Digital Security Threats in Healthcare

How to Protect Your Hospital System

Presentation by Barr Beneli, Demetris Perdikos, Anand Patel, Johnny Yu

Current State of Threats: An Overview

- Most common cyber threats in healthcare:a ransomware, phishing, insider threats
- Recent examples of high-profile breaches: Scripps and Trinity Health
- Impact of cyber attacks on patient care: delays in treatment, loss of records, misdiagnosis
- Consequences for hospital operations: downtime, financial losses, legal liabilities

Photo by Pexels

Current State of Threats

- Increased frequency and severity of attacks
- Various types of attacks (e.g. phishing, DDoS)
- New and evolving threats (e.g. AI-powered attacks)
- Impact on healthcare organizations

Modes of Attacks

- Malware and ransomware: encrypting data, locking systems, demanding ransom payments
- Phishing and social engineering: targeting employees, impersonating trusted sources, stealing login credentials
- Insider threats: unauthorized access, data theft, intentional sabotage
- Emerging threats: IoT vulnerabilities, supply chain attacks, Advanced Persistent Threats (APTs)

Impact on Healthcare Systems

- Patient Data Compromises
- Disruption of Healthcare Services
- Healthcare Research and Intellectual Property

Photo by Pexels

Securing Healthcare Systems

- Risk Assessment and Vulnerability Analysis
- Implementing Robust Security Measures
- Incident Response Planning

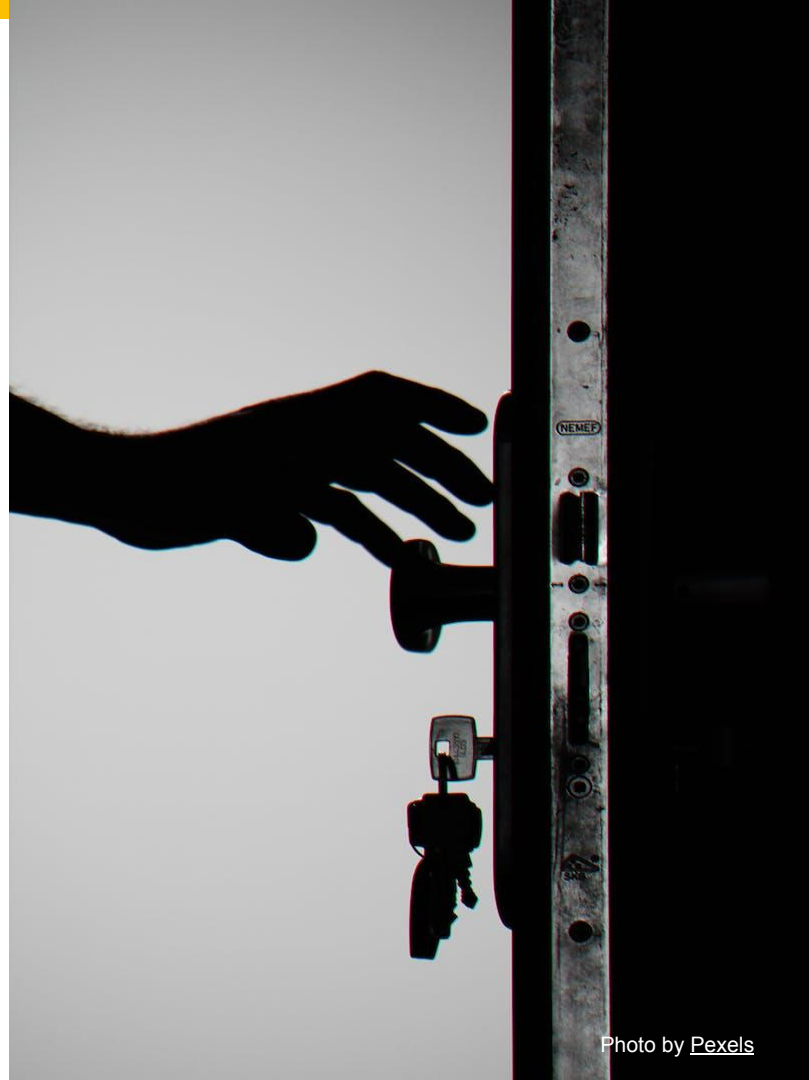
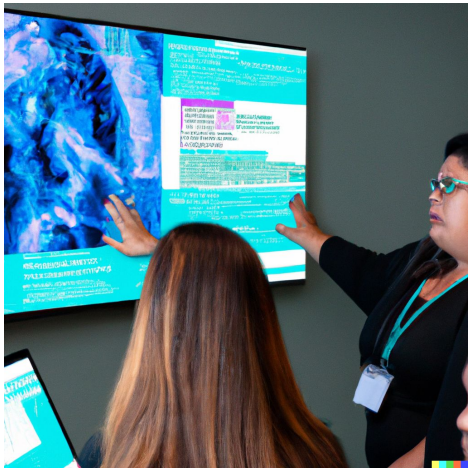


Photo by Pexels

Cybersecurity Best Practices

- Employee Training and Awareness
- Access Control and Authentication
- Backup and Recovery



Case Study - Scripps

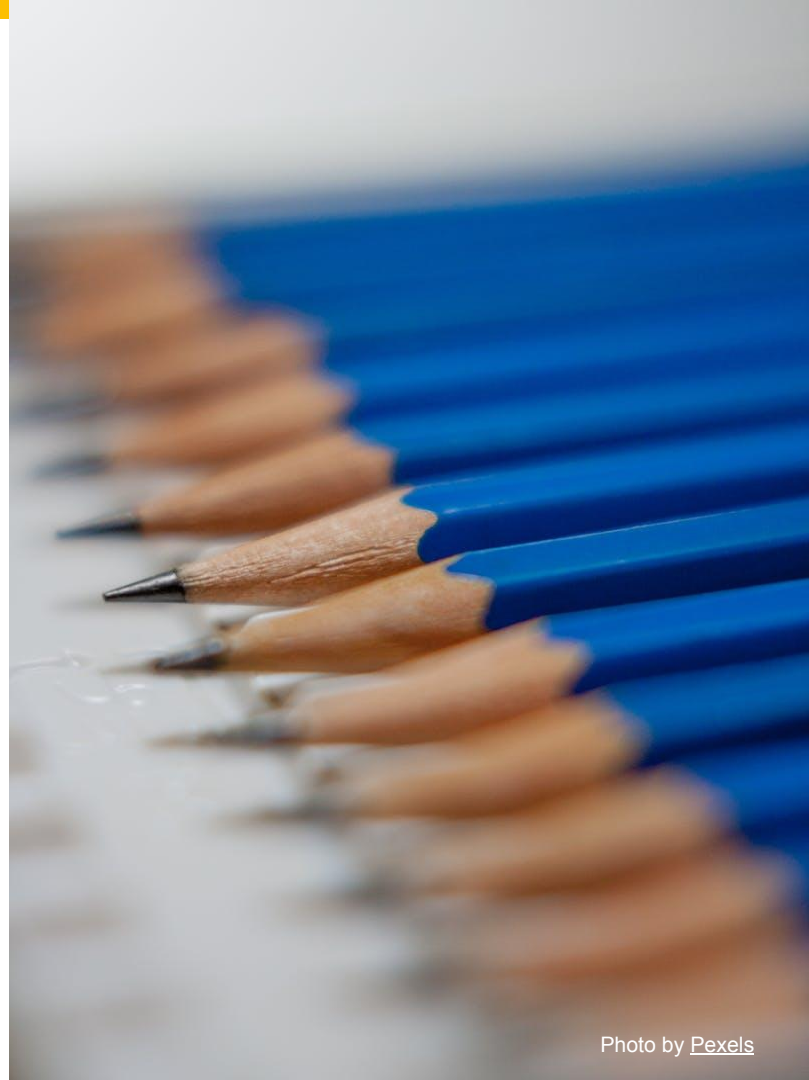
- Scripps Health faced attack in May 2021
  - Ransomware
- Cost $112.7 Million
  - Insurance covers $14 Million
- Data of ~150000 patients stolen
- Took more than 1 month to resolve
- Several Class Action Lawsuits

Case Study - Trinity Health

- Trinity Health faced attack in May 2020
  - Ransomware
  - Resolved by paying hackers
  - Potentially still data
- Another Attack in 2021
  - Collateral of Accellion Ransomware
  - Data of more than ~500000 patients stolen

Preparing Your Healthcare System

- Developing and implementing a cybersecurity plan
- Risk assessment done regularly, comprehensively every two years
  - Includes any 3rd party vendors
- Integrating security into the organization's culture
- Encouraging safe cybersecurity practices for all personnel.



Conclusion

- Cybersecurity training and good practices
- Importance of digital security in healthcare
- Healthcare systems remain as the most critical sector for cybersecurity
- Preparing defenses for AI-based attacks

Sources:

- https://www.fiercehealthcare.com/health-tech/healthcare-data-breach-costs-reach-record-high-10m-attack-ibm-report
- https://www.fiercehealthcare.com/hospitals/may-cyber-attack-cost-scripps-nearly-113m-lost-revenue-more-costs
- https://www.upguard.com/blog/biggest-data-breaches-in-healthcare
- https://www.paubox.com/blog/over-half-million-trinity-health-patients-affected-data-breach

Photo by Pexels