Institute of Information Technology (IIT)

Jahangirnagar University

Course Code: MICT 5315

Course Title: Applied Cyber Security

Assignment - 01

Submitted to:

Risala Tasin Khan, PhD

Professor

IIT, JU

Submitted by:

Name: Md. Shakil Hossain

Roll No: 1061

MSc 2nd Semester

IIT, JU

Submission Date: 28/07/2025

Contents

Cybersecurity Incident Response Report

Lubana General Hospital
Prepared by: Md. Shakil Hossain
Date: 28/7/2025

Summary

On July 20, 2025, Lubana General Hospital identified suspicious activity within its network, culminating in the unauthorized access of patient records. The suspected data breach has significant implications, not only for the privacy and trust of patients, but also for the hospital's legal, ethical, and regulatory obligations. This report provides a detailed exploration of how vulnerabilities in healthcare IT systems can be identified and mitigated, the best practices for penetration testing and preventing breaches, the forensic approach following an incident, comprehensive methods for evidence collection with proper chain-of-custody, and finally, actionable recommendations to strengthen Lubana General Hospital's cyber defenses.

1. Introduction

1.1 Purpose

The purpose of this report is to:

- Analyze the causes and impact of the recent cyber incident at Lubana General Hospital,
- Illustrate effective strategies for vulnerability identification and remediation,
- Detail a structured forensic investigation process suitable for healthcare environments,
- Discuss best practices for evidence collection and maintaining legal integrity,
- Furnish actionable recommendations for future prevention.

1.2 Scope

This report covers Lubana General Hospital's digital infrastructure, including Electronic Medical Record (EMR) systems, networked medical devices, employee workstations, communication platforms, and related systems that could be the target of cyberattackers.

1.3 Audience

This document is intended for hospital executive leadership, IT and security teams, compliance officers, and authorized external auditors.

2. Ethical Hacking and Vulnerability Identification

2.1 Overview

The complexity and rapid digital transformation within healthcare has exposed hospitals to a growing threat landscape. Ethical hackers also known as penetration testers or white-hat hackers use the tools and techniques of real-world attackers, but within a legal and controlled framework, to help organizations like Lubana General Hospital uncover and remediate security weaknesses before they can be exploited.

2.2 Common Vulnerabilities in Healthcare

Healthcare organizations are uniquely susceptible to cyber threats due to a combination of legacy equipment, regulatory requirements, and high-value data. Key vulnerabilities include:

- **Phishing Susceptibility:** Staff are frequent targets for phishing campaigns, potentially leading to credential theft or malware infection.
- **Outdated and Unpatched Systems:** Many hospitals run legacy operating systems and medical devices that are difficult to patch.
- **Weak Access Controls:** Overprivileged user accounts, poor password policies, and loosely segmented network zones.
- **Lack of Security Monitoring:** Insufficient centralized log management or real-time alerts leading to delayed incident detection.

2.3 Ethical Hacking Methodology

The ethical hacking process typically follows a systematic approach:

1. **Reconnaissance:** Gathering information about the hospital’s digital footprint.
2. **Scanning & Enumeration:** Using tools like Nmap and Nessus to identify vulnerabilities in systems and applications.
3. **Vulnerability Analysis:** Prioritizing discovered weaknesses based on severity, exploitability, and potential impact.
4. **Exploitation:** Safely attempting to exploit vulnerabilities to demonstrate risk, such as gaining unauthorized access or escalating privileges.
5. **Post-Exploitation:** Mapping the internal network, attempting lateral movement, and accessing sensitive data.
6. **Reporting:** Documenting findings, risk analysis, demonstration of exploitability, and actionable remediation guidance.

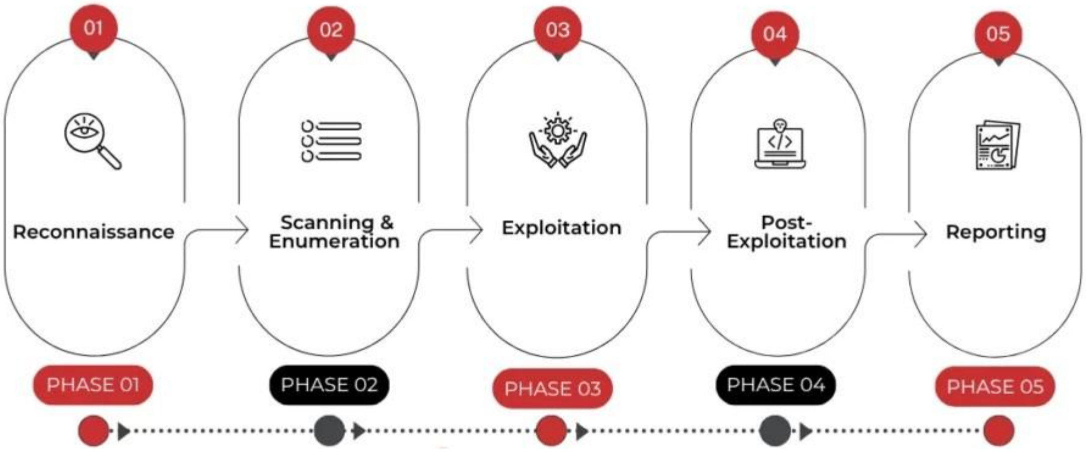

Figure: 5 Penetration Testing Phases

2.4 Application in the Hospital Environment

Ethical hackers working with Lubana General Hospital would, for example, simulate phishing attacks to test employee awareness and authentication technologies, conduct password audits to reveal weak credentials, and examine medical equipment for unpatched security flaws. These exercises mimic real-world threats but in a controlled fashion, providing the hospital with a prioritized roadmap for security enhancements.

3. Preventing Breaches: Penetration Testing and Vulnerability Scanning

3.1 Penetration Testing

Penetration testing is a goal-oriented assessment in which security professionals attempt to exploit vulnerabilities to determine the true risk they present. Critical aspects of pen testing in healthcare include:

- **Comprehensive Testing:** EMR systems, network segmentation, IoT/medical devices, employee endpoints, and data backups.
- **Social Engineering:** Simulated phishing to test human factors and incident reporting processes.
- **Physical Security Checks:** Testing the resilience of physical barriers, such as badge access controls and video surveillance, especially relevant if attackers could gain in-person access.

3.1.1 Benefits

- **Uncovering Exploitation Paths:** Penetration testers document step-by-step how an attacker could start with a minor foothold and escalate to sensitive information.

- **Measuring Response Effectiveness:** Controlled attacks help test the incident detection and response capabilities of IT and security staff ("blue team").
- **Actionable Remediation:** Reports provide concrete, prioritized fixes, often scored by risk, so limited hospital resources can be used efficiently.

3.1.2 Healthcare-Specific Considerations

- **Patient Safety:** Testing on production systems must be coordinated to avoid risk to clinical operations or patient care.
- **Data Privacy:** All data must be handled according to HIPAA and local data protection laws.

3.2 Vulnerability Scanning

Vulnerability scanners are automated tools that assess systems for known security flaws.

3.2.1 Process

- **Asset Inventory:** The first step is maintaining an up-to-date inventory of all systems and devices in the hospital.
- **Automated Scanning:** Tools such as Nessus, Qualys or OpenVAS can scan large environments efficiently.
- **Patch & Remediation Workflow:** Scanning should feed directly into patch management and system hardening procedures.

3.2.2 Role in Prevention

- **Early Detection:** Regular scanning can spot risky misconfigurations or vulnerabilities before attackers do.
- **Compliance:** Helps demonstrate regulatory due diligence.

3.3 How These Approaches Would Have Prevented the Breach

Had Lubana General Hospital implemented regular penetration testing and automated vulnerability scanning:

- Phishing and credential theft would have been proactively addressed through simulations and user training.
- Critical system vulnerabilities, especially those in outdated devices or EMR applications, could have been remediated before exploitation.
- Gaps in network segmentation would have been discovered and closed.
- Incident response processes could have been rehearsed, reducing detection and containment time.

4. Forensic Investigation: Structured Approach

Once a cyber incident is detected, a structured forensic investigation is paramount to minimize harm, restore operations, and meet legal/regulatory requirements.

4.1 Principles of Digital Forensics

- **Preservation:** Avoid alteration of original evidence.
- **Repeatability:** Ensuring investigation steps can be independently verified.
- **Documentation:** Detailed, contemporaneous records of all actions.

4.2 Digital Forensic Investigation Process

4.2.1 Preparation

- Assemble forensics team, define scope of investigation.
- Secure legal approvals, notify stakeholders per incident response plan.
- Ensure all tools and techniques are forensically sound.

4.2.2 Identification and Containment

- Isolate compromised systems from the network to prevent further infection.
- Identify all potentially affected assets.

4.2.3 Evidence Preservation

- Create forensic images of suspect hard drives and volatile memory.
- Secure all logs, including firewalls, VPN, application servers, email gateways, and Active Directory.
- Take snapshots of virtual machines, cloud systems, and device configurations.

4.2.4 Collection

- Gather system, user, and network evidence.
- Maintain chain-of-custody documentation for each evidence item.

4.2.5 Analysis

- Investigate timeline of compromise: identify initial attack vector, lateral movement, privilege escalation, and data exfiltration.
- Use digital forensics tools (EnCase, FTK, Volatility, Wireshark) to analyze disk images, memory dumps, and network logs.
- Correlate findings with external threat intelligence feeds, known malware signatures, and attack indicators.

4.2.6 Reporting

- Produce a detailed narrative of the incident: what happened, how it happened, impact, and recommendations.

- Ensure findings are clear, evidence is well-documented, and report is suitable for executive and regulatory review.

4.2.7 Remediation and Lessons Learned

- Work with IT to eradicate threats.
- Close discovered vulnerabilities.
- Update procedures based on post-incident review.

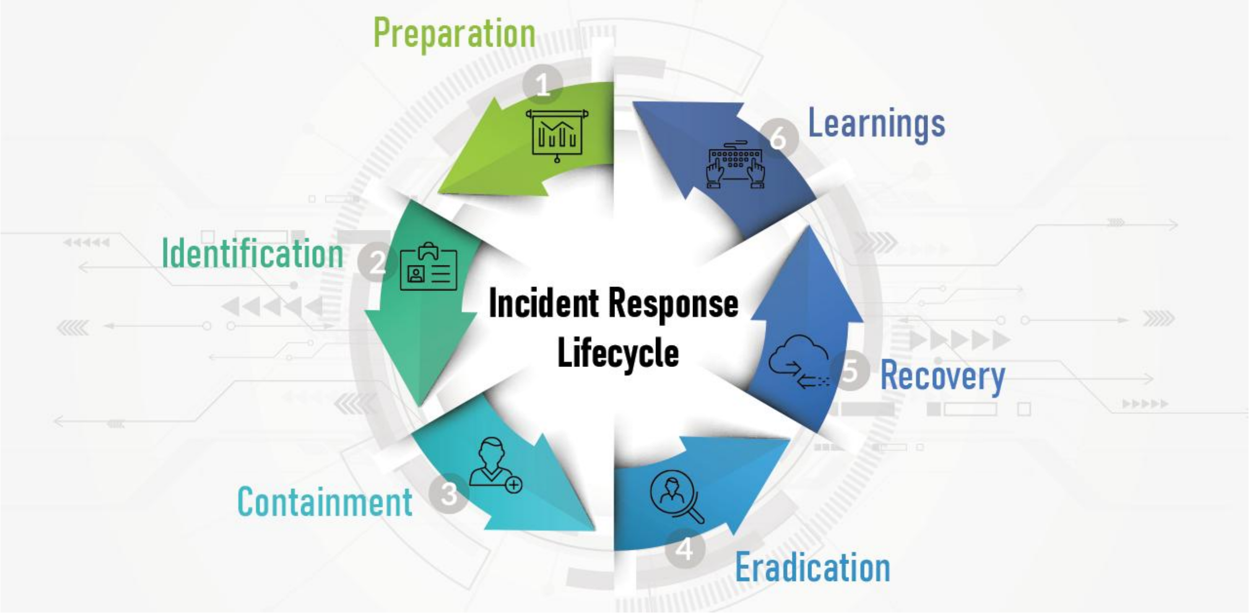

Figure: Incident Response Life Cycle

5. Evidence Collection and Chain of Custody

5.1 Types of Evidence to Collect

A robust forensic investigation hinges on identifying, collecting, and preserving the right evidence sources:

Evidence Type	Relevance
System Logs	Authenticate access, track attacker movements, correlate events across systems
Firewall & IDS/IPS Logs	Detect network intrusion, lateral movement, exfiltration attempts

Disk Images	Provide unaltered snapshots for post-incident review and legal action
Memory (RAM) Dumps	Contain malware in memory, active attacker sessions, volatile data
Network Packet Captures (pcaps)	Reveal real-time attacker actions, data exfiltration
Email Gateways & Messages	Confirm spear phishing, business email compromise
Databases/EMR System Logs	Determine what/whose records were accessed or altered
Configuration Backups	Reveal pre- and post-incident system states
Physical Security Logs	Correlate digital attacks with possible physical intrusions

5.2 Evidence Collection Steps

1. **Identify and Label Evidence:** Assign unique IDs to all evidence items.
2. **Secure Originals:** All evidence collection must preserve original data.
3. **Documentation:** Meticulously log every access, transfer, or analysis operation.
4. **Use Write Blockers:** For disk imaging and analysis to prevent data modification.
5. **Integrity Assurance:** Use cryptographic hashes to ensure files/images are unaltered during analysis or transfer.

Sample Chain-of-Custody Log Table:

Item ID	Description	Date/Time	Collected By	Received By	Hash Value	Location
001	Disk image – Laptop	2025-07-20 10:00	J. Smith	B. Lee	abcd1234...	Evidence safe

5.3 Chain of Custody Process

Chain of custody ensures the integrity of evidence by meticulously tracking its collection, handling, storage, and analysis from the initial response through all stages of the investigation.

5.3.1 Documentation

- Every person who handles the evidence signs and timestamps the chain-of-custody log.
- All evidence transfers, even within the team, are logged.
- Evidence is stored in a secure, access-controlled environment.

5.3.2 Integrity Controls

- **Hash Verification:** Every transfer validated by comparing cryptographic hash values.

- **Access Restriction:** Only personnel with a direct need-to-know have access.

5.3.3 Legal and Regulatory Importance

Failure to maintain chain of custody can result in evidence being inadmissible in court, regulatory penalties, or loss of organizational trust. Proper documentation is essential to respond effectively to health data breach notification laws.

6. Regulatory, Legal, and Ethical Considerations

6.1 Healthcare Data Regulations

Hospitals are bound by several data privacy frameworks depending on jurisdiction:

- **HIPAA (USA):** Establishes rules for the safeguarding, use, and breach notification of Protected Health Information (PHI).
- **GDPR (EU/EEA):** Sets strict standards for personal data protection, including patient data, and requires prompt breach notification.
- **Local Health Regulations:** Many countries have their own additional personal data protection or medical record security laws.

6.2 Legal Obligations Post-Breach

- **Notification:** Timely reporting to regulators and affected individuals may be required.
- **Forensic Integrity:** Investigations must stand up to later legal or regulatory scrutiny.
- **Litigation Risk:** Inadequate safeguards or investigation processes may increase exposure to lawsuits or fines.

7. Recommendations and Best Practices

7.1 Security Controls

- **Security Awareness Training:** Mandatory, regular training for all staff, with phishing exercises to reinforce risk recognition.
- **Multi-Factor Authentication (MFA):** Enforce for all remote access and privileged accounts.
- **Patch Management:** Implement timely, regular software and device updates, including medical devices and third-party applications.
- **Network Segmentation:** Limit access to critical systems with VLANs, firewalls, and logic controls.
- **Centralized Logging and Monitoring:** Deploy a Security Information and Event Management (SIEM) system for real-time alerting.

- **Principle of Least Privilege:** Review and restrict user privileges; require strong, unique passwords stored in a secure vault.

- **Third-Party Management:** Require vendors to adhere to security standards, and regularly audit their access and practices.

7.2 Incident Response Improvement

- **Regular Incident Response Drills:** Test and refine response procedures.

- **Threat Intelligence Integration:** Subscribe to information-sharing platforms relevant to healthcare.

- **Post-Incident Review:** Document "lessons learned" from drills and real incidents to update policies and technologies.

- **Quick Remediation Cycles:** Streamline the process for fixing detected vulnerabilities.

7.3 Forensics and Evidence Handling

- **Forensic Readiness:** Prepare tools, processes, and training so staff can act efficiently during an incident.

- **Routine Evidence Integrity Checks:** Run periodic reviews of chain-of-custody documentation and evidence storage.

- **Privacy by Design:** Build security controls into all new systems, minimizing data collection and retention to only what is necessary.

7.4 Compliance and Governance

- **Policy Review:** Regularly updating internal security policies to reflect evolving best practices, hospital-specific risks, and regulatory requirements.

- **External Audits:** Engage an independent cybersecurity firm annually to review controls and incident response readiness.

- **Continuous Improvement:** Foster a culture of security, where reporting incidents or weaknesses is rewarded, not penalized.

8. Conclusion

The data breach at Lubana General Hospital underscores the criticality of robust cybersecurity practices in healthcare. By employing ethical hacking and regular vulnerability assessments, implementing effective evidence collection and forensic procedures, and maintaining a strong chain of custody, the hospital can not only meet regulatory obligations but also reinforce the trust it holds with patients and the community.

Swift, decisive action paired with a culture of continuous improvement will minimize the risk of recurrence and demonstrate the hospital's commitment to data privacy and patient care. Leadership is strongly encouraged to consider the recommendations herein and to prioritize the ongoing investment in cybersecurity as a key component of healthcare delivery.

Reference

1. NIST, "Computer Security Incident Handling Guide," NIST Special Publication 800-61 Revision 2, National Institute of Standards and Technology, 2012.
2. NIST, "Technical Guide to Information Security Testing and Assessment," NIST Special Publication 800-115, National Institute of Standards and Technology, 2008.
3. NIST, "Guide to Integrating Forensic Techniques into Incident Response," NIST Special Publication 800-86, National Institute of Standards and Technology, 2006.
4. U.S. Department of Health & Human Services, "Health Insurance Portability and Accountability Act (HIPAA)," [Online]. Available: https://www.hhs.gov/hipaa/
5. European Union, "General Data Protection Regulation (GDPR)," Regulation (EU) 2016/679, 2016.
6. M. Schatz, "Incident Response and Digital Forensics," SANS Institute Reading Room, [Online]. Available: https://www.sans.org/
7. Guidance Software, "EnCase User Manual," Guidance Software, Pasadena, CA.
8. AccessData, "Forensic Toolkit (FTK) Documentation," AccessData Group, Orem, UT.
9. The Volatility Foundation, "Volatility Framework Documentation," [Online]. Available: https://www.volatilityfoundation.org/
10. G. Combs, "Wireshark User Guide," Wireshark Foundation, [Online]. Available: https://www.wireshark.org/
11. Health Information Sharing & Analysis Center (H-ISAC), "Resources and Threat Intelligence Reports," [Online]. Available: https://h-isac.org/
12. Cisco Systems, "Cybersecurity Threats in Healthcare: White Paper," Cisco Security Publications, 2023.
13. Palo Alto Networks, "Medical Device Security in Hospitals: Best Practices," Palo Alto Networks, 2024.
14. CrowdStrike, "2024 Healthcare Cyber Threat Report," CrowdStrike, Sunnyvale, CA, 2024.
15. Peer-reviewed case study: A. Brown, "A Case Study of Healthcare Data Breach Response," Journal of Cybersecurity, vol. 9, no. 2, pp. 112-124, March 2024.