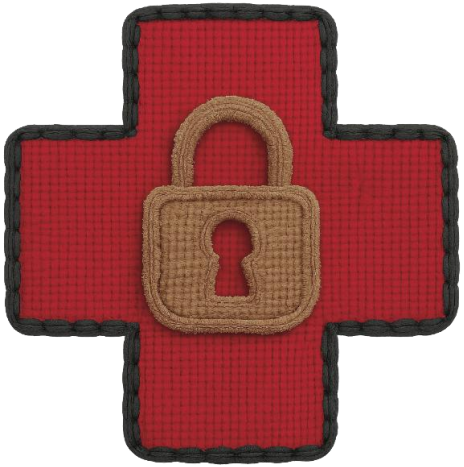
Northeastern University



Medical Device Cybersecurity – Week 4

01/27/2025 – Cybersecurity in Healthcare

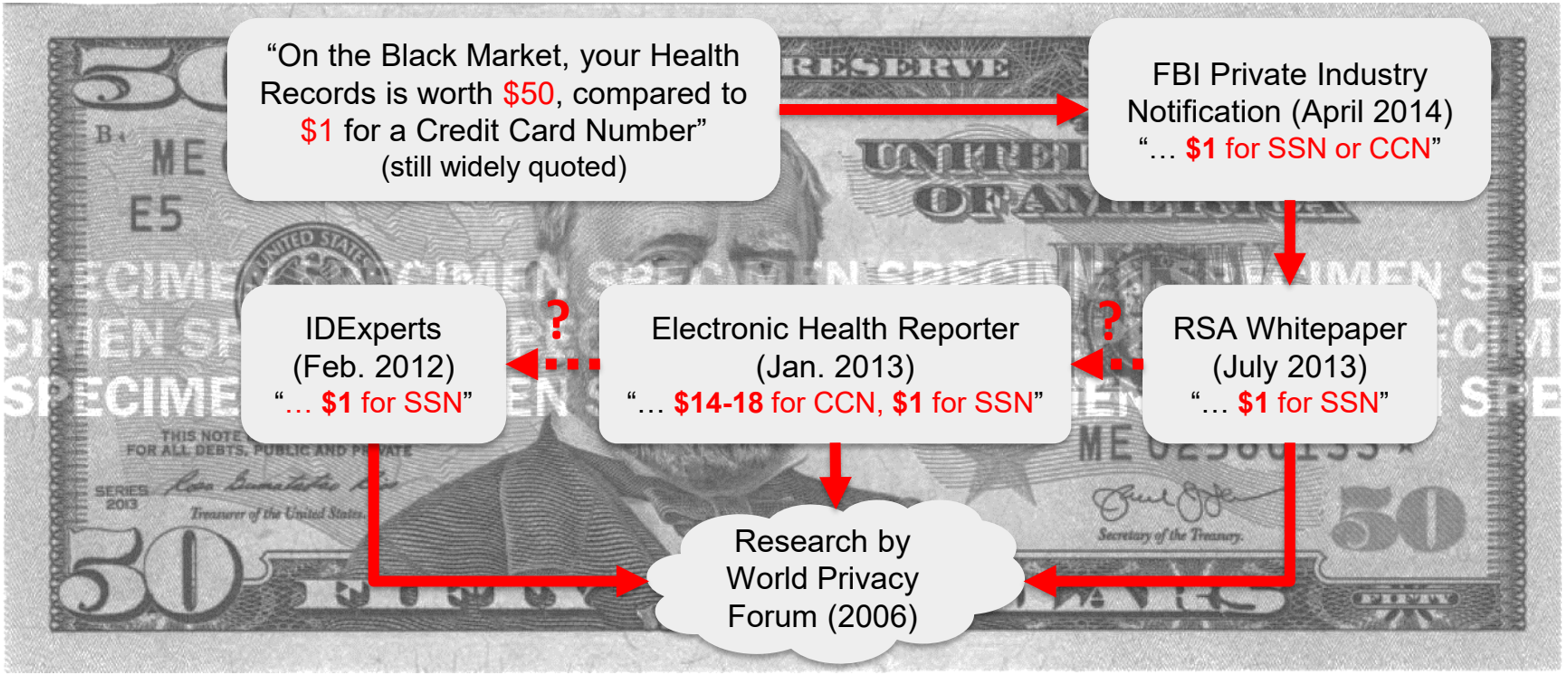
Axel Wirth | Chief Security Strategist | Medcrypt
axel@medcrypt.com

Healthcare Cybersecurity
Knowns and unknowns

- Cyber Threats
- Systemic Vulnerabilities
- Reported Events & Incidents
- Healthcare Industry Posture and Response

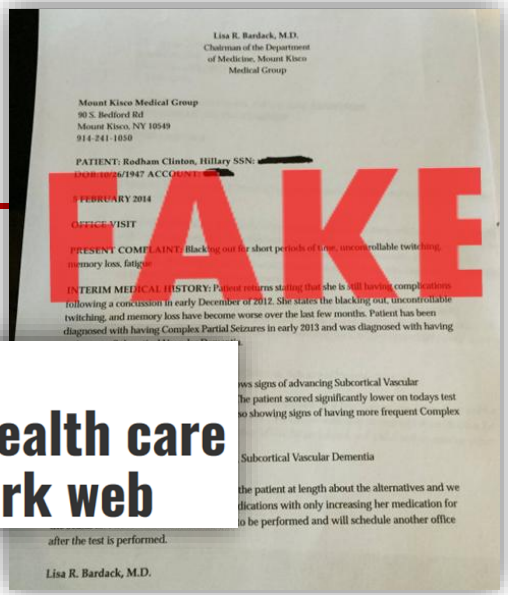
The Danger of Examples …

Value of Health Data in the Underground Economy – Myths



Today's Reality is Far More Complex

But - there certainly is plenty.



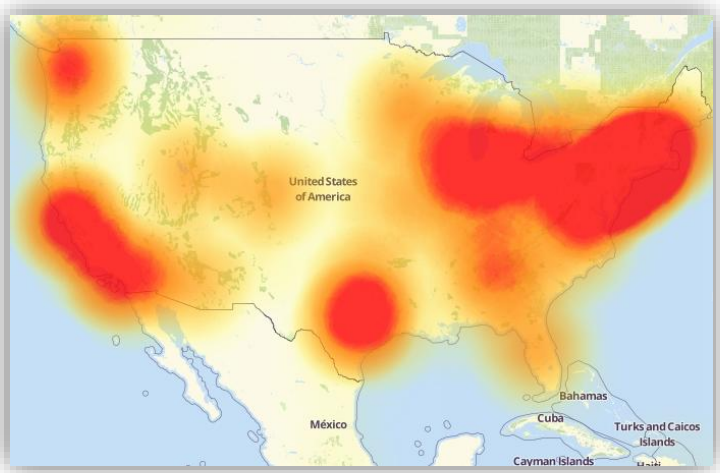
From a few $'s to $1,000 …
to free …

… to unquantifiable.

Adversary Motivation and Objectives

- Nation States – political motivation
  - Intellectual property
  - Supporting political or economic goals
- Hacktivists – varying causes
  - Political or social goals
  - Have not shied away from critical infrastructure (e.g., Boston Children's; Flint, MI water district)
- Cybercriminals – financial motivation
  - Most simple form – make money through ransomware attacks or dark web sale of goods
  - Highly professionalized – cybercrime as a service
  - May contract with or sell to nation states – lines can be blurry
- Individual Hackers
  - Still out there
  - Intellectual curiosity, fame, idealism
  - Some recent headline-grabbing cyber events were eventually traced back to individuals

Security Never Sleeps - the Mirai Botnet

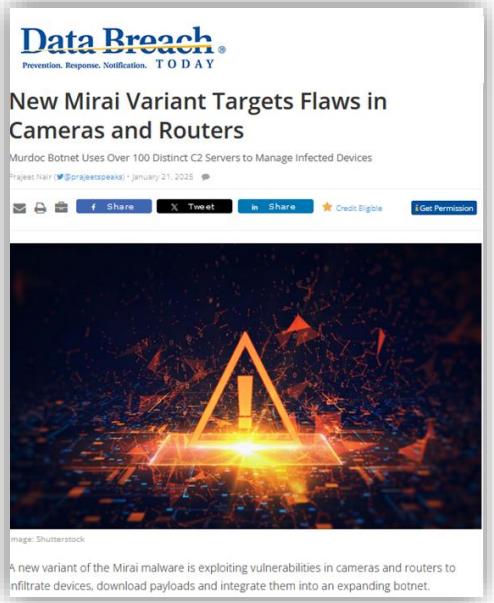


2016

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

2023

https://spectrum.ieee.org/mirai-botnet



2025

https://www.databreachtoday.com/new-mirai-variant-targets-flaws-in-cameras-routers-a-27343

Destructive Threat Actors

https://www.infosecurity-magazine.com/news/wiper-attack-polish-power-grid/

Few Known Cases of Direct Patient Harm

Harvard Business School

FEBRUARY 2023 CASE HBS CASE COLLECTION

Ransomware Attack at Springhill Medical Center

By: Suraj Srinivasan and Li-Kuan (Jason) Ni

Format: Print | **Language:** English | **Pages:** 12

Email Print Share Recommend 0 Share

ABSTRACT

In July, 2019, Springhill Medical Center ("SMC") in Mobile, Alabama, fell prey to a malicious ransomware attack that crippled the hospital's internal network systems and public-facing web page. While the hospital rushed to securely restore the network, medical personnel scrambled workarounds to continue medical services. Amidst the chaos, a baby was born in the hospital with the umbilical cord wrapped around her neck that had resulted in severe brain injury and died nine months later. The mother and family sued SMC, alleging the hospital failed to inform her of the cyber incident, which she believed had compromised the quality of care and led to an otherwise preventable tragedy. The case discusses the important questions of how SMC had responded to the ransomware attack and how hospitals and other organizations should treat the ever-increasing threat of cyber breaches.

https://www.hbs.edu/faculty/Pages/item.aspx?num=63611

BBC

Ransomware attack contributed to patient's death

25 June 2025 Share

Jess Warren BBC News

The death of one person has been linked to a ransomware attack on NHS blood services at London hospitals and GP surgeries last June.

King's College Hospital NHS Foundation Trust confirmed that one patient had "died unexpectedly" during the cyber attack on 3 June 2024, which disrupted more than 10,000 appointments.

A spokesperson for the trust said a number of contributing factors led to the patient's death including "a long wait for a blood test result".

https://www.bbc.com/news/articles/cp3ly4v2kp2o

ECRI Top 10 Health Technology Hazards

PATCH

Since 2015, Cybersecurity has been on ECRI's Top 10 list

The List for 2026

1. The Misuse of AI Chatbots in Healthcare
2. Unpreparedness for a "Digital Darkness" Event
3. The Growing Challenge of Combating Substandard and Falsified Medical Products
4. Recall Communication Failures for Home Diabetes Management Technologies
5. Tubing Misconnections Remain a Threat Amid Slow ENFit and NRFit Adoption
6. Underutilizing Medication Safety Technologies in Perioperative Settings
7. Deficient Device Cleaning Instructions Continue to Endanger Patients
8. Cybersecurity Risks from Legacy Medical Devices
9. Technology Designs or Configurations That Prompt Unsafe Clinical Workflows
10. Water Quality Issues During Instrument Sterilization

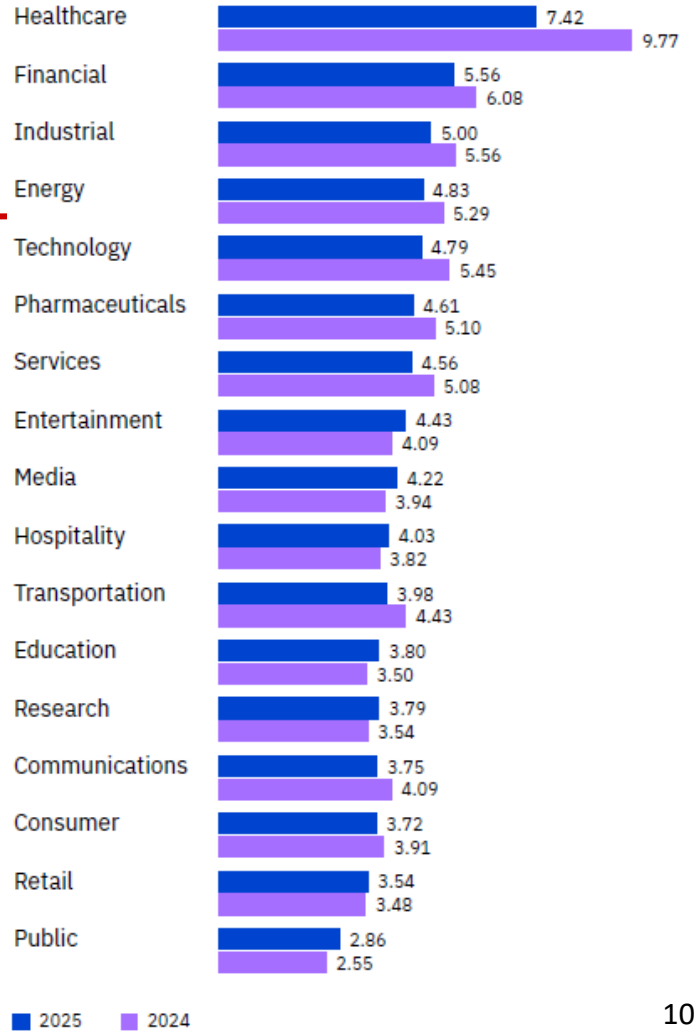
https://www.ecri.org/2026hazards

2026 #2	Unpreparedness for a "Digital Darkness" Event
2026 #8	Cybersecurity Risks from Legacy Medical Devices
2025 #4	Medical Error and Delay in Care Resulting from Cybersecurity Breaches
2024 #6	Ransomware Targeting the Healthcare Sector Remains a Critical Threat
2023 #5	Failure to Manage Cybersecurity Risks Associated with Cloud-Based Clinical Systems
2022 #1	Cybersecurity Attacks can Disrupt Healthcare Delivery, Impacting Patient Safety
2021 #7	Vulnerabilities in Third-Party Software Components Present Cybersecurity Challenges
2020 #7	Cybersecurity Risks in the Connected Home Healthcare Environment
2019 #1	Hackers Can Exploit Remote Access to Systems, Disrupting Care Delivery
2018 #1	Ransomware and Other Cybersecurity Threats
2017 #6	Software Management Gaps Put Patients, and Patient Data, at Risk
2016 #10	Misuse of USB Ports Can Cause Medical Devices to Malfunction
2015 #9	Cybersecurity: Insufficient Protections for Medical Devices and Systems

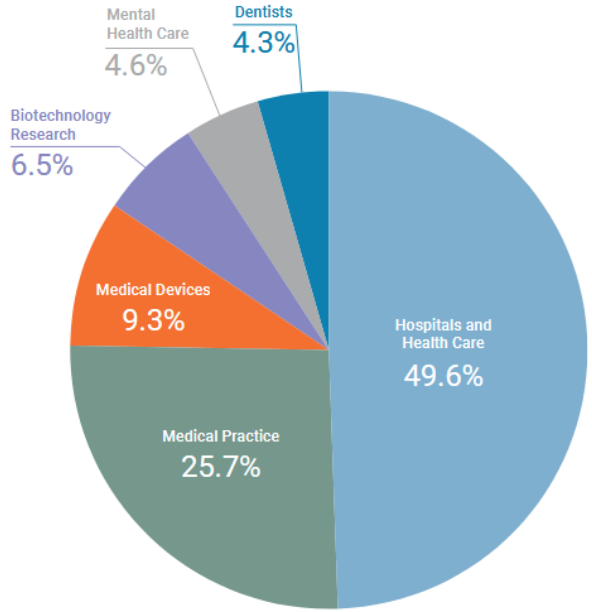
Cost of Data Breach
(USD millions)

Although down from 2024 (which was down from 2023), the Healthcare industry still leads as the highest cost of a data breach.

IBM: Cost of a Data Breach Report 2025
Healthcare = Hospitals & Clinics



Threat Landscape



Health Sector Ransomware Victimology

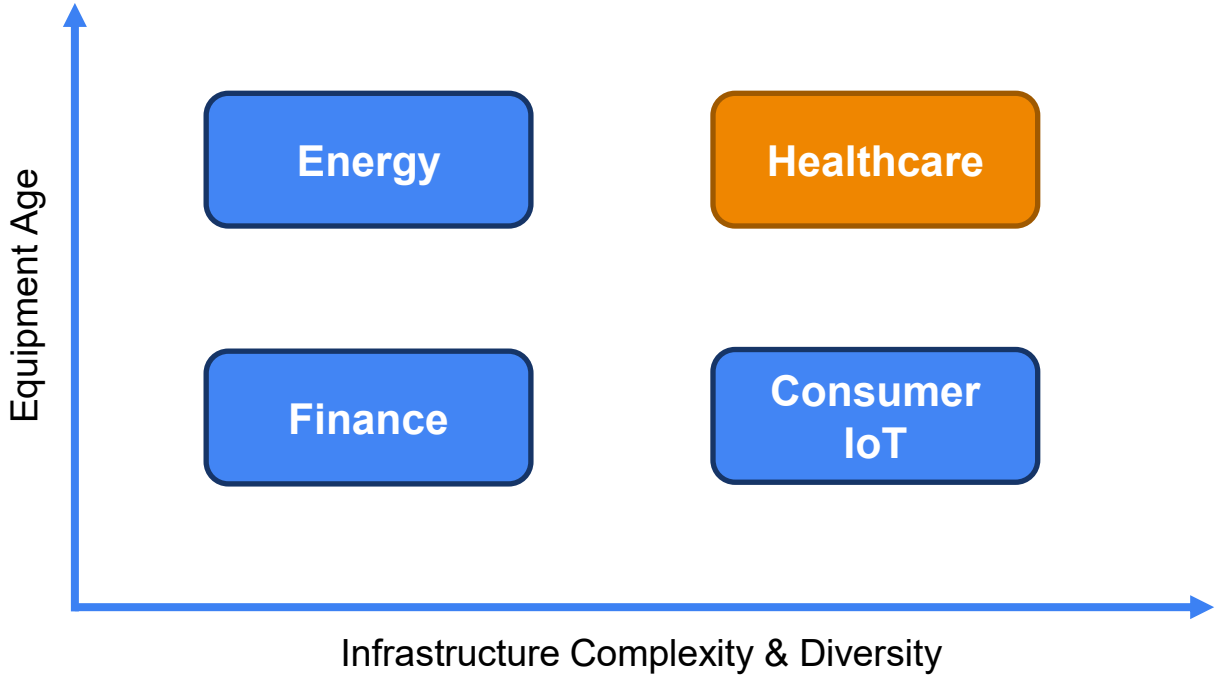
Healthcare Cybersecurity
Knowns and unknowns

- Cyber Threats
- Systemic Vulnerabilities
- Reported Events & Incidents
- Healthcare Industry Posture and Response

Challenges with Implementing Cybersecurity in Healthcare

- Legacy System Challenges (medical devices and others)
  - Can also be found in other industries
  - SW EOL << Equipment useful life
  - Greatest concern: EOL Operating Systems (e.g. Windows)
  - Replacement cost, clinical utility, vendor mandare
- Technical Complexity
  - Disparate inventory of systems - large number of devices and vendors
  - Complex attack surface to secure and defend
  - Wide variety of security maturity
- Organizational Complexity
  - Distributed responsibilities and complex decision making
- Common Healthcare Practices Conflict Strict Security
  - Patients first
  - Traditionally trusting and open
  - Traditionally a compliance-driven industry (HIPAA)

Healthcare is a Uniquely Challenged Industry – Conceptual Comparison



Complexity and Impact of Risks – Beyond C-I-A

Patient Safety

- Intentional or unintentional incidents
- Quality of care (functionality, reliability)
- Direct impact due to misdiagnosis, treatment errors

Privacy

- Confidentiality: breach of PHI, PII, credentials
- Intellectual property (clinical trials & research)
- Financial data, HR, contracts, M&A, etc.

Care Delivery

- Downtime due to system availability
- Impact on hospital operations
- Reduction or delay in ability to deliver care

Attack Vector

- Exploitation of a weak system – beachhead attack
- Denial of Service (DDoS) attack (origin of or impacted by)
- May be targeted or purely opportunistic

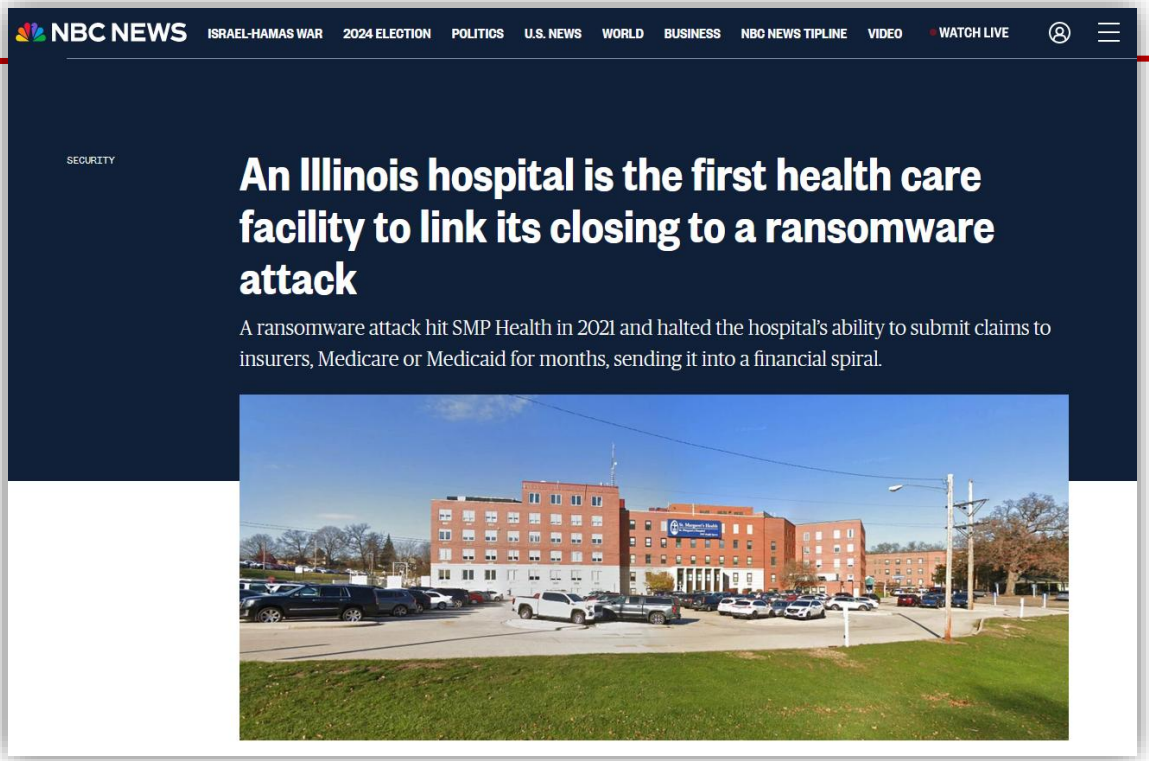
Business & Financial

- Reputation
- Revenue / Referrals
- Lawsuits / fines
- Stock value

Indirect Risks

- Patient trust
- Patient treatment decisions
- Staff morale
- National Security

Potential for Dire Consequences



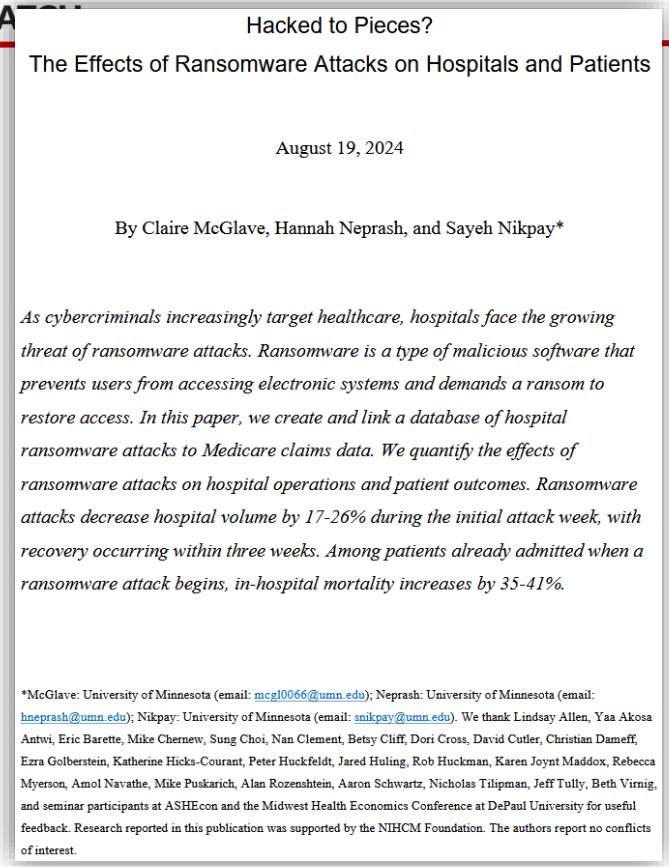
https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983

Healthcare Cybersecurity
Knowns and unknowns

- Cyber Threats
- Systemic Vulnerabilities
- Reported Events & Incidents
- Healthcare Industry Posture and Response

CSI Cyber, Season 2 Episode 5: Hack E.R.

Cybersecurity Incident - Mortality Rate Impact



Hacked to Pieces?

The Effects of Ransomware Attacks on Hospitals and Patients

August 19, 2024

By Claire McGlave, Hannah Neprash, and Sayeh Nikpay*

As cybercriminals increasingly target healthcare, hospitals face the growing threat of ransomware attacks. Ransomware is a type of malicious software that prevents users from accessing electronic systems and demands a ransom to restore access. In this paper, we create and link a database of hospital ransomware attacks to Medicare claims data. We quantify the effects of ransomware attacks on hospital operations and patient outcomes. Ransomware attacks decrease hospital volume by 17-26% during the initial attack week, with recovery occurring within three weeks. Among patients already admitted when a ransomware attack begins, in-hospital mortality increases by 35-41%.

*McGlave: University of Minnesota (email: mcgl0066@umn.edu); Neprash: University of Minnesota (email: hneprash@umn.edu); Nikpay: University of Minnesota (email: snikpay@umn.edu). We thank Lindsay Allen, Yaa Akosa Antwi, Eric Barette, Mike Chernew, Sung Choi, Nan Clement, Betsy Cliff, Dori Cross, David Cutler, Christian Dameff, Ezra Golberstein, Katherine Hicks-Courant, Peter Huckfeldt, Jared Huling, Rob Huckman, Karen Joynt Maddox, Rebecca Myerson, Amol Navathe, Mike Puskarich, Alan Rozenshtein, Aaron Schwartz, Nicholas Tilipman, Jeff Tully, Beth Virnig, and seminar participants at ASHEcon and the Midwest Health Economics Conference at DePaul University for useful feedback. Research reported in this publication was supported by the NIHCM Foundation. The authors report no conflicts of interest.

University of Minnesota study:

- Ransomware attacks decrease hospital volume by 17-26% during the initial attack week, with recovery occurring within three weeks.
- Among patients already admitted when a ransomware attack begins, in-hospital mortality increases by 35-41%.
- Estimates suggest that ransomware attacks resulted in the deaths of between 68 and 75 Medicare patients over the course of our study period.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292

Cybersecurity Incident – Regional Impact

National Library of Medicine
National Center for Biotechnology Information

Crit Care Explor. 2024 Apr 10;6(4):e1079. doi: 10.1097/CCE.0000000000001079. eCollection 2024 Apr.

Ransomware Cyberattack Associated With Cardiac Arrest Incidence and Outcomes at Untargeted, Adjacent Hospitals

Thaidan T Pham [1], Theoren M Loo [2], Atul Malhotra [3], Christopher A Longhurst [4 5], Diana Hylton [6], Christian Dameff [4 7 8], Jeffrey Tully [6], Gabriel Wardi [3 7], Rebecca E Sell [9], Alex K Pearce [3]

Affiliations + expand

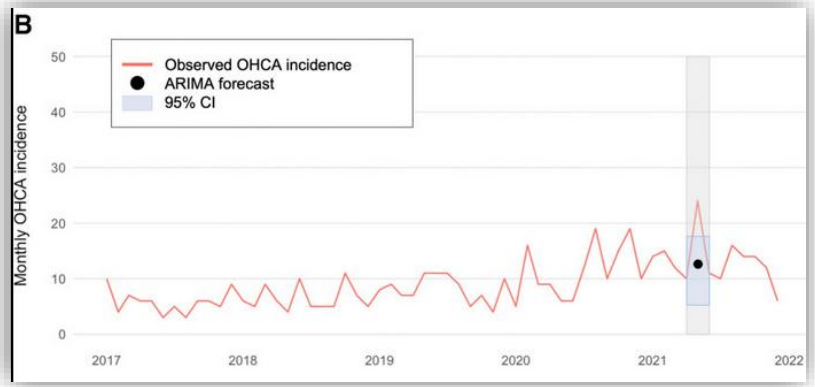
PMID: 38605720 PMCID: PMC11008621 DOI: 10.1097/CCE.0000000000001079

Abstract

Objectives: Healthcare ransomware cyberattacks have been associated with major regional hospital disruptions, but data reporting patient-oriented outcomes in critical conditions such as cardiac arrest (CA) are limited. This study examined the CA incidence and outcomes of untargeted hospitals adjacent to a ransomware-infected healthcare delivery organization (HDO).

Design setting and patients: This cohort study compared the CA incidence and outcomes of two untargeted academic hospitals adjacent to an HDO under a ransomware cyberattack during the pre-attack (April 3-30, 2021), attack (May 1-28, 2021), and post-attack (May 29, 2021-June 25, 2021) phases.

Conclusion: Untargeted hospitals adjacent to ransomware-infected Healthcare Delivery Organizations may see worse outcomes for patients suffering from out-of-hospital Cardiac Arrest (OHCA). These findings highlight the critical need for cybersecurity disaster planning and resiliency.



https://pubmed.ncbi.nlm.nih.gov/38605720/

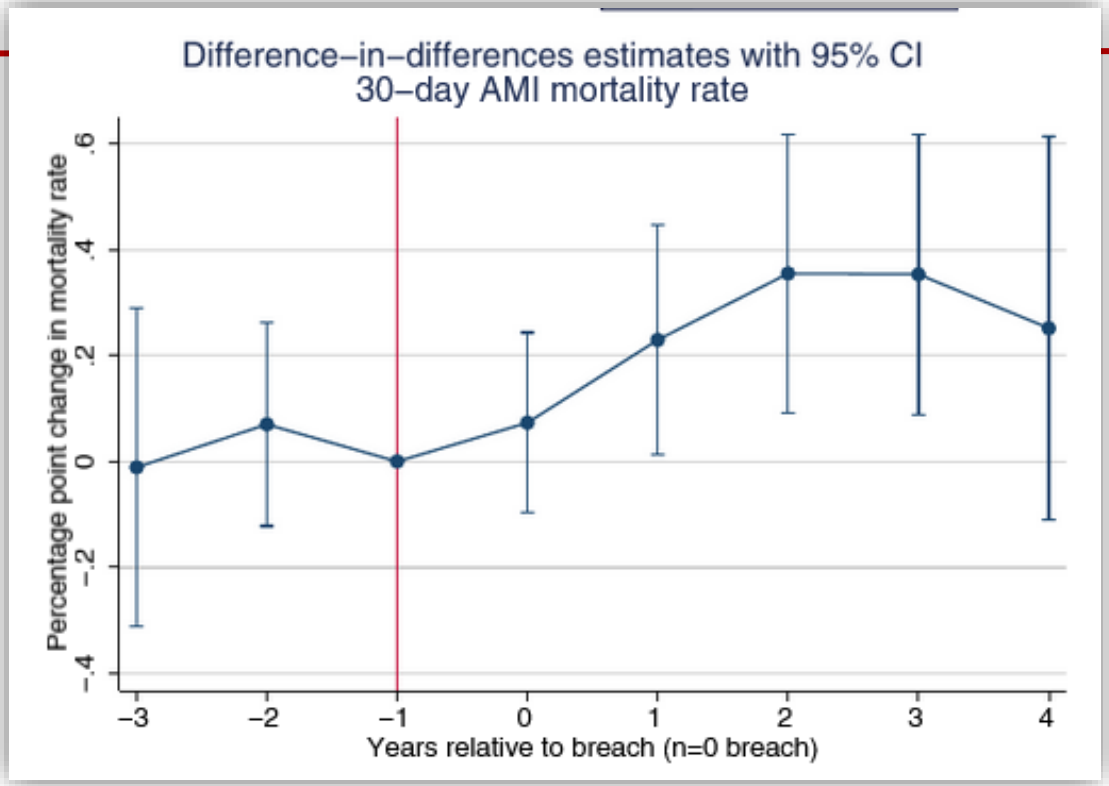
Cybersecurity Incident – Long Term Impact

Findings:

- Hospital time-to-electrocardiogram increased as much as 2.7 minutes.
- 30-day acute myocardial infarction mortality increased as much as 0.36 percentage points during the 3-year window following a breach.

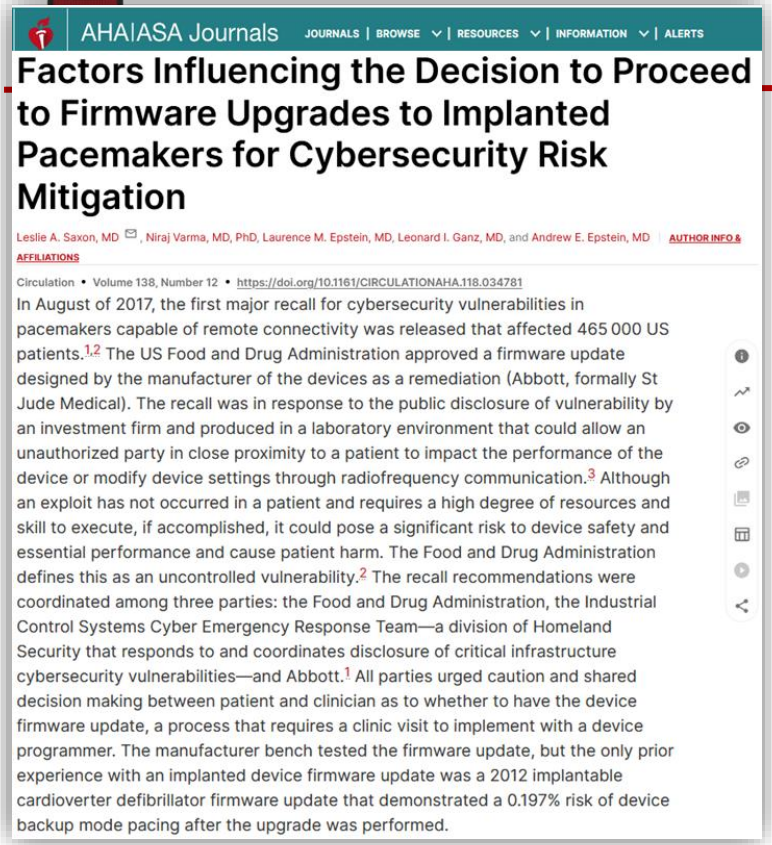
Conclusion:

- Breach remediation efforts were associated with deterioration in timeliness of care and patient outcomes.



Source: Choi, Johnson, Lehman "Data breach remediation efforts and their implications for hospital quality"

To Patch or Not to Patch, that is the Question



AHA|ASA Journals JOURNALS | BROWSE | RESOURCES | INFORMATION | ALERTS

Factors Influencing the Decision to Proceed to Firmware Upgrades to Implanted Pacemakers for Cybersecurity Risk Mitigation

Leslie A. Saxon, MD, Niraj Varma, MD, PhD, Laurence M. Epstein, MD, Leonard I. Ganz, MD, and Andrew E. Epstein, MD AUTHOR INFO & AFFILIATIONS

Circulation • Volume 138, Number 12 • https://doi.org/10.1161/CIRCULATIONAHA.118.034781

In August of 2017, the first major recall for cybersecurity vulnerabilities in pacemakers capable of remote connectivity was released that affected 465 000 US patients.[1,2] The US Food and Drug Administration approved a firmware update designed by the manufacturer of the devices as a remediation (Abbott, formally St Jude Medical). The recall was in response to the public disclosure of vulnerability by an investment firm and produced in a laboratory environment that could allow an unauthorized party in close proximity to a patient to impact the performance of the device or modify device settings through radiofrequency communication.[3] Although an exploit has not occurred in a patient and requires a high degree of resources and skill to execute, if accomplished, it could pose a significant risk to device safety and essential performance and cause patient harm. The Food and Drug Administration defines this as an uncontrolled vulnerability.[2] The recall recommendations were coordinated among three parties: the Food and Drug Administration, the Industrial Control Systems Cyber Emergency Response Team—a division of Homeland Security that responds to and coordinates disclosure of critical infrastructure cybersecurity vulnerabilities—and Abbott.[1] All parties urged caution and shared decision making between patient and clinician as to whether to have the device firmware update, a process that requires a clinic visit to implement with a device programmer. The manufacturer bench tested the firmware update, but the only prior experience with an implanted device firmware update was a 2012 implantable cardioverter defibrillator firmware update that demonstrated a 0.197% risk of device backup mode pacing after the upgrade was performed.

2017 St. Jude Pacemaker Recall:

- First Class 2 recall due to a cybersecurity vulnerability
- Identified by researcher
- Disclosed via investment firm
- ~500,000 affected devices
- FDA “Patients should consult with their Physicians ….”

Expected the failure rates for a firmware update:

- 1 in 620: Incomplete update (~800 patients)
- 1 in 4,300: Loss of programmed settings (~110)
- 1 in 33,000: Complete loss of functionality (~16)

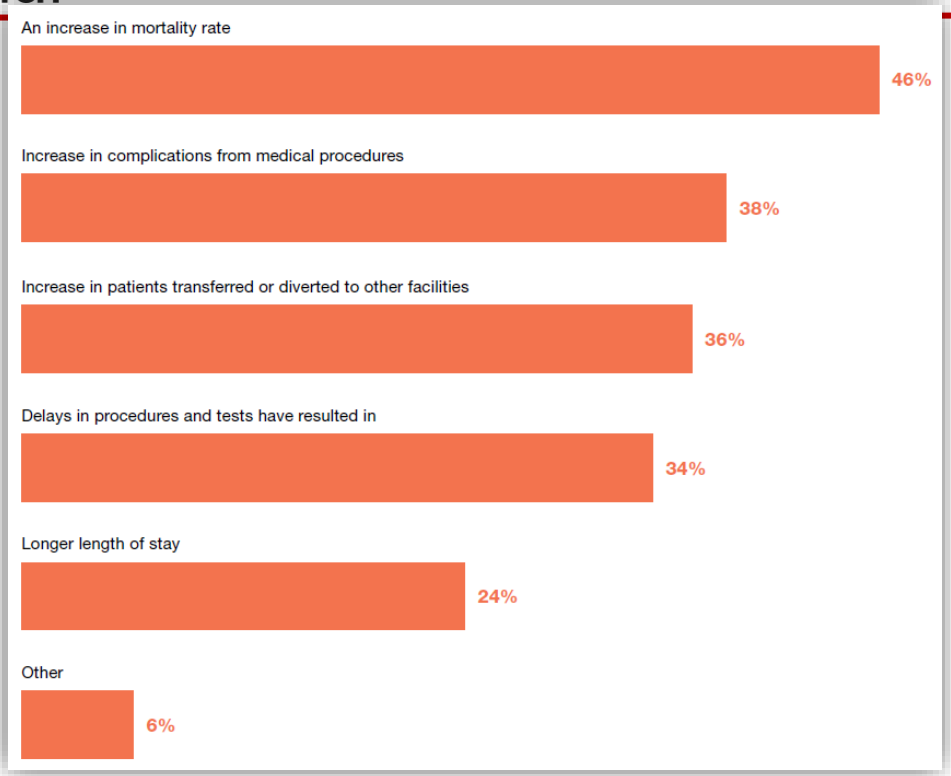
Data indicates* (not scientific sound research and with unknown number of updates):

- 11 pacemaker removal and replacement
- 18 cases of side effects, including hospitalization

https://www.ahajournals.org/doi/10.1161/CIRCULATIONAHA.118.034781?doi=10.1161/CIRCULATIONAHA.118.034781

* https://www.linkedin.com/posts/activity-7396190127842242560-GAia/

Impact of Data Loss or Exfiltration



Note – we still lack systemic and broad studies about the occurrence and impact of security incidents in healthcare.

Although anecdotal reporting and single-institution studies also reported increase in mortality rates, the numbers in this study appear high.

Ponemon Institute Study
Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care

Healthcare Cybersecurity
Knowns and unknowns

- Cyber Threats
- Systemic Vulnerabilities
- Reported Events & Incidents
- Healthcare Industry Posture and Response

Compliance vs. Security

Traditionally, Healthcare has been a Compliance-driven Industry

Compliance
Occasional audit against well defined regulations; failure may result in fines – but you'll live

Today's Security
Any adversary, any type of conflict, unknown attack, any time, anywhere, highly skilled, no rules, any weapon – people die

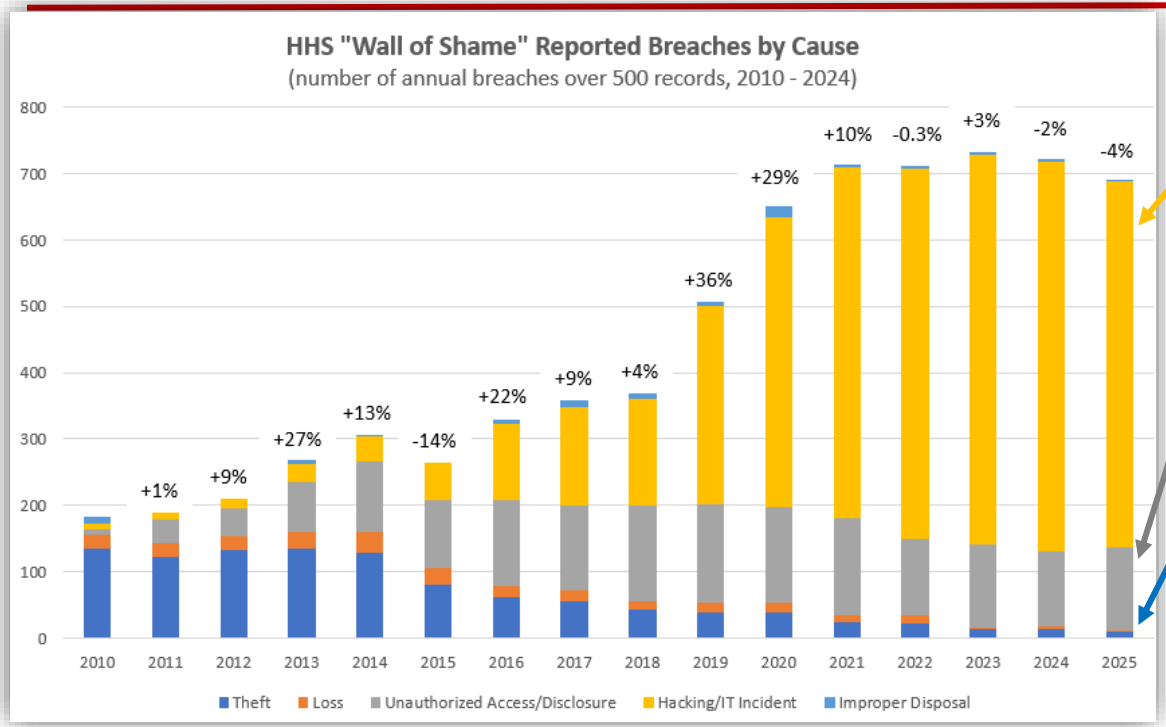
Strict Compliance Controls ≠ Need for Nimble Security

HHS Breach Analysis 2009-2025

- HITECH Act / HIPAA Breach Notification Law:
  - Since Sept. 2009, mandatory reporting of breaches over 500 records to Health and Human Services (HHS)
  - ”Wall of Shame”: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf,
  - Breaches <500 records are to be reported annually but are not published
- Notes and Limitations:
  - Dates are reporting dates and not incident dates
    - Reporting required within 60 days but some report with delay
    - Self-reporting creates some uncertainty across criteria
  - Analysis based on full-year data for 2010 – 2025
    - 2009 excluded from YoY comparison, partial reporting year (Sept-Dec)
  - Does not include non-breach security incidents
    - But ransomware is considered a breach (per HHS interpretation of HIPAA)
  - Data was retrieved Jan. 2025, some additional reports may still be posted

HHS “Wall of Shame” Breach Data Analysis: 2010-2025

Reported Breaches affecting 500 or more Individuals



(removed “Other” and “Unknown” categories that were used until 2014)

Hacking / IT Incident
- 5% → 80% of breach events
- Sole driver of growth since 2015

Unauthorized Access
- Far second
- 18% of breaches

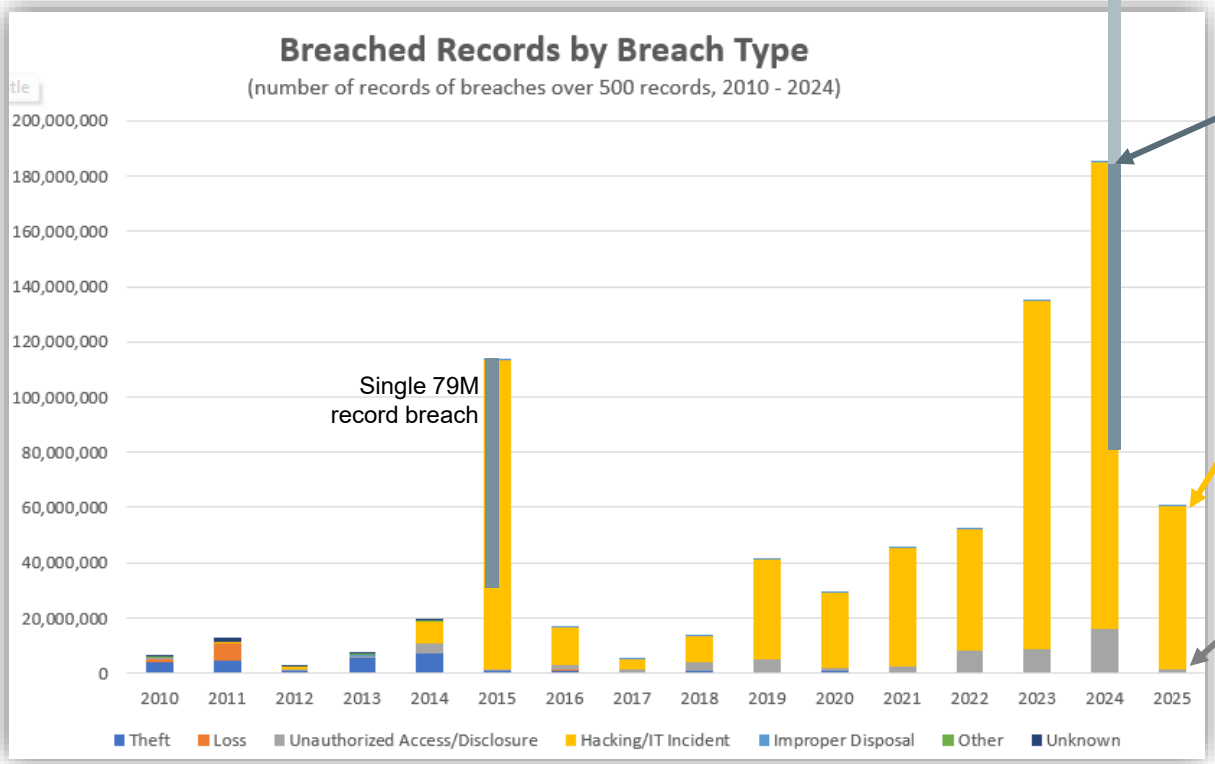
Theft & Loss
- Formerly leading, now negligible
- 75% → 1.6% of breaches

2010 - 2025:
- ~9.3% CAGR
- 7279 reported breaches
- 746 million breached records

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HHS “Wall of Shame” Breach Data Analysis: 2010-2025

Reported Breaches affecting 500 or more Individuals



UnitedHealth / Change Breach

- 100 million reported in 2024
- Later updated to 190 million

Hacking/IT Incident

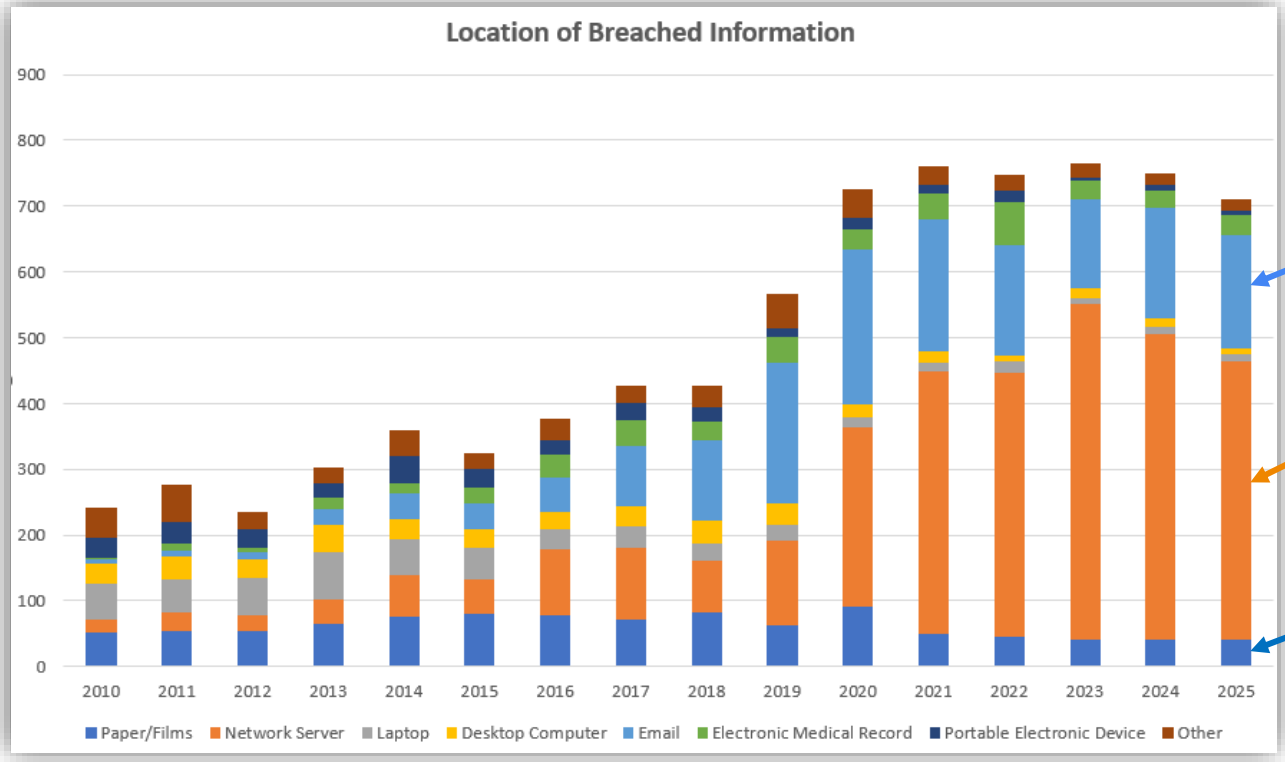
- Far leading cause
- Dominant driver
- Now 98% of breached records

2010-2024: Unauthorized Access

- Far second
- Now 2%

HHS “Wall of Shame” Breach Data Analysis: 2010-2025

Reported Breaches affecting 500 or more Individuals



Email
- Second place
- 2% -> 24% of breaches

Network Server
- Leading category
- 9% -> 59% of breaches

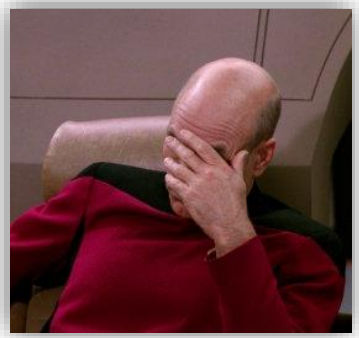
Paper / Films
- Apparently, it’s still a thing
- 21% -> 5.8% of breaches

HHS “Wall of Shame” Breach Data Analysis: 2010-2024

Year	Breaches	Records	1M+	Notes
2009	18	0.13M	0	Partial reporting year
2010	199	5.9M	2	
2011	200	13.2M	4	
2012	218	2.9M	0	
2013	277	7.0M	1	
2014	314	17.5M	4	
2015	270	113.3M	6	Including one 78M breach
2016	329	16.7M	3	
2017	358	5.1M	0	
2018	371	13.9M	3	
2019	506	41.2M	5	
2020	650	29.4M	5	
2021	714	45.7M	10	
2022	712	52.1M	11	
2023	733	134.8M	26	Highest in 1M+ breaches
2024	721	185.0M	13	Including one 100M breach
2025	689	60.3M	9	1M – 14M
Total	**7279**	**746M**	**102**	

2024 - 2025 Trends:

- Breach events ↓
- Breached records ↓
- Large breaches ↓
- Malicious breaches ↑

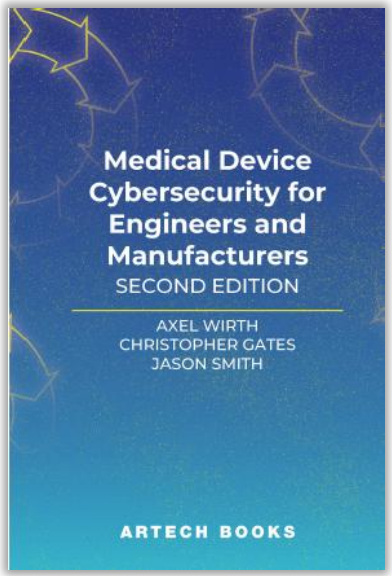


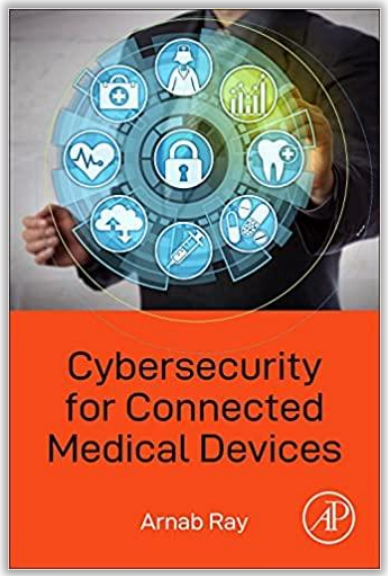
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Thank you!

axel@medcrypt.com

General Resources - For Medical Device Manufacturers

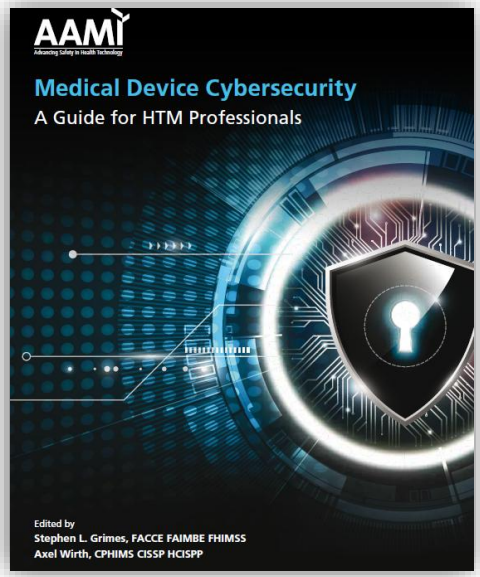




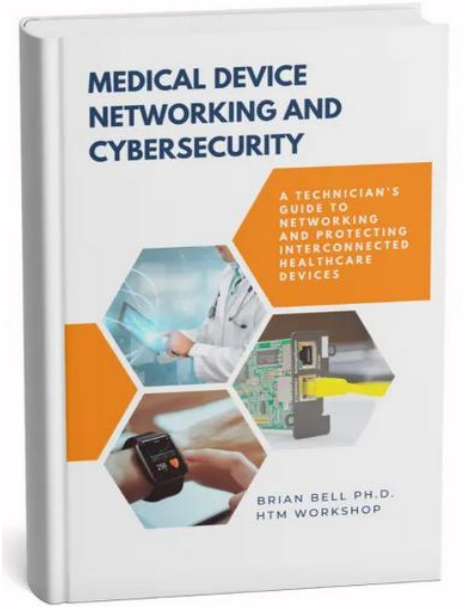
US: https://us.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2416.aspx
UK: https://uk.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2354.aspx

https://www.amazon.com/Cybersecurity-Connected-Medical-Devices-Arnab/dp/0128182628/ref=sr_1_4

General Resources - For Healthcare Delivery Organization

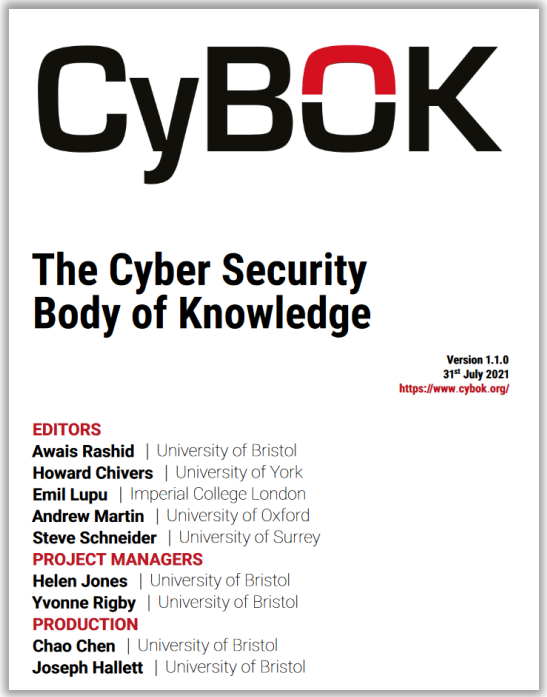


https://store.aami.org/s/store#/store/browse/detail/a152E000006j66qQAA



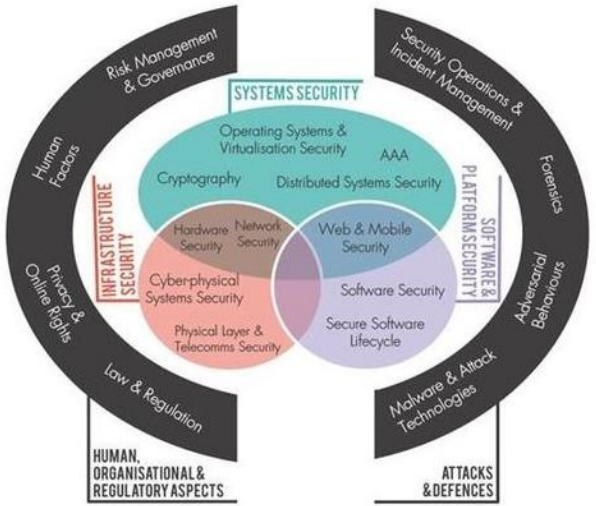
https://htm-workshop.com/shop/medical-device-networking-and-cybersecurity/

General Resources - CyBOK



The Cyber Security Body of Knowledge v1.1,
https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

CyBOK Knowledge Base
https://www.cybok.org/knowledgebase1_1/



Staying Informed on the Day-to-Day

- Security briefs and threat alerts via Health Sector Cybersecurity Coordination Center (HC3) https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- US Department of Homeland Security's Industrial Control Systems—Cyber Emergency Response Team (ICS-CERT) medical device alerts (ICSMA) https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A96
- Healthcare and Public Sector Highlights - Cybersecurity (via HHS) https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare
- CISA HPH Sector https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector