CYBERSECURITY IN HEALTHCARE: A SOCIAL SCIENCE PERSPECTIVE

By Jamil Palacios

WHY TARGET HEALTHCARE?

PATIENT DATA

Medical records have higher resale value than credit card and can be exploited longer

SHARED IT SYSTEMS

Hospitals and healthcare providers often share systems, allowing a larger vector of theft

VITAL DEPENDENCY

When lives and data are at risk, hospitals must decide between human health and finances.

LEGACY SYSTEMS

It's not uncommon to find hospitals still running outdated software and hardware.

BUDGET RESTRAINTS

As public institutions, they don't often prioritize money for cybersecurity.

Reasons

KEY CYBERSECURITY CHALLENGES

Ransomeware attacks:

Locking staff out of vital systems behind encryption, thus making it inaccessible and effectively paralyzing operations. Until a usually high extortion is paid out, even then there's no guarantee that data is intact or confidential.

Social engineering:

Posing as collogues online though to obtain credentials and/or records from the hospital staff. Utilizing a mix of fear and trust to coarse the mostly busy and susceptible personnel from question their legitimacy.

Thrid party vulnerabilities :

the same standard of cybersecurity is not applied to external vendors, who may have a considerably gaps whilst retaining their access. Which in some cases may be patient data that isn’t protected.

SOCIAL SCIENCE ASPECTS

Equity

As the frequency of cyber attacks on hospitals increases, it's the rural and low-income areas that are disproportionately affected. They're staff are often unequipped and untrained to handle the growing sophistication that data breaches entail.

Behavioral Factors

It's the human factor that often causes a gap in security, enabling exploitation. A mere click makes it possible to cripple and expose systems of high importance.

Trust and Patient Confidence

Once a breach does occur, the damages are not limited to the patients; the institutions themselves become the target of many in ire. Eroding trust in the public sector's ability to handle sensitive information.

Policy and Governance

It's the structure of organizations and regulations that determines the effectiveness of an institution's responses. Accountability can only be achieved if the policy that governs is clear and adaptive.

Ethical Responsibility

Leadership and management must rebalance their priorities of safety and swiftness to extend into the digital world. The respect for their patients must carry over to all the facets the hospital operates in, even the intangible ones like cybersecurity.

CASE STUDY 1 – WANNACRY ATTACK (2017)

Details	Damage	Legal reaction
On May 12, 2017, a ransomware outbreak occurred globally, propagating itself through the EternalBlue exploit and reaching 150 countries. This malware relied on the SMB protocol exploit and the DoublePulsar backdoor. It had infected the UK's NHS resulting in 19,000 canceled appointments.	£92m (about $122m)	The UK parliament would come to spend a further £150m to accelerate cyber hygiene measure improvements and upgrades.

CASE STUDY II – UNIVERSAL HEALTH SERVICES (2020)

Details	Damage	Legal reaction
Between September 26-27, 2020, Universal Health Services experience a ransomware attack that forced its systems offline for several weeks. Resulting in staff using paper-based process for the duration, causing undue stress and increased risk of errors.	$67m	No large demands from government were made, however serval suits were field against UHS on grounds on HIPPA violations, most did not proceed.

CASE STUDY III – CHANGE HEALTHCARE BREACH (2024)

Details	Damage	Legal reaction
In February 2024, Change Healthcare suffered a ransomware attack that had affected its national operations, as it was a subsidiary of UnitedHealth Group. Insurance claims, billing, and transactions were halted, leaving hospitals stuck as to validating coverage and creating a financial strain. An exploit had been discovered in the infrastructure of Change Healthcare, who themselves were an intermediary and vital point in the healthcare industry.	$22m in ransomed, with an estimated total of $3b	The Nebraska Attorney General had filed a lawsuit against Change Healthcare, alleging 900,000 Nebraskan were affected. With many other lawsuits filed by both regulators and individuals.

SOCIETAL IMPLICATIONS AND IMPROVEMENTS

Far Reaching Safety:

We cannot continue to look at cybersecurity as an IT issue, that view does nothing good. As seen in healthcare, those with absolutely nothing to do in that department are simultaneously helpless and affected once a breach occurs. If we are to properly address this issue, then it must be recognized for the real-world damages it causes and treated as such.

Trust & Equity:

Health institutions must rebuild the trust of the public by establishing better and fairer safety investments and making them transparent. To avoid vulnerable populations from suffering disproportionately and present themselves as unreliable.

Necessary Collaboration:

It’s simply not possible for one group to solve this matter themselves; it’s therefore necessary to draw on other institutions in a united effort to develop resilience and standards against cyber attacks. By accepting a collective responsibility that enforces industry-wide standards and safeguard patients can we begin to effectively protect against breaches.

REFERENCE

Cyber-attack on the NHS - Committee of Public Accounts - House of Commons. (2015). Parliament.uk. . https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/78707.htm

Hughes, O. (2018, October 12). Government puts cost of WannaCry to NHS at £92m. Digital Health. https://www.digitalhealth.net/2018/10/dhsc-puts-cost-wannacry-nhs-92m/

Jiang, J. X., Ross, J. S., & Bai, G. (2025). Ransomware Attacks and Data Breaches in US Health Care Systems. JAMA Network Open, 8(5), e2510180. https://doi.org/10.1001/jamanetworkopen.2025.10180

Johnson, L. (2024, December 5). Change Healthcare Data Breach Settlement Talks to Start This Month. The HIPAA Guide. https://www.hipaaguide.net/change-healthcare-data-breach/

MSU study: Ransomware drives US health data breaches. (2025). Michigan State University. https://msutoday.msu.edu/news/2025/05/msu-study-ransomware-drives-us-health-data-breaches

National Audit Office. (2017, October 27). Investigation: WannaCry cyber attack and the NHS - National Audit Office (NAO) report. National Audit Office (NAO). https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

Newman, L. H. (2020, September 28). A Ransomware Attack Has Struck a Major US Hospital Chain. Wired. https://www.wired.com/story/universal-health-services-ransomware-attack/

Popowitz, E. (2025). Top trends of 2026: Cybersecurity breaches emphasize the importance of secure tech in healthcare. Definitive Healthcare. https://www.definitivehc.com/blog/healthcare-cybersecurity-impacts-patient-care

VALiNTRY360. (2025, September 18). VALiNTRY360. https://valintry360.com/blogs/6-cybersecurity-lessons-from-the-universal-health-cyber-attack