GROUP 2

POTENTIAL CYBER SECURITY RISK FOR HOSPITAL

Group Members

- Onilude Hammed
- Olakunle Mustapha
- Akinde Gideon
- Aremu Ayodeji
- Adelekan Kafayat
- Mahmud Nafisa

INTRODUCTION

A cyber-attack on a hospital is considered as an attack on a health care facility. WHO defines an attack as any act of verbal or physical violence, threat of violence or other psychological violence, or obstruction that interferes with the availability, access and delivery of curative and/or preventive health services.

NEED FOR CYBERSECURITY IN HEALTHCARE

Technology advancements enable medical institutions to treat patients, access shared data, and communicate with patients and workers via linked devices. However, all of the talents mentioned above are risky. A dependable and experienced partner aware of compliance minimize that risk significantly.

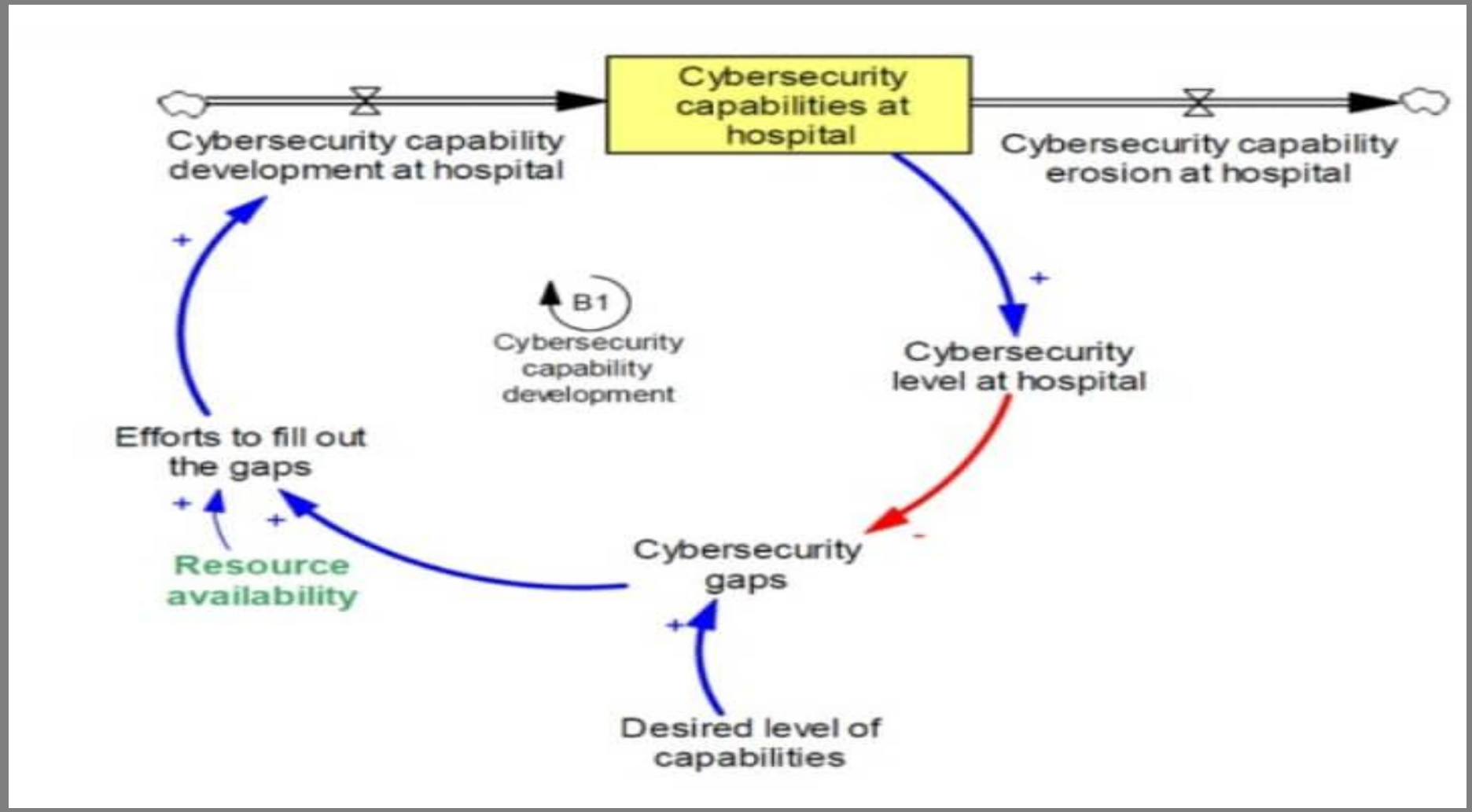
Ransomware attacks: Malware attacks encrypting critical healthcare data, disrupting patient care.

Medical device hacking: Vulnerabilities in medical devices, such as pacemakers, insulin pumps, and MRI machines.

Phishing and social engineering: Staff falling victim to phishing attacks, compromising sensitive information.

Insider threats: Authorized personnel misusing access or intentionally compromising data.

Denial of Service (DoS): Devices becoming unusable due to hacking.


Cybersecurity capabilities at hospital
Cybersecurity capability development at hospital
Cybersecurity capability erosion at hospital
B1
Cybersecurity capability development
Cybersecurity level at hospital
Efforts to fill out the gaps
Resource availability
Cybersecurity gaps
Desired level of capabilities

DISCUSSION ON POTENTIAL CYBER SECURITY RISK FOR HOSPITAL

Patient Data Security

Patient data is one of the most sensitive types of information in the health sector. Protecting this data from breaches is crucial, as unauthorized access can lead to identity theft, fraud, and even physical harm if medical information is altered. Implementing encryption, strict access controls, and regular audits are essential steps to ensure the security of patient health information.

Medical Device Security

Many medical devices are now connected to hospital networks, making them potential targets for cyber-attacks. If compromised, these devices could endanger patient lives. Securing these devices involves regular firmware updates, network segmentation to isolate them from the main network, and strong authentication mechanisms to prevent unauthorized access(Heart monitor machine).

DISCUSSION ON POTENTIAL CYBER SECURITY RISK FOR HOSPITAL

Staff Payroll

Manipulation of employee data, change payment details, or even steal sensitive information like social security numbers. This could lead to incorrect payments, identity theft, and financial loss for both the employees and the company.

Employee Records

Unauthorized access to sensitive employee information, financial theft. Hospitals must prioritize cybersecurity measures to protect employee record and prevent potential cyber threats from impacting staff record system.

Assets	Threat	Likelihood	Impact	Risk	Mitigation	Justification
Patient data	Natural Disaster	2	2	4	Strong encryption, regular back-up update	Policies, procedures, and training programs to reduce human error and insider threat.
Medical devices	Availability	2	4	8	Regular software update	Implementing encryption, network segmentation, and continuous monitoring.
Staff payroll	Unauthorized access	2	2	4	Strong encryption, educational training	Robust security protocols so likelihood is low.
Employee record	Unauthorized access	4	5	20	Cyber-security training for employee	Policies.