ASSOCIATION OF MEDICAL COUNCILS OF AFRICA

2025

AMCOA

CAPACITY BUILDING WORKSHOP

INTEGRATED HEALTHCARE REGULATION AND LEADERSHIP IN BUILDING RESILIENT HEALTH SYSTEMS

MEDICAL AND DENTAL COUNCIL OF NIGERIA

TECHNOLOGY AND CYBERSECURITY

BELLO HAYATUDEEN

FEDERAL MINISTRY OF
HEALTH &
SOCIAL WELFARE

CONTENTS

✓ Introduction

✓ Technology in Healthcare

✓ Common Cyber Threats

✓ Addressing Cyber Threats

✓ Enhancing IT Infrastructure Integrity

✓ Collaboration and Building Resilience

✓ Key Terms

✓ References

INTRODUCTION

- In today's digital age, **technology drives almost every aspect of modern life**—from communication and business to health and national security. As organizations increasingly depend on digital systems, the threat landscape grows.
- **Cybersecurity** is the practice of protecting systems, networks, and data from digital attacks. It is essential for maintaining the trust, safety, and resilience of both public and private sector operations.
- One of the most significant improvements brought about by technology is in the field of healthcare.

INTRODUCTION (CONT'D)

"The average cost of a healthcare data breach was $9.8 million in 2024, a decrease from $10.9 million in 2023 but still significantly higher than the cross-industry average of $148 per record (Veronis)"

TECHNOLOGY IN HEALTHCARE

- Digital tools enhance patient access to healthcare services.
- Electronic Health Records (EHRs) support accurate diagnoses and personalized treatment.
- AI enables early disease detection through advanced diagnostics.
- Robotics improve surgical speed, precision, and reduce errors.
- Wearables empower individuals to track health and build healthy habits.

MOST COMMON CYBER THREATS

- ***Phishing and Social Engineering:*** Deceptive emails or messages trick employees into revealing credentials or installing malware.
- ***Supply Chain Attack:*** Threat actors compromise third-party vendors or software providers to gain access to healthcare networks.
- ***Malicious Codes*** (Virus, Trojans, Worms, Keyloggers, spywares, backdoors, etc): Malicious software introduced through infected emails, websites, USBs, or compromised software to steal data, spy on activity, or disrupt systems.
- ***Business Email Compromise (BEC):*** Cybercriminals spoof or hack into official email accounts to deceive staff into transferring funds or disclosing sensitive information

MOST COMMON CYBER THREATS

- ***DDOS:*** Overwhelming hospital networks or patient portals with traffic, making them unavailable.
- ***Ransomware:*** Malicious software encrypts healthcare data, demanding payment for decryption.
- ***Vulnerabilities:*** Weaknesses in software, hardware, configurations, or processes that can be exploited by threat actors. This includes unpatched systems, misconfigurations, and unknown (zero-day) flaws.
- ***Insider threats:*** Malicious or negligent actions by employees, contractors, or third-party vendors.

ADDRESSING CYBER THREATS

According to Tedros Adhanom Ghebreyesus (WHO DG)

“The digital transformation of healthcare, combined with the high value of health data, has made the sector a prime target for cybercriminals.”

*“Ransomware and other cyberattacks on hospitals and other health facilities **are not just issues of security and confidentiality, they can be issues of life and death.”***

ADDRESSING CYBER THREATS

“Malicious actors accounted for 52% of healthcare breaches, with social engineering, phishing attacks, business email compromise (BEC), distributed denial of service (DDoS), and botnets being the primary attack vectors. (IBM)”

“Despite numerous high-profile ransomware attacks, overall ransomware payments within the healthcare sector totaled $814 million in 2024. (WIRED)”

ADDRESSING CYBER THREATS (CONT'D)

- ***Access Management:*** Enforce MFA, least privilege, and strong password policies.
- ***Security Monitoring:*** Deploy EDR (Endpoint Detection & Response)/XDR (Extended Detection & Response), SIEM (Security Information and Event Management), and UEBA (User and Entity Behavior Analytics) tools for real-time threat detection.
- ***Patch & Vulnerability Management:*** Regularly patch systems and monitor for zero-days with threat intelligence.
- ***Staff Awareness:*** Conduct regular training on phishing, BEC, and insider threats.

ADDRESSING CYBER THREATS (CONT'D)

- ***Data Protection:*** Encrypt PHI and sensitive data; apply DLP solutions
- ***Third Party Risk Management:*** Perform vendor risk assessments; enforce cybersecurity clauses in contracts.
- ***Incident Response:*** Maintain tested IR plans and offline backups for ransomware recovery.
- ***DDoS Protection:*** Use cloud-based mitigation services and maintain redundant connectivity
- ***Network Segmentation:*** Isolate IoMT and critical systems using VLANs and NAC controls

IT INFRASTRUCTURE INTEGRITY

IT infrastructure:

the hardware, software, and networks that support operations—must be secured from the inside out.

Infrastructure Integrity:

The assurance that systems function correctly, securely, and without unauthorized interference.

ENHANCING IT INFRASTRUCTURE INTEGRITY

To enhance IT infrastructure integrity:

- Apply patches and updates regularly to fix known vulnerabilities.
- Implement access controls and multi-factor authentication (MFA) to reduce unauthorized access.
- Adopt a Zero Trust Architecture, which assumes no user or device is trustworthy by default.
- Build security into systems by design, not as an afterthought.

“When infrastructure is protected, the organization becomes less vulnerable to disruptions and data breaches.”

COLLABORATION AND BUILDING RESILIENCE

- Cybersecurity is a shared responsibility.
- Governments, industries, and organizations must collaborate to detect, prevent, and respond to cyber threats.
- Platforms like Malware Information Sharing Platforms (MISPs), Information Sharing and Analysis Centers (ISACs) provide trusted spaces to exchange critical security information.
- Collaboration with your National and Sectoral CSIRTs.

COLLABORATION AND BUILDING RESILIENCE (CONT'D)

At the same time, **resilience** must be built into operations:

- Create and regularly test business continuity and disaster recovery plans (NIST SP 800-34r1, 2010).
- Adopt cyber resilience frameworks that combine risk management with incident response and recovery (World Economic Forum, 2020).
- Invest in cyber insurance to support financial recovery when incidents occur (OECD, 2022).

Cyber resilience focuses not just on preventing attacks—but on ensuring organizations can recover quickly and continue operating.

KEY TERMS

- **Cyber Threat:** A potential malicious act targeting digital systems or data.
- **Incident Response:** The structured approach to handling and managing security breaches or attacks.
- **Threat Intelligence:** Actionable insights about existing or emerging cyber threats.
- **IT Infrastructure Integrity:** The assurance that systems function correctly, securely, and without unauthorized interference.
- **Zero Trust Architecture:** A model that requires verification of every access attempt, assuming no user or device is inherently trusted.
- **Cyber Resilience:** The ability to prepare for, respond to, and recover from cyber disruptions.
- **Security Operations Center (SOC):** A team dedicated to monitoring, detecting, and responding to cyber threats.
- **Telemedicine:** Telemedicine is a term used to describe the remote delivery of healthcare services using telecommunications technology.

REFERENCES

1. *Computer Security Incident Handling Guide*, National Institute of Standards and Technology - **NIST SP 800-61r2 (2012)**
2. *Zero Trust Architecture*, National Institute of Standards and Technology - **NIST SP 800-207 (2020)**
3. *Contingency Planning Guide for Federal Information Systems* - **NIST SP 800-34r1 (2010)**
4. *Cybersecurity Best Practices*, Cybersecurity & Infrastructure Security Agency - **CISA (2023)**
5. *Threat Landscape Reports*, European Union Agency for Cybersecurity - **ENISA (2023)**
6. *Security Awareness Planning Kit* - **SANS Institute (2023)**
7. *Information Security Management* - **ISO/IEC 27001 (2022)**
8. *Cyber Signals Report: Identity Protection and MFA* - **Microsoft (2023)**
9. *Information Sharing and Collaboration Initiatives* - **National Council of ISACs (2023)**
10. *Cyber Resilience Playbook for Public-Private Collaboration* - **World Economic Forum (2020)**
11. *Cyber Insurance: Policy Approaches in the Digital Age* - **OECD (2022)**