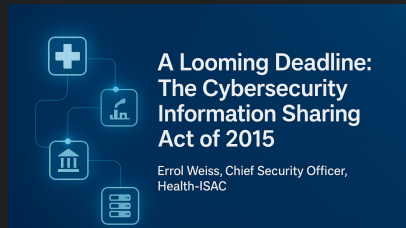
Cybersecurity in Healthcare

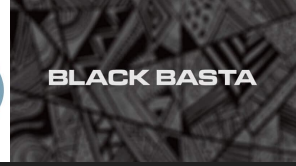
By MYLES DAMOAH, ASHER EMBRY, DERRICK HURDLE, NICHOLAS ROSSLER AND ERIC ZHAO

Introduction to Cybersecurity in Healthcare

- Cybersecurity was introduced as a formal and critical component of the healthcare system with the HIPAA act of 1996
- In 2003 HIPAA passed the security rule which established a national standard for hospitals around the world that protects electronic protected health information which contains private information of patients ,employees and much more.
- After the 2003 security rule was enforced in 2005 action started being taken against those who broke it.
- Following that in 2015 The: Cybersecurity Information Sharing Act of 2015 (CSA) was passed due to several breaches and attacks on healthcare
- To pair with that in 2017 the FDA mandated all medical device manufacturers to improve security to maximize patient safety if machines were attacked.



Present Day Challenges

- Cybercriminals take advantage of any world health crisis ex.COVID-19(1,587 attacks)
- According to hhs.gov anywhere from between 14%-20% of malicious attacks are inside jobs and with negligence it increases to between 53%-63%
- 25% of healthcare providers also had their ID stolen which led to data leaks
- Millions of lives are at stake, hackers can threaten things like life support,diversion of medical assistance, leaking of medical information among many others.
- Critical life-saving functions consists of connected, networked systems that leverages wireless technologies, which in turn leave such systems more vulnerable to cyber-attacks.
- In America alone 28.5 million ambulances rides are active and if a hospital gets attacked emergency services have to divert risking patient safety
- 61% of hospitals are reported to pay the ransom due to lack of time or too many lives at risks
- Cybersecurity professionals report they have to do 24/7 hour surveillance with a underfunded budget which can increase human error with less sleep and support from the hospital itself.
- High-stress small team security facing a focused hacker group which most of the time has an inside leak

Attacks on the Industry

- Attacks on the Healthcare industry continue to increase, in 2022 the number of attacks increased by 42% compared to 2021.
- Industrial Cyber shows In 2025, it grew 30% compared to 2024.
- According to ASPR, the average cost of a healthcare data breach is 10.93 million. This is an 8% increase from the previous year of 10 million.
- Between the years 2005-2019 249.09 million individuals were affected by healthcare data breaches, with over 150 million of those being in the last 5 years.
- Breached data on patients can be altered leading to the wrong data being stored, leading to faulty treatment or no treatment at all endangering patients.
- An example of this is the WannaCry virus attack in 2017, which diverted ambulances and caused surgeries to be canceled.
- HIPAA Journal reports, 29% of reported cyber attacks saw an increase in mortality rates.

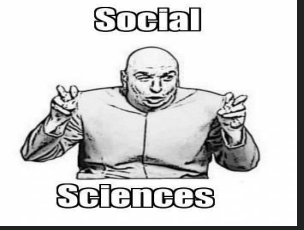
Notable Attacks

Change Healthcare (UnitedHealth Group) – Feb 2024

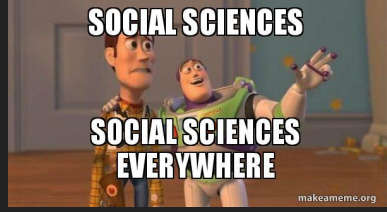
- Type: Ransomware
- Target: The largest healthcare payment processor in the U.S.
- Impact:
  - Financial: Estimated total cost to UnitedHealth exceeds $1 billion
  - Operational: Processed 15 billion transactions annually; outage stopped payments to hospitals and pharmacies nationwide for weeks
  - Significance: highlighted extreme vulnerability in the healthcare supply chain (third-party vendor risk)

Anthem (now Elevance Health) – Jan 2015

- Type: State-sponsored Data Breach / Phishing
- Target: Second-largest health insurer in the U.S
- Impact:
  - Data Stolen: 78.8 million patient records (names, SSNs, DOBs)
  - Cost: Agreed to a $115 million class-action settlement (largest in history for a data breach at the time)
  - Significance: Marked a shift towards hackers targeting medical data for identity theft rather than just immediate financial extortion



Social Sciences and Theories



Criminology- Society fears hackers more because it deals with immediate life and death.

Psychology- Hackers use human emotions against them to get the ransom paid.

Sociology- The hospitals job in the social sphere is to protect the patient first so they can be an easy target to pay out without much fight back.

2 Personality Traits

Neuroticism- Healthcare and Cyber workers are highly stressed due to low funding and long hours making it easier to attack.

Agreeableness- Workers cooperate more than often due to having lives at stake.

Protection of Patient Data

Protecting Patient data is important because it protects patient privacy, build patient trust, and leads to better and accurate care. Here are some ways healthcare providers have entrusted cybersecurity to protect your information using the CIA triad.

- RBAC - Medical professionals can only access certain patient information based on their roles in the system
  - This secures confidential patient information to only a select few members of the healthcare staff

- Encryption - Patient data cannot be accessed unless user has the right key
  - Even if data is stolen it cannot be read as it is scrambled.

- Regular data backups

  -In case of a disaster or massive data breach, hospitals constantly backup patient information to keep their data available incase of a crisis.

Implications For Public Health

- As medical infrastructure rapidly digitizes, there is a increased need for stronger cybersecurity.

  - Ewoh & Vartiainen conducted a study in 2024 on cybersecurity vulnerabilities in healthcare systems it showed that the vulnerabilities are grouped into 5 themes: human error, old legacy systems, lack of investment, complex network connected end-point devices, and technological advancement.

- If the defensive measures against cyber attacks are lacking, patient data can be lost and other crucial systems can be severely affected.

- Investment into cybersecurity programs and education becomes necessary to secure the public health sector not just technologically, but also as a means to maintain trust in the healthcare system.

- Healthcare is the critical infrastructure that has fallen behind the most and the recent attacks should be seen as a wake-up call to increase funding into digital protection especially when lives can be at risk.

- As over 37.5% of attacks on the industry come from an employee in healthcare, HIPAA officials can implement stricter security and background checks in the future. Per https://www.hhs.gov/sites/default/files/insider-threats-in-healthcare.pdf

Key Takeaways

- The healthcare industry is a high-priority target for cyber criminals due to its importance in daily life and potential profit from carrying out an attack.
- Regulations aim to ensure proper security within the industry, and impose harsh punishments when not properly followed
- The Healthcare industry falls behind in terms of cybersecurity and is underfunded leading to stressful situations more than other infrastructure
- Healthcare is catching up but due to a later start can still suffer more attacks than average
- One of the most important infrastructures only behind national security due to the amount of lives at stake
- Cybersecurity is essential in healthcare and needs even more attention as hackers evolve in the modern day

THANK YOU

Works Cited

- Ewoh P, Vartiainen T

  Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review

  J Med Internet Res 2024;26:e46904

  URL: https://www.jmir.org/2024/1/e46904

  DOI: 10.2196/46904

- Insurance.gov

  Anthem Data Breach

  URL: https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm

- U.S Department of Health and Human Services

  The Service Rule

  URL:https://www.hhs.gov/hipaa/for-professionals/security/index.html

- Center For Internet Security

  Cybersecurity for Healthcare & Life Sciences

  URL: https://www.cisecurity.org/industry/healthcare

Works Cited (continued)

- Cybersecurity and Infrastructure Agency

  Information Sharing Act of 2015

  URL: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf

- Anna Ribeiro

  IndustrialCyber.co

  Healthcare ransomware attacks surge 30% in 2025, as cybercriminals shift focus to vendors and service partners

  URL: https://industrialcyber.co/reports/healthcare-ransomware-attacks-surge-30-in-2025-as-cybercriminals-shift-focus-to-vendors-and-service-partners/

- Health and Human Services

  Insider Threats in Healthcare

  URL: https://www.hhs.gov/sites/default/files/insider-threats-in-healthcare.pdf

- Adil Hussain Seh, et al.

  Healthcare Data Breaches: Insights and Implications

  URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC7349636/#sec1-healthcare-08-00133