitive information and resources from misuse.

- Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Access Control Lists (ACLs)

Cyber Attack

What is Cyber Attack?

- **Definition**: A cyber attack is an intentional attempt by hackers to damage, disrupt, or gain unauthorized access to computer systems, networks, or data.

- **Purpose**: Can be for stealing information, financial gain, espionage, sabotage, or just to cause disruption.

- **Common Targets**:

- Government agencies

- Corporations

- Financial institutions

- Individuals

Common Attacks

Types of Cyber Attacks:

- **Malware**: Malicious software like viruses, worms, ransomware.
- **Phishing**: Fake emails or messages to trick users into revealing sensitive info.
- **Denial of Service (DoS/DDoS)**: Overwhelming a system to make it unavailable.
- **Man-in-the-Middle (MitM)**: Intercepting communications between two parties.

Common Attacks Pt.2

- **Consequences**:
  - Data loss or theft
  - Financial damage
  - Reputation damage
- **Protection Measures**:
  - Firewalls and antivirus software
  - Strong passwords and authentication
  - Backups and incident response plans

Cybersecurity in Health Care

What is Cybersecurity in Health Care?

- Healthcare cybersecurity involves protecting medical data and health care systems and networks and devices from unauthorized access and cyber threats including data breaches and ransomware attacks.

Practices

- **Data Encryption**: This helps with records of sensitive data which moves through networks, to prevent unauthorized access.

- **Network Security**: Use firewalls, intrusion prevention systems (IDS/IPS), and secure Wi-Fi networks to protect internal systems.

- **Staff Training and Awareness:** Workers Conduct regular training for all staff on phishing, social engineering, and other common threats.

Challenges/ Solutions

Challenges:

Human Error

- Health care staff members may accidentally open phishing emails and use weak passwords or share login credentials which makes the system vulnerable.
- The staff members do not prioritize cybersecurity because their main responsibility is to save lives rather than handle IT risks.

Outdated Technology

- Hospitals and clinics continue to operate with outdated systems which fail to integrate with contemporary security systems and updates.
- The majority of MRI machines and infusion pumps operate with hardware limitations that prevent straightforward patch implementation.

Challenges/ Solutions Pt.2

Solutions:

1. Upgrade and Secure Legacy Systems

Replace or isolate outdated systems that can't be patched.

Use virtual patching or network segmentation to reduce risk when systems can’t be replaced immediately.

2. Strengthen Access Controls

All users must use Multi-Factor Authentication (MFA) when accessing sensitive systems and all users should implement this security measure.

Users should only access data they need through role-based access control (RBAC).

Cyber Technology in the Workplace

Balancing Innovation and Deviance

Introduction

- Cyber technology has reshaped the modern workplace.
- Boosts communication, collaboration, and flexibility.
- However, technology misuse—like cyberloafing—presents challenges.
- This presentation explores both benefits and drawbacks, and strategies for balance.

Benefits of Cyber Technology

- **Real-time communication:** Instant messaging, video conferencing.
- **Remote work capabilities:** Flexibility for employees.
- **Cloud computing & AI:** Streamlined processes and task automation.
- **Global collaboration:** Breaks down geographical barriers.
- **Innovation boost:** Frees up time for strategic, creative work.

Challenges –
Cyberloafing & Deviance

- **Cyberloafing:** Personal internet use during work hours.
- **Impact on productivity:** Less focus, more distractions.
- **Team morale suffers:** When some work while others don’t.
- **Security risks:** Exposure to phishing, malware from non-work activity.
- **Remote work issues:** Harder to monitor, enforce boundaries.

Addressing the Issue

- **Clear internet use policies:** Defined rules and consequences.
- **Cybersecurity training:** Awareness of risks and responsibilities.
- **Monitoring tools:** Respect employee privacy while ensuring compliance.
- **Promote accountability:** Lead by example and foster trust.
- **Set realistic expectations:** Avoid burnout and unnecessary restrictions.

Conclusion

Cyber technology is a **powerful asset** but not without risk.

Innovation must be balanced with **responsible use**.

Key to success:

- **Policies**
- **Training**
- **Culture of integrity**

Ethics, Responsibility, and the Future of Cyber Policy

The "Short Arm" of Predictive Knowledge

The Role of Ethics in Cybersecurity

- Cybersecurity is not just technical—it's moral
- Ethical foresight protects humanity's digital future
- Inspired by Hans Jonas's warning: **"Act so that the effects are compatible with meaningful human life."**

Philosophical Foundations

- **Hans Jonas (1984):** Act with caution, long-term impact in mind
- **Luciano Floridi (2013):** Respect privacy, dignity, and autonomy in digital spaces
- **David Guston (2014):** Anticipatory governance—plan for future outcomes

From Defense to Leadership

- Ethics should guide system design and policy decisions
- Cybersecurity pros must think ahead—not just react
- Our goal: protect systems *and* human values

Our Vision & Commitment

- We see cybersecurity as a moral calling
- We aim to lead with ethics, foresight, and responsibility
- Together, we can shape a safer, more ethical digital future