INTERNATIONAL JOURNAL OF SCIENTIFIC HARMONIZATION OF DIGITAL HORIZONS (IJSHODH)
ISSN: 3108-1495 (Online)
Volume 1 2025

Cyber Security in Health Industry

Ms. Vanshika Kondar
Student, Master of Computer Applications, (2024-2026 Batch)
St. Wilfred's College of Computer Sciences
Vanshikakondar445@gmail.com

Abstract - The healthcare sector faces significant cyber security challenges, largely because many organizations still rely on outdated systems, insufficient security practices, and weak protective measures. As a result, it has become one of the primary targets for cybercriminals who seek to exploit sensitive information such as usernames, passwords, patient histories, and medical records. Although new technologies are being introduced into healthcare, their adoption is often slow and demanding, requiring careful planning, proper training, and substantial time for implementation. Because the sector has not evolved at the same pace as modern cyber threats, healthcare organizations remain increasingly vulnerable to emerging risks and attacks.

Keywords – Cyber security, Healthcare Industry, Data Protection, Ransomware, Phishing, Insider Threats, Electronic Health Records (EHR), Information Security, HIPAA, GDPR, ISO 27799, NIST Framework, Healthcare Data Breach, Cyber Risk Management, Cloud Security, Artificial Intelligence (AI), Blockchain, Staff Training, Digital Health, Patient Safety, Cyber Awareness

I. INTRODUCTION

The digital transformation of healthcare—through EHRs, telemedicine, IoMT devices, and cloud platforms—has improved patient care and operational efficiency. However, it has also introduced new cyber security threats, making healthcare one of the most targeted sectors globally **[1]**. Sensitive patient information such as clinical records and authentication credentials holds significant value on the black market **[2]**.
Ransomware, phishing, malware, and insider threats have disrupted medical operations, delayed treatments, and caused financial losses **[3]**. Therefore, cyber security is now a critical component of patient safety and hospital continuity.

A. NEED FOR CYBERSECURITY

Incidents such as the WannaCry attack on the UK NHS highlighted the devastating impact of weak security and outdated systems **[4]**. Healthcare systems often lack patch management, use unsupported operating systems, and depend on insecure IoMT devices, increasing risk exposure.

B. PROBLEM STATEMENT

Despite global frameworks like HIPAA, GDPR, and ISO/IEC 27799, healthcare systems frequently face cyber incidents due to:

- Legacy infrastructure
- Limited budgets
- Low training and awareness
- Shortage of cybersecurity professionals **[5]**

C. RESEARCH OBJECTIVES

- Identify major cyber threats in healthcare
- Analyze causes of rising cyber incidents
- Assess regulatory compliance
- Examine emerging technologies (AI, Blockchain, Cloud)
- Propose recommendations for cybersecurity improvement

D. SCOPE

The study covers cybersecurity challenges in hospitals, clinics, healthcare providers, and digital health platforms from 2015–2024, focusing on data security and technology-driven risks.

II. LITERATURE REVIEW

A. HEALTHCARE INFORMATION SYSTEMS

Healthcare Information Systems (HIS) include EHRs, EMRs, PACS, telemedicine, and IoMT networks. These systems improve diagnostic accuracy and data accessibility but expand the cyber-attack surface **[1]**.

B. EVOLUTION OF DIGITAL HEALTHCARE

Digital healthcare evolved through cloud adoption, AI integration, mobile platforms, and IoMT expansion. However, interconnected systems create vulnerabilities exploitable by cybercriminals **[6]**.

C. MAJOR CYBERSECURITY THREATS

1. **Ransomware:** Encrypts hospital data and halts critical operations **[3]**.
2. **Phishing & Social Engineering:** Exploits human error—responsible for nearly 90% of breaches **[5]**.
3. **IoMT Device Vulnerabilities:** Many devices run outdated firmware and lack encryption **[7]**.
4. **Data Breaches:** Weak authentication and misconfigured databases often lead to large-scale breaches **[2]**.

D. CYBERSECURITY STANDARDS

- **HIPAA:** Ensures administrative, physical, and technical security for patient data (USA).

- **GDPR:** Regulates data privacy and breach notification (EU).
- **NIST CSF:** Provides guidelines for identifying, protecting, detecting, responding, and recovering from threats **[8]**.
- **ISO/IEC 27799:** Applies cyber security controls specifically for healthcare environments **[9]**.

E. CHALLENGES IN HEALTHCARE CYBERSECURITY

- Legacy systems
- Lack of funding
- Human errors
- Limited cyber security workforce
- Weak vendor and third-party security **[5]**

F. IMPACT OF CYBERATTACKS

Cyber incidents cause:

- Disruption of medical services
- Financial losses
- Reputational damage
- Compromised patient safety **[10]**

G. EMERGING TECHNOLOGIES

AI-based anomaly detection, blockchain for secure data exchange, cloud security tools, and zero-trust architecture are reshaping healthcare cyber security **[8]**.

III. METHODOLOGY

A. RESEARCH DESIGN

A descriptive and analytical research **design** was adopted.

- The **descriptive** part identifies threats, behaviors, and patterns in healthcare cyber security.
- The **analytical** part interprets relationships between technology usage, threat exposure, staff awareness, and regulatory compliance.

B. DATA COLLECTION METHODS

- Secondary Data Collection

Collected from:

  - Peer-reviewed journals
  - Reports from IBM, ENISA, Symantec, Deloitte, Ponemon Institute
  - HIPAA, GDPR, NIST CSF publications
  - Case studies (WannaCry, UHS attack)

- **Systematic Literature Review (SLR)**

Steps included: keyword selection, database searching, and relevance filtering, thematic grouping.

- **Case Study Analysis**

Case studies included:

  - WannaCry attack (2017)
  - UHS hospital ransomware attack (2020)
  - IoMT device vulnerabilities (FDA reports)

- **SAMPLING DESIGN**

A purposive sampling method was used.

- **Total respondents: 19**
- **Mode:** Online Google Forms
- **Participants:** Healthcare workers, IT professionals, and students in health informatics
- **Reason:** To gather insights from individuals with relevant knowledge about digital systems and cyber security.

The survey consisted of 15 structured questions assessing awareness, security habits, threats, compliance, and cyber security practices.

- **VARIABLES CONSIDERED**

Independent Variables

  - Cyber threat type
  - Staff awareness level
  - Technology adoption (AI, cloud, IoMT)
  - Budget and resource allocation
  - Compliance level (HIPAA, GDPR, ISO standards)

Dependent Variables

  - Number of incidents
  - Severity of breaches
  - Financial/operational impact
  - Recovery duration
  - Risk to patient safety

- **DATA ANALYSIS METHOD**

  - Data exported from Google Forms to Excel
  - Responses cleaned and coded
  - Frequency and percentage calculations performed
  - Pie charts and bar graphs used for graphical analysis
  - Open-ended responses analyzed using **thematic analysis**

This provided both quantitative measurement and qualitative insight.

- **TOOLS AND FRAMEWORKS USED**

  - NIST Cyber security Framework (Identify–Protect–Detect–Respond–Recover)
  - ISO/IEC 27799 for health data protection
  - HIPAA Security Rule
  - GDPR data protection principles
  - OWASP, CVSS scoring for threat evaluation

- **ETHICAL CONSIDERATIONS**

  - Full anonymity of respondents
  - No personal or medical data collected
  - Data used strictly for academic purposes

- Compliance with ethical guidelines of HIPAA & GDPR

IV. SURVEY RESULT AND INTERPRETATION

A. RESULTS

- **GENERAL AWARENESS**

100% respondents are aware of cyber security.
Majority age group: **20–30 years**. Good foundation of basic cyber security knowledge.

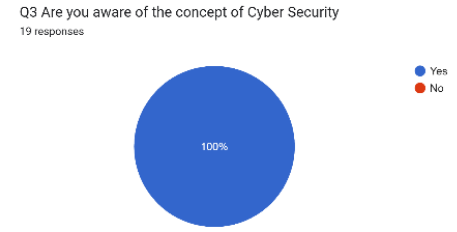

Fig. 1. Output of Q3 of survey form

A high level of awareness suggests a positive foundation for implementing cyber security practices. Younger respondents tend to be more familiar with technology, which may contribute to stronger basic knowledge of cyber security risks.

- **THREAT UNDERSTANDING**

Most recognized threats:
Hospital system vulnerabilities – 60% and Weak passwords – 40%

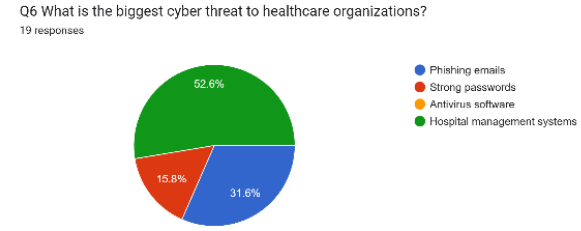

Fig. 2. Output of Q6 of survey form

The respondents correctly recognize technical vulnerabilities and poor authentication practices as key risk areas. This indicates that while awareness exists, organizations must improve technical controls, password policies, and access security.

- **DEVICE & SOFTWARE HABITS**

63% enable automatic updates, **37%** update manually. Manual updates increase vulnerability.

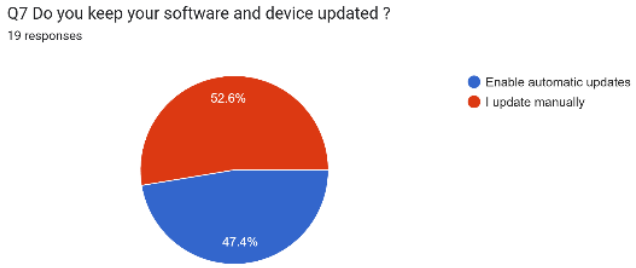

Fig. 3. Output of Q7 of survey form

Automatic updates reduce vulnerability to known exploits. Manual updating indicates potential risk exposure because delayed updates can make systems susceptible to malware or ransomware attacks.

- **PHISHING AWARENESS**

53% correctly identified "urgent action message" as phishing. Some confusion remains with "secure-looking links (https://)"

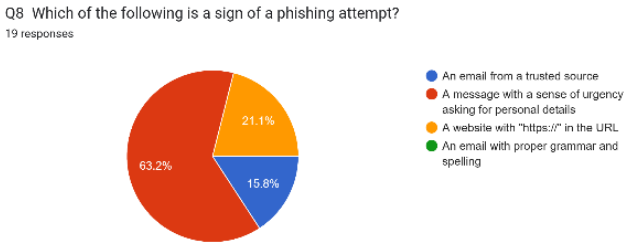

Fig. 4. Output of Q8 of survey form

This shows basic awareness of phishing threats but also highlights the need for better training in spotting deceptive URLs and email spoofing techniques. Human error continues to be a major risk factor.

- **REPORTING BEHAVIOUR**

Almost all respondents (around 90%) would report a threat immediately to IT/security.

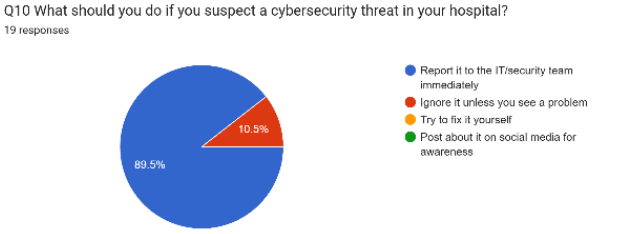

Fig. 5. Output of Q10 of survey form

This indicates a strong culture of reporting incidents, which is a positive sign for early detection and mitigation of cyber threats.

- **USB/EXTERNAL DEVICES**

80% aware that USB use causes malware risk and **20%** unaware or unsure

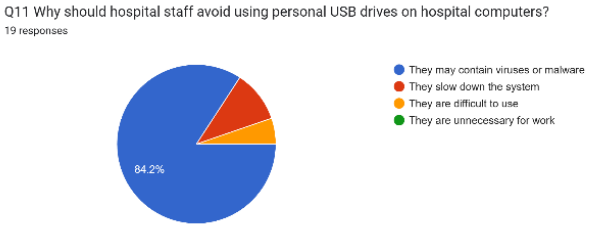

Fig. 5. Output of Q11 of survey form

External device misuse is a major cause of infections in hospital systems. Although awareness is high, the lack of 100% understanding highlights the need for strict device control policies and user education.

- **SYSTEM LOGOUT PRACTICE**

95% agree logging out prevents unauthorized access

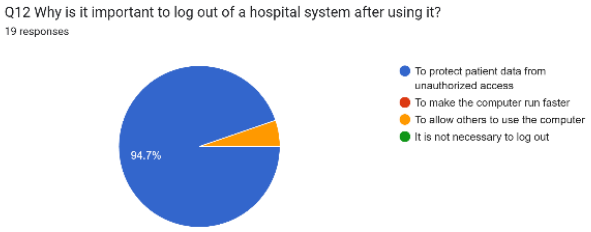

Fig. 6. Output of Q12 of survey form

This reflects good understanding of access control principles; however, real-world compliance must still be monitored because forgetting to log out is common in busy hospital environments.

- **WI-FI SECURITY AWARENESS**

60% prefer strong passwords **20%** change router credentials. Remaining respondents were unsure

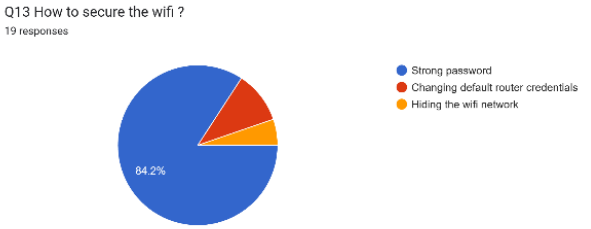

Fig. 7. Output of Q13 of survey form

Wi-Fi security awareness is moderate but not sufficient. Hospitals need stronger enforcement of secure wireless policies, especially because many medical devices connect over Wi-Fi.

- **IMPORTANCE OF CYBERSECURITY**

73% selected "All of the above" (protection, patient safety, service continuity)

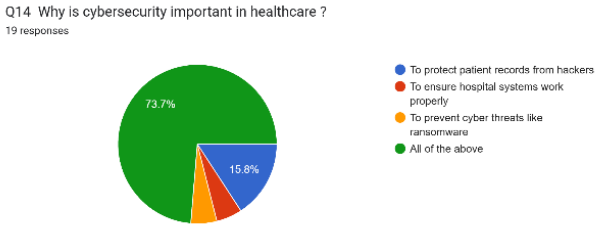

Fig. 8. Output of Q14 of survey form

Respondents understand cybersecurity as a multi-dimensional requirement rather than just a technical task. This mindset supports adoption of best practices.

- **PREFERRED IMPROVEMENT MEASURES**

67% selected "All of the above" (training, strong passwords, policies)

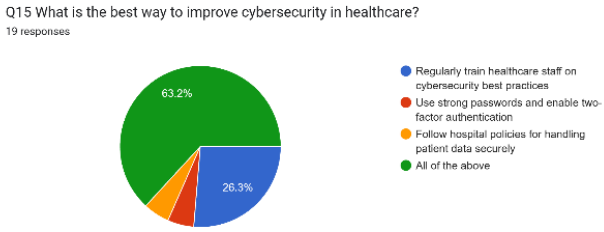

Fig. 9. Output of Q15 of survey form

This indicates support for integrated cybersecurity programs, emphasizing that no single solution is sufficient—technical, administrative, and human factors must all be addressed.

- **LEAST ADOPTED PRACTICE**

AI-based monitoring tools were used by **less than 20%**

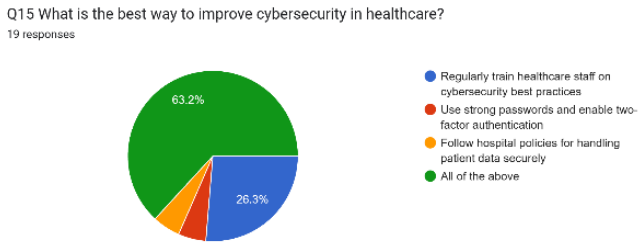

Fig. 10. Output of Q15 of survey form

Healthcare organizations still depend on traditional security measures. Limited adoption of modern monitoring tools exposes systems to sophisticated and persistent threats.

So, the insight from this is Phishing and IoMT vulnerabilities are the most common threats, whereas ransomware and data breaches are the most dangerous.

B. INTERPRETATION

- Awareness is high, but **implementation is inconsistent**.
- Human factors such as weak passwords and phishing susceptibility remain major concerns.

- IoMT and system vulnerabilities continue to increase healthcare risk exposure.
- Strong desire exists for more training and clear security policies.
- Advanced technologies (AI monitoring, automation, blockchain) are underutilized.
- Budget, outdated systems, and insufficient training remain the biggest barriers.

The results show that while respondents understand the importance of cyber security, healthcare institutions struggle with practical implementation due to technology constraints, lack of training, and limited resources. Strengthening cyber security awareness, enforcing stricter policies, and adopting modern security tools are essential for improving healthcare cyber security resilience.

V. ANALYSIS

- COMPARATIVE ANALYSIS

1. Healthcare vs Finance Sector

Parameter	Healthcare	Banking/Finance
Cyber Budget	5–6%	12–15%
Incident Response	Mostly Reactive	Proactive
Compliance	Partial	Strict
Data Sensitivity	Very High	High

2. Technology Comparison

Technology	Adoption	Security Risk	Mitigation
Cloud EHR	Increasing	Medium	Encryption & access control
AI/ML	Moderate	Low–Medium	Data anonymization
Blockchain	Low	Low	Decentralized storage

- ANALYSIS OF REGULATORY COMPLIANCE

.

Framework	Awareness	Implementation	Interpretation
HIPAA	70%	46%	Technical safeguards partially implemented
GDPR	52%	33%	Inconsistent enforcement
ISO/IEC 27799	40%	21%	Low adoption due to budget limitations
NIST CSF	28%	12%	Least followed framework

- THREAT ANALYSIS

Threat Type	Survey Frequency	Severity Level	Preventive Priority
Phishing	56%	High	Critical
Ransomware	22%	Very High	Critical
Insider Threat	16%	Medium	Moderate
IoMT Exploits	28%	High	High
Data Breach	10%	Very High	Critical

Insight: High awareness but low implementation due to training gaps, outdated systems, and minimal funding. Phishing and IoMT vulnerabilities are the most common threats, whereas ransomware and data breaches are the most dangerous.

VI. CONCLUSION

Healthcare systems today operate in an environment of increasing connectivity, with **Electronic Health Records (EHRs)**, **Internet of Medical Things (IoMT)** devices, **cloud-based infrastructures**, and **telemedicine platforms** forming the backbone of modern clinical operations. While these technologies enhance healthcare accessibility and efficiency, they also expand the attack surface available to cybercriminals.

The chapter begins by summarizing the research outcomes and key findings from literature, followed by an analytical conclusion regarding the state of cyber security preparedness in healthcare. It then provides practical recommendations—technical, administrative, and policy-oriented—to help organizations mitigate cyber risks. Finally, the chapter explores the future direction of research and innovation in healthcare cyber security.

The research underscores that cyber security in healthcare is not merely an IT concern—it is a **critical patient safety issue**. Hospitals and medical institutions are custodians of highly sensitive data, and breaches in these systems can lead to devastating outcomes, including financial loss, operational disruption, and even risk to human life.

Cyber security in healthcare is at a critical juncture. The convergence of technology and healthcare has brought unparalleled benefits but also unprecedented risks. Protecting patient information must become a **strategic priority**, not an afterthought. Strengthening cyber security requires **technical innovation, continuous staff education, and strong policy**

enforcement. Ultimately, safeguarding healthcare data is equivalent to **safeguarding patient trust and lives**.

VII. RECOMMENDATIONS

This section provides a set of **practical recommendations** based on the findings of the research. The recommendations are categorized into **technical**, **administrative**, and **policy-level** measures.

Category	Recommendation	Outcome
Technical	AI-based threat detection	Faster detection
Administrative	Staff training	Reduced human errors
Policy	Strong compliance audits	Improved data protection
Strategic	Increased security budget	Long-term resilience

VIII. FUTURE SCOPE

A. Integration of AI and Predictive Analytics: Future research should explore how predictive algorithms can automatically detect anomalies and predict security breaches before they occur.

B. Blockchain for Decentralized Health Record Systems:
Studies can focus on building scalable blockchain-based EHR systems ensuring data immutability, interoperability, and patient-controlled access.

C. Quantum-Resistant Encryption:
As quantum computing evolves, existing encryption methods may become obsolete. Research into quantum-safe cryptographic models for healthcare data is crucial.

D. Cybersecurity Maturity Models for Healthcare: Development of a universal maturity model can help institutions self-assess their cybersecurity readiness and prioritize improvements.

E. Cloud Governance and Compliance Automation: Investigate automated compliance monitoring tools for healthcare organizations migrating to hybrid or multi-cloud environments.

F. Socio-Behavioural Aspects of Cyber security: Understanding human psychology in phishing susceptibility and insider threat behavior can lead to better awareness and behavior-based defences.

G. Cross-Border Data Protection Frameworks: Global cooperation is needed to create consistent laws governing international sharing of medical data while maintaining privacy and security.

IX. REFERENCES

[1] Almgren, M., & Lindqvist, U., "Cybersecurity Challenges in Healthcare," *Journal of Medical Systems*, 2022.
[2] Ponemon Institute, "Cost of a Data Breach Report," 2021.
[3] Symantec, "Global Ransomware Trends," 2023.
[4] Symantec, "WannaCry Attack Impact Report," 2019.
[5] IBM Security, "Cybersecurity and Human Error Statistics," 2019.
[6] Braun, V., & Clarke, V., "Using Thematic Analysis," 2006.
[7] ENISA, "IoT and IoMT Security Challenges," 2021.
[8] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2018.
[9] ISO/IEC 27799, "Health Informatics—Information Security Management," 2016.
[10] Kruse, C. S., et al., "Cybersecurity in Healthcare: Systematic Review of Modern Threats," 2017.