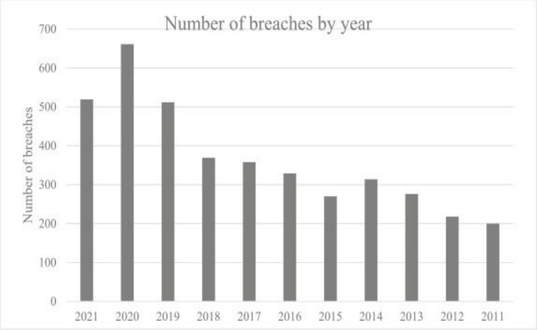
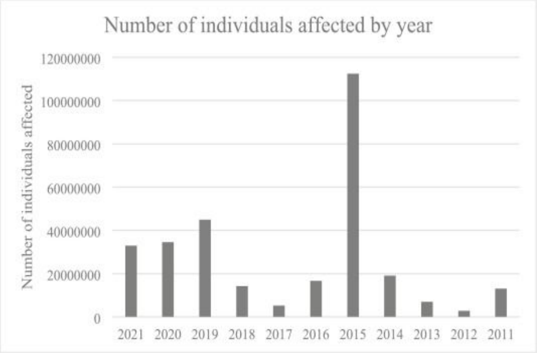
Ransomware and Device Vulnerabilities in Healthcare

Daniel Rajaram
New York University
Tandon School of Engineering
New York, USA

01

Problem/ Motivation





Ransomware and Device Vulnerabilities in Healthcare

Problem/Motivation

Healthcare cybersecurity challenges: ransomware and device vulnerabilities

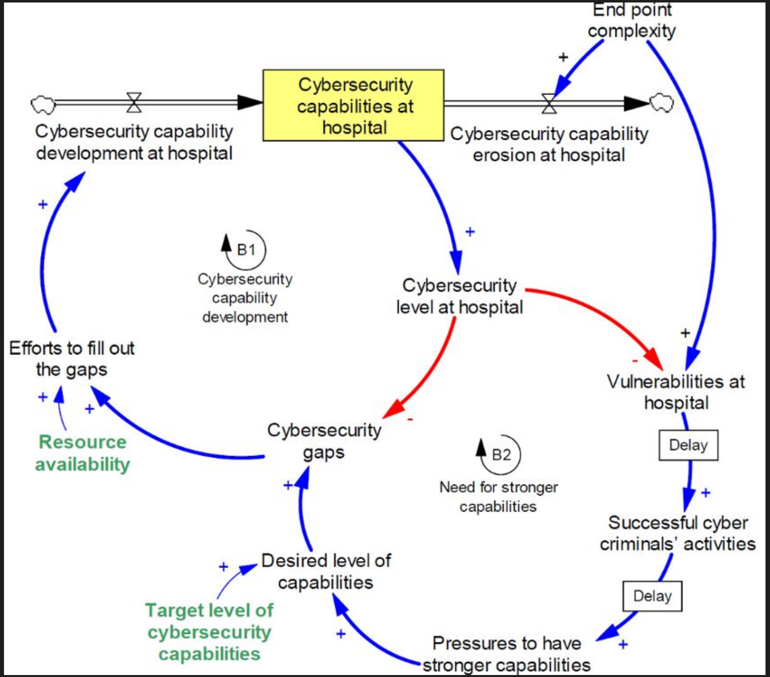
Personal experience at a cancer-focused biotech firm highlights data criticality

Vulnerability of medical institutions underscores the urgent need for robust cybersecurity.

The impact on patient care, privacy, and trust due to evolving cyber threats

02

Hypothesis


End point complexity
+
Cybersecurity capabilities at hospital
Cybersecurity capability development at hospital
Cybersecurity capability erosion at hospital
+
B1
Cybersecurity capability development
+
Cybersecurity level at hospital
+
-
Vulnerabilities at hospital
Efforts to fill out the gaps
+
+
Resource availability
-
Cybersecurity gaps
B2
Need for stronger capabilities
Delay
+
Successful cyber criminals' activities
+
Desired level of capabilities
+
Target level of cybersecurity capabilities
Delay
+
Pressures to have stronger capabilities
+

Ransomware and Device Vulnerabilities in Healthcare

Hypothesis

1 Comparative analysis of existing healthcare cybersecurity frameworks.

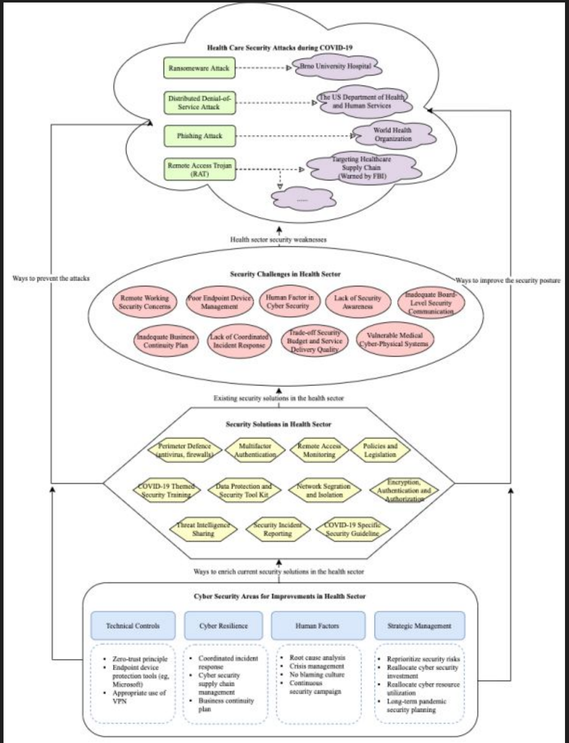
2 Development and implementation of a comprehensive medical device security structure.

3 Regular vulnerability assessments to expose strengths and weaknesses.

4 Aim for a 15% increase in the security resilience of medical institutions and devices.

03

Related Research


Health Care Security Attacks during COVID-19
Ransomeware Attack
Brno University Hospital
Distributed Denial-of-Service Attack
The US Department of Health and Human Services
Phishing Attack
World Health Organization
Remote Access Trojan (RAT)
Targeting Healthcare Supply Chain (Warned by FBI)
......
Health sector security weaknesses
Ways to prevent the attacks
Ways to improve the security posture
Security Challenges in Health Sector
Remote Working Security Concerns
Poor Endpoint Device Management
Human Factor in Cyber Security
Lack of Security Awareness
Inadequate Board-Level Security Communication
Inadequate Business Continuity Plan
Lack of Coordinated Incident Response
Trade-off Security Budget and Service Delivery Quality
Vulnerable Medical Cyber-Physical Systems
Existing security solutions in the health sector
Security Solutions in Health Sector
Perimeter Defence (antivirus, firewalls)
Multifactor Authentication
Remote Access Monitoring
Policies and Legislation
COVID-19 Themed Security Training
Data Protection and Security Tool Kit
Network Segration and Isolation
Encryption, Authentication and Authorization
Threat Intelligence Sharing
Security Incident Reporting
COVID-19 Specific Security Guideline
Ways to enrich current security solutions in the health sector
Cyber Security Areas for Improvements in Health Sector
Technical Controls
Cyber Resilience
Human Factors
Strategic Management
Zero-trust principle
Endpoint device protection tools (eg, Microsoft)
Appropriate use of VPN
Coordinated incident response
Cyber security supply chain management
Business continuity plan
Root cause analysis
Crisis management
No blaming culture
Continuous security campaign
Reprioritize security risks
Reallocate cyber security investment
Reallocate cyber resource utilization
Long-term pandemic security planning

Related Research

Overview of cyber threats in healthcare: emphasis on the high value of medical data.

Importance of the System Dynamics Model in reducing successful cybercriminal activity.

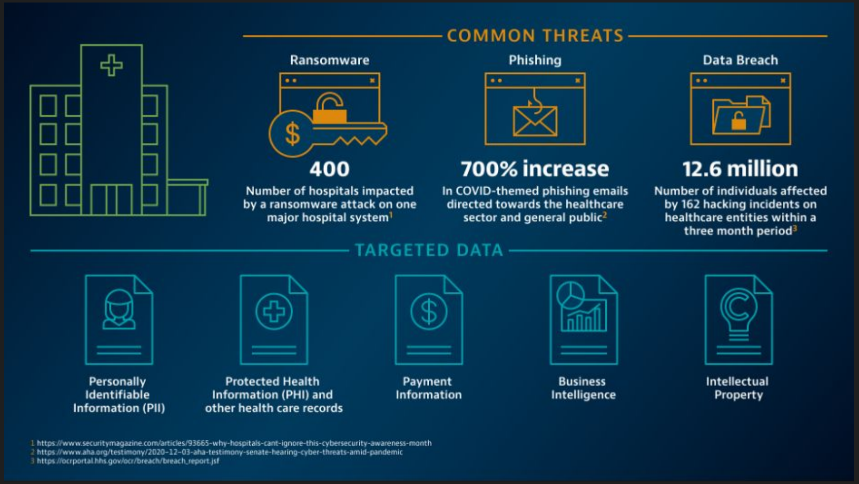
Impact of remote work on healthcare cybersecurity and documented cyber attacks during COVID-19.

Global growth of cyberattacks on healthcare: urgency for robust security measures.

The resource imbalance and the need for ongoing cybersecurity training in healthcare.

04

Implementation



COMMON THREATS

Ransomware

400

Number of hospitals impacted by a ransomware attack on one major hospital system[1]

Phishing

700% increase

In COVID-themed phishing emails directed towards the healthcare sector and general public[2]

Data Breach

12.6 million

Number of individuals affected by 162 hacking incidents on healthcare entities within a three month period[3]

TARGETED DATA

Personally Identifiable Information (PII)

Protected Health Information (PHI) and other health care records

Payment Information

Business Intelligence

Intellectual Property

[1] https://www.securitymagazine.com/articles/93665-why-hospitals-cant-ignore-this-cybersecurity-awareness-month
[2] https://www.aha.org/testimony/2020-12-03-aha-testimony-senate-hearing-cyber-threats-amid-pandemic
[3] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Ransomware and Device Vulnerabilities in Healthcare

Implementation

1 Methodology for empirical studies and vulnerability assessments.

2 Analytical supported analysis of the current issue domain (Section II).

3 All-encompassing framework for device security outlined in Section VI.

Implementation

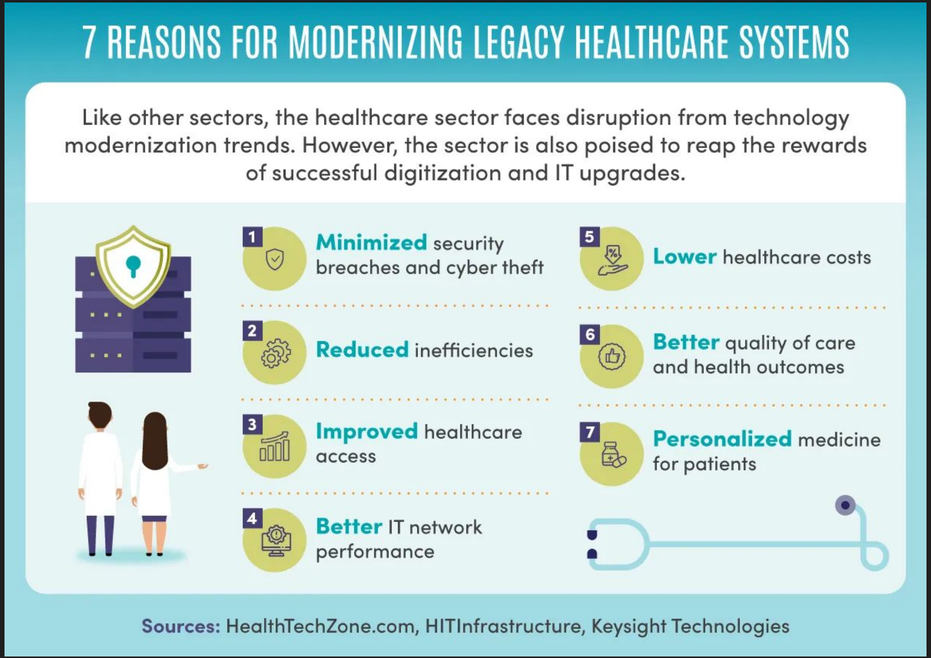
4 Challenges of diverse IT infrastructure, evolving attack methods, and legal limitations.

5 Acknowledgment of natural constraints like resistance to change in healthcare institutions.

6 Detailed insights into the research process, emphasizing practical approaches.

05

Findings



7 REASONS FOR MODERNIZING LEGACY HEALTHCARE SYSTEMS

Like other sectors, the healthcare sector faces disruption from technology modernization trends. However, the sector is also poised to reap the rewards of successful digitization and IT upgrades.

1. **Minimized** security breaches and cyber theft
2. **Reduced** inefficiencies
3. **Improved** healthcare access
4. **Better** IT network performance
5. **Lower** healthcare costs
6. **Better** quality of care and health outcomes
7. **Personalized** medicine for patients

Sources: HealthTechZone.com, HITInfrastructure, Keysight Technologies

Ransomware and Device Vulnerabilities in Healthcare

Findings

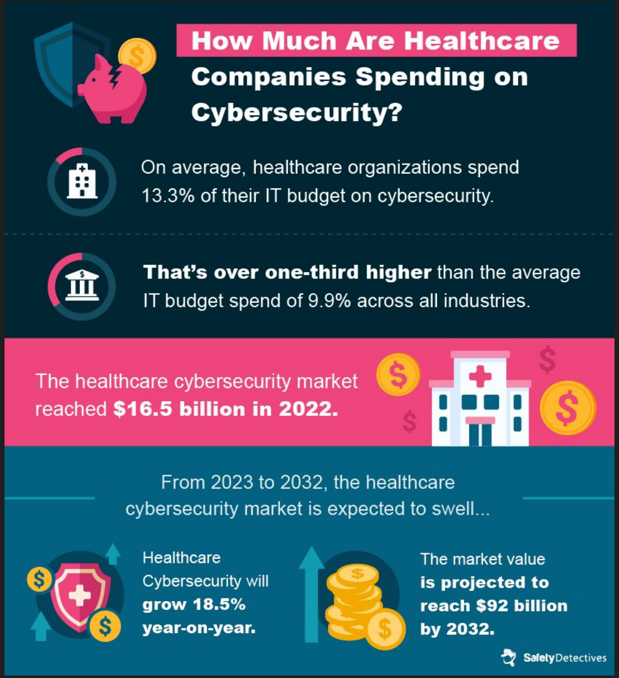
Evidence from studies: healthcare industry caught between funding restraints and cybersecurity.

Stats from past decade's cyber incidents emphasize the urgency for dependable solutions.

Proposed solution of a proactive medical device security framework finds strong backing.

06

Next Steps



How Much Are Healthcare Companies Spending on Cybersecurity?

On average, healthcare organizations spend 13.3% of their IT budget on cybersecurity.

That's over one-third higher than the average IT budget spend of 9.9% across all industries.

The healthcare cybersecurity market reached **$16.5 billion in 2022.**

From 2023 to 2032, the healthcare cybersecurity market is expected to swell...

Healthcare Cybersecurity will **grow 18.5% year-on-year.**

The market value **is projected to reach $92 billion by 2032.**

SafetyDetectives

Ransomware and Device Vulnerabilities in Healthcare

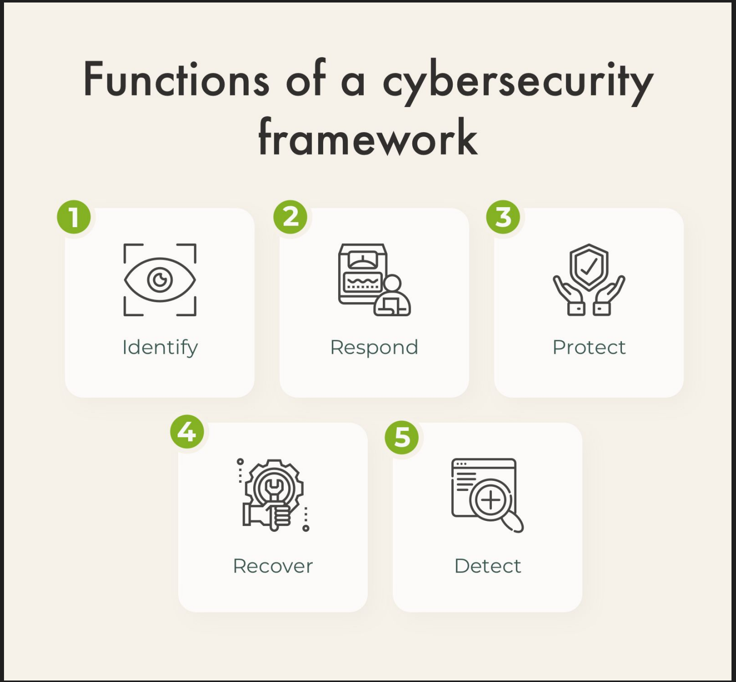
Next Steps

- Exploration of innovative approaches and emerging technologies.
- Addressing ongoing needs for cybersecurity training and advanced security tools.
- Collaborative efforts to establish industry-wide cybersecurity standards.

- Extending research to include specific case studies and real-world implementations.
- Partnerships with healthcare institutions for practical testing and refinement of proposed solutions.

07

Conclusion



Functions of a cybersecurity framework

1 Identify

2 Respond

3 Protect

4 Recover

5 Detect

Ransomware and Device Vulnerabilities in Healthcare

Conclusion

Recap of Research

- Internal stakeholder alignment issues exacerbate the challenge, making it difficult to strike a balance between IT needs and security imperatives.

- The dynamic culture of healthcare institutions, coupled with the use of diverse devices, adds complexity to cybersecurity efforts.

Conclusion

Proactive Approach and Industry Resistance:

- Proposed solution advocates a proactive medical device security framework, deviating from reactive fixes commonly seen in the healthcare sector.
- Industry resistance to change necessitates not just patching up after an attack but staying ahead of the game in the often-change-resistant healthcare environment.

Challenges and Urgency:

- Healthcare industry faces a critical juncture balancing funding constraints and the pressing need for robust cybersecurity.
- The era of remote work and the aftermath of the COVID-19 pandemic intensify vulnerabilities, exposing gaps in technological literacy and security measures.

References

- [1] M. S. Jalali and J. P. Kaiser, “Cybersecurity in Hospitals: A Systematic, Organizational Perspective,” Journal of Medical Internet Research, vol. 20, no. 5, p. e10059, May 2018, doi: https://doi.org/10.2196/10059.
- [2] Y. He, A. Aliyu, M. Evans, and C. Luo, “Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review (Preprint),” Journal of Medical Internet Research, vol. 23, no. 4, 2020, doi: https://doi.org/10.2196/21747.
- [3] D. Tin, R. Hata, F. Granholm, R. G. Ciottone, R. Staynings, and G. R. Ciottone, “Cyberthreats: A primer for healthcare professionals,” The American Journal of Emergency Medicine, Apr. 2023, doi: https://doi.org/10.1016/j.ajem.2023.04.001.
- [4] Neprash HT, McGlave CC, Cross DA, et al. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. JAMA Health Forum. 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873