POTENTIAL CYBER SECURITY RISK FOR HOSPITAL

STAFF PAYROLL

Staff payroll is the process by which a company pays its employees. It involves tracking hours worked, calculating pay, and distributing payments which consist of employee payment details or sensitive information (social security numbers).

Using national institute of standards and technology cybersecurity framework

IDENTIFY

Manipulation of employee data, change payment details can lead to incorrect payment, identity theft and financial loss for both the company and employees

PROTECT

Data security (Encryption).

Access is limited to unauthorized user.

Hardware and managed commensurate with the assessed risk of unauthorized access.

Awareness and training (enlighten the empolyee on the effect of cyber breach on payroll system).

DETECT

Network and network service constant monitoring

1. Monitor the wired and wireless networks for connection from unauthorized endpoint.
2. Monitoring of software configuration for deviation, attempts against credentials and unauthorized credentials reuse.

Physical environment monitoring (personnel activity).

1. Monitor and review logs from physical access to control system.

RESPOND

Analysis

1. Check any cyber deception technology for additional information on attacker behavior.
2. Review other target to search for the compromise and evidence of persistence.

Mitigation

1. Cybersecurity technologies (antivirus software) must be regular updated.

RECOVER

The recovery activities and progress should be communicated.

The integrity of backups should be verified be restoration.

GOVERN

Policies that ensure cybersecurity is integrated into the hospital governance framework along with the risk management.