Digital Security Threat in Hospital Systems

Team 6: Dhruv Amin, Rashmi Hazarika, Jakub Kowal

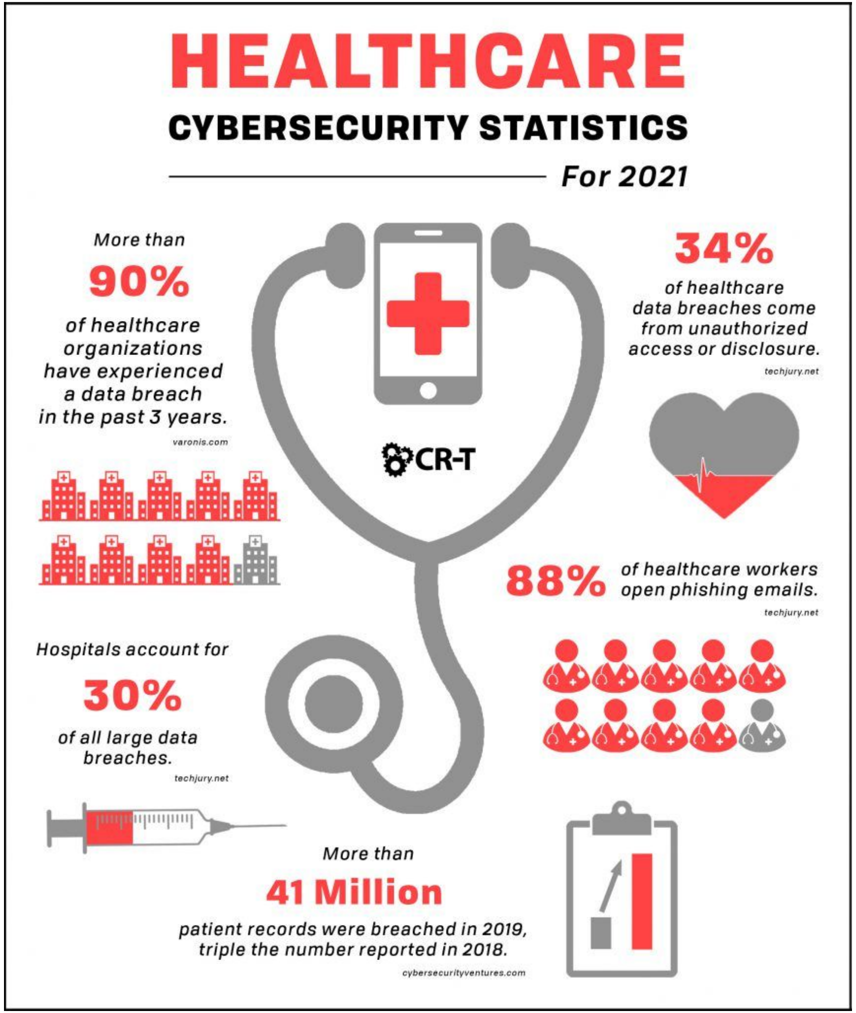
Introduction

As the digital world continues to grow, so do the volume, variety, and velocity of cyber threats and attacks. The world is awash in data, and there is always someone trying to turn it into their own virtual currency. Today malware and ransomware are hitting everything from our personal cell phones to mission-critical infrastructure and supply chains.

We have been hired by a large hospital system to do an analysis of the digital security threat that it may be facing.

Background

- Increased interconnectivity raises digital security concerns
- Poses major risks to individuals, corporations, and civilizations
- Chronic cybercrime and hacking techniques that are always changing
- Data breaches, malware assaults, phishing scams, and ransomware exploits
- Can harm personal and organizational privacy, economics, and reputation.
- Understanding these dangers is critical for digital security.



HEALTHCARE

CYBERSECURITY STATISTICS

For 2021

More than **90%** *of healthcare organizations have experienced a data breach in the past 3 years.* varonis.com

34% *of healthcare data breaches come from unauthorized access or disclosure.* techjury.net

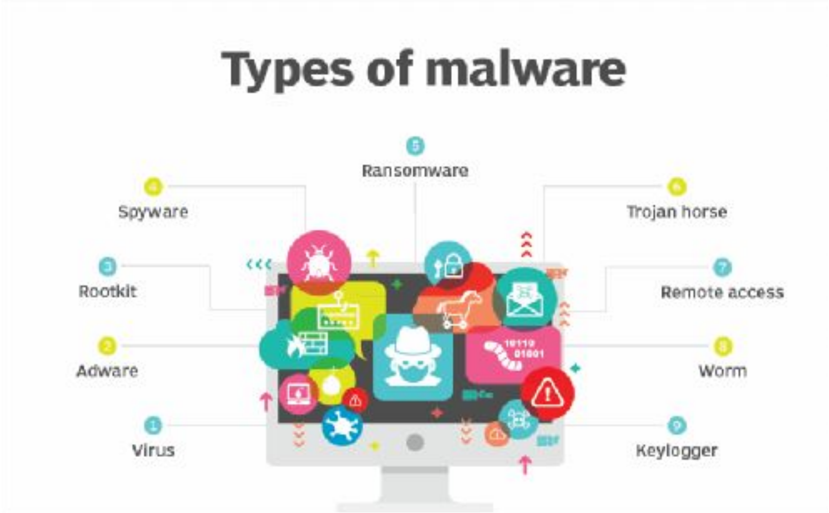
88% *of healthcare workers open phishing emails.* techjury.net

Hospitals account for **30%** *of all large data breaches.* techjury.net

More than **41 Million** *patient records were breached in 2019, triple the number reported in 2018.* cybersecurityventures.com

Malware

- Malicious software intentionally created to harm a computer, network, or server.
- Trojan Horse
- Viruses
- Spyware

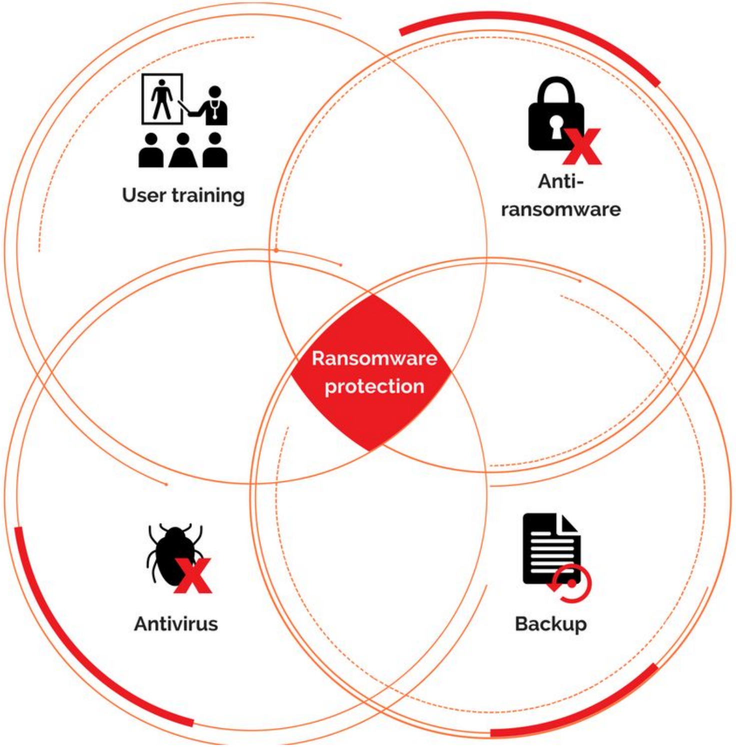


Ransomware

- Designed to deny a user or organization access to files on their system
- WannaCry
- Petya/NotPetya

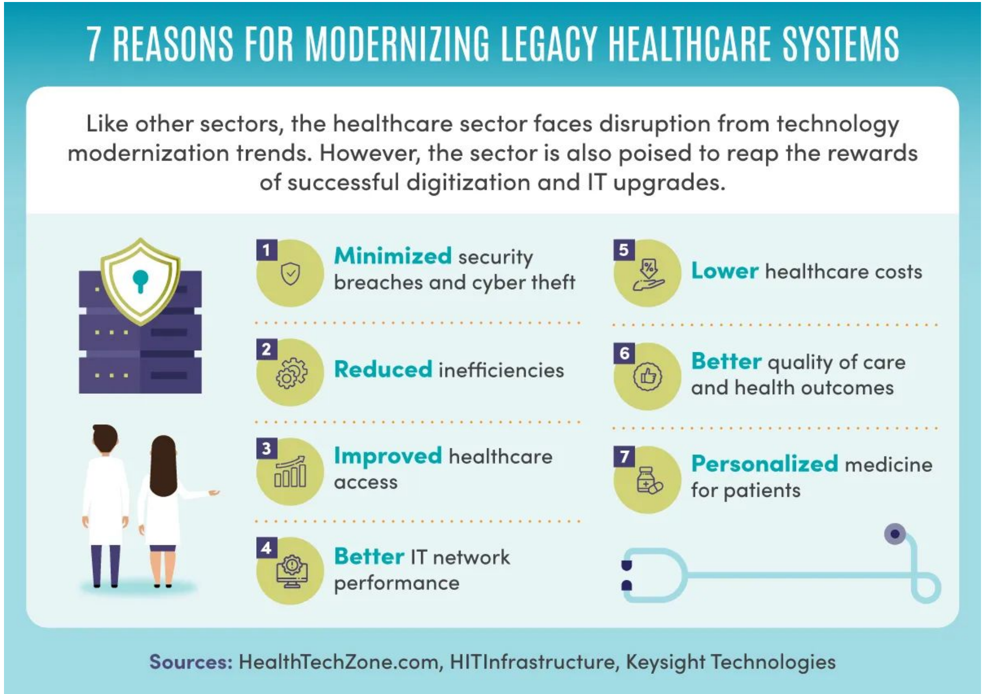
Common Protection Strategies

- Use Reliable Security Software
- Regular Updates
- Backup Data
- Educate Users
- Network Segmentation
- Incident Response Plan



Hospital Information Systems

- Manages administrative, financial, and clinical needs
- Electronic Health Records (EHRs)
- Health tracking devices
- Medical equipment
- Software used for healthcare delivery and management



7 REASONS FOR MODERNIZING LEGACY HEALTHCARE SYSTEMS

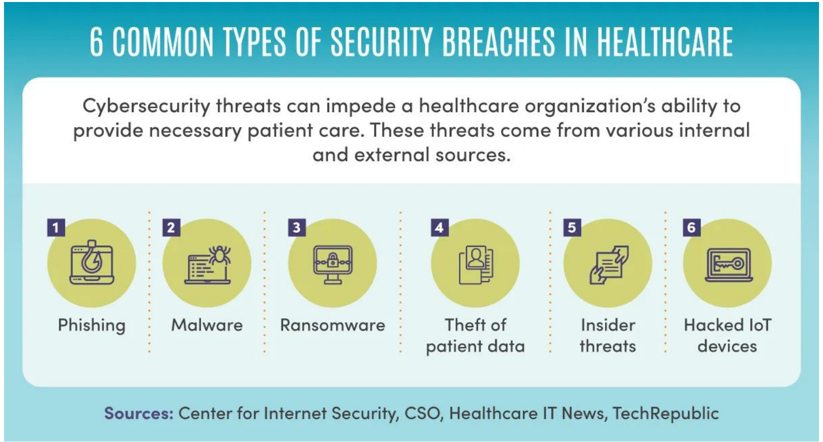
Like other sectors, the healthcare sector faces disruption from technology modernization trends. However, the sector is also poised to reap the rewards of successful digitization and IT upgrades.

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

Hospital Security Threats

- External with local or remote actors
- Internal though deliberate or inadvertent acts
- Motives: Financial gains, terrorism
- The cybersecurity firm Emsisoft reports that the U.S. had more than 560 cyber attacks against healthcare facilities in 2020



6 COMMON TYPES OF SECURITY BREACHES IN HEALTHCARE

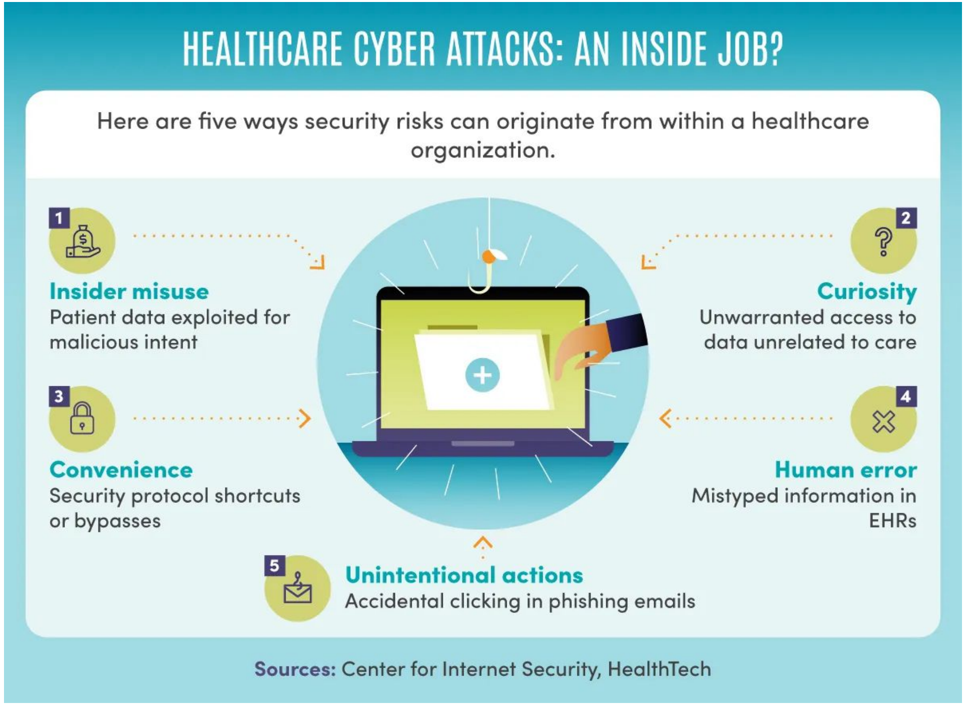
Cybersecurity threats can impede a healthcare organization's ability to provide necessary patient care. These threats come from various internal and external sources.

1. Phishing
2. Malware
3. Ransomware
4. Theft of patient data
5. Insider threats
6. Hacked IoT devices

Sources: Center for Internet Security, CSO, Healthcare IT News, TechRepublic

Vulnerabilities

- Electronic Patient Record (ERP) Systems focus on functionality over cybersecurity
- Nature of the work makes it extremely sensitive to any disruption in its services
- Humans are the weakest link in cybersecurity



HEALTHCARE CYBER ATTACKS: AN INSIDE JOB?

Here are five ways security risks can originate from within a healthcare organization.

1 **Insider misuse**
Patient data exploited for malicious intent

2 **Curiosity**
Unwarranted access to data unrelated to care

3 **Convenience**
Security protocol shortcuts or bypasses

4 **Human error**
Mistyped information in EHRs

5 **Unintentional actions**
Accidental clicking in phishing emails

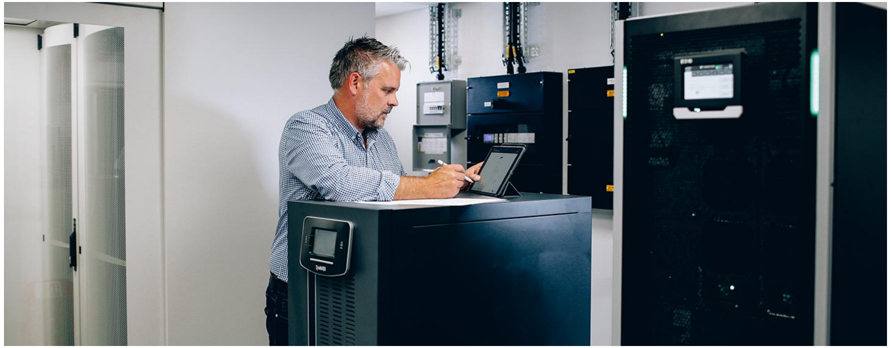
Sources: Center for Internet Security, HealthTech

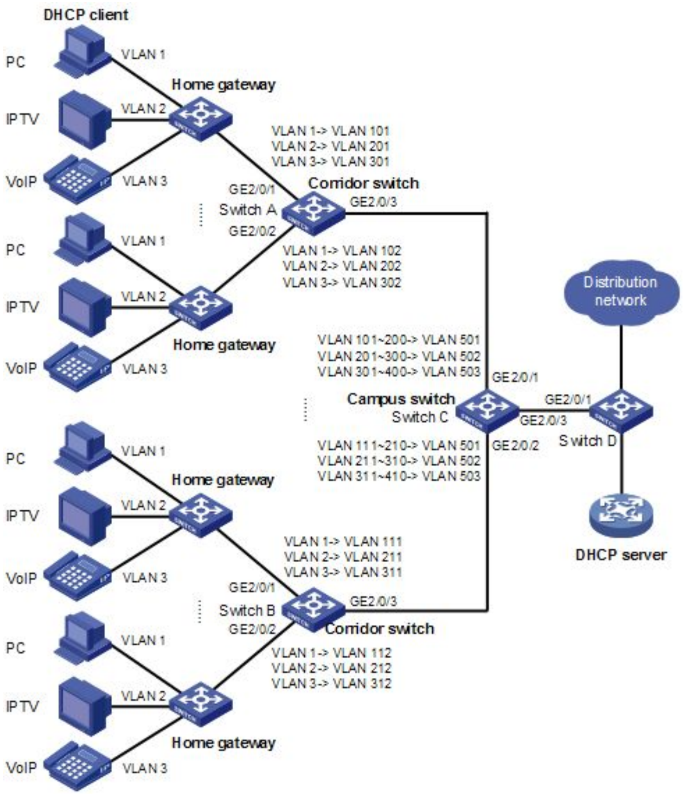
Current Actions taken by Hospitals: Personal

- User training
- Practice phishing emails
- Authorizations
- Multi Factor Authorization (MFA)
- Secrecy
- Familiarity

Current Actions taken by Hospitals: Network

- Multiple Networks
- Backups
- Disaster planning
- Collaboration with cyber security experts





Current Actions taken by Hospitals: Hardware

- Keeping systems up to date
- Encryption
- Anti-virus software

Conclusion

- Malware and ransomware are major security threats
- Hospital systems store health and patient information
- Critical steps include improving security procedures, raising staff awareness, revising contingency actions, and incorporating ongoing assessment in real time

References

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7062337/

https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-018-0724-5

https://usa.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

https://online.maryville.edu/blog/healthcare-cybersecurity/

https://www.emsisoft.com/en/blog/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/

https://www.talkinghealthtech.com/glossary/hospital-information-systems-his

https://www.digitalguardian.com/blog/20-information-security-tips-hospitals

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2655907/

https://www.ivanti.com/blog/securing-iomt-devices-best-practices-for-hospitals-to-prevent-cyberattacks

https://www.techtarget.com/searchsecurity/definition/malware

https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/