Healthcare Security Breaches in the US: Insights and their Socio-Technical Implications

Megha M Moncy, BDS, MSHI, **Saptarshi Purkayastha,** PhD, **Sadia Afreen,** BTech
Department of BioHealth Informatics
Luddy School of Informatics, Computing and Engineering, Indiana University Indianapolis, IN, USA.

Research Focus

- Examine the critical role of human behavior in healthcare data management.
- Analysis of security breaches in the U.S. healthcare system from 2009 to present
- Acknowledge the presence of technological weaknesses in the healthcare data system.

Methodology

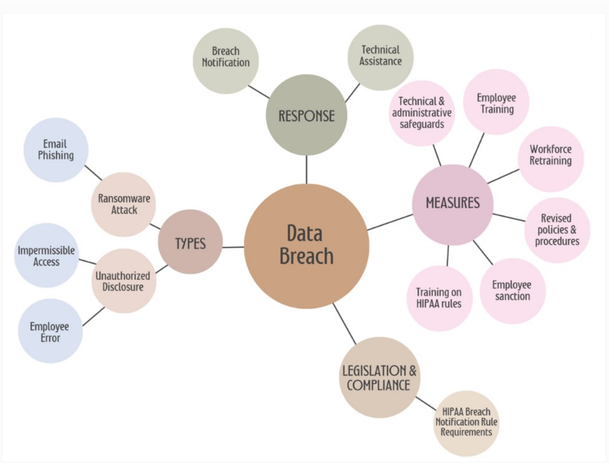
We employed a mixed-methods approach structured in two primary phases:

- *Quantitative analysis of breach notification reports*
- *Qualitative discourse analysis of text descriptions.*

Data composition- Comprises of *4751 rows* and *9 columns [1]*

Qualitative Findings

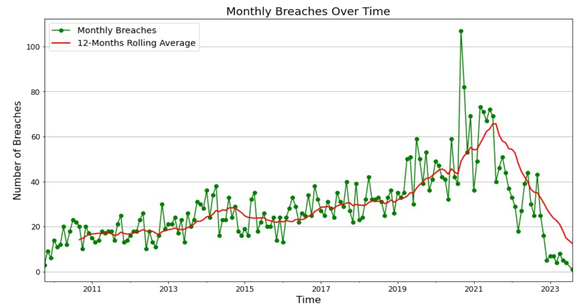
- **Systematic 5-Step Analysis:** Involved familiarization with content, generating initial codes, searching for themes, and defining and naming themes.
- **Content Examination:** Analyzed textual content in 'Web Description' column.
- **Key Themes Identified:**
  - ✓ 'Technical' and 'Administrative safeguards' identified as vital for preventing breaches.
  - ✓ Notable rise in 'ransomware attacks' highlights urgent need for proactive security measures.



Quantitative Findings

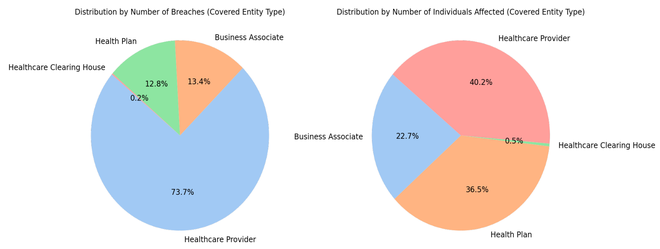
- ***Data breaches over the years:***

Noticeable increase in breaches over the years, peaking in 2021, after which further years data is yet under investigation.



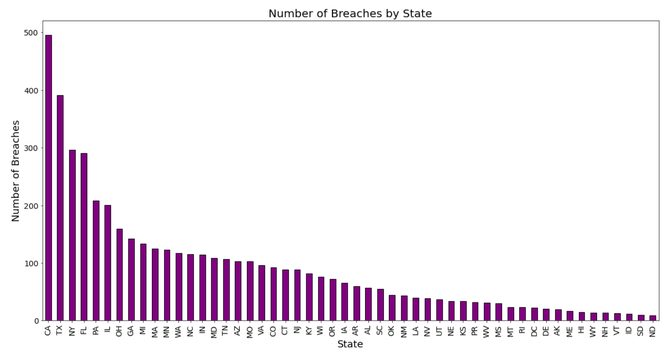
- ***Breach Frequency and Impact Analysis:***

Pie chart reveals healthcare providers as the most breached entities.
Healthcare providers and health plans show substantial impact on people.

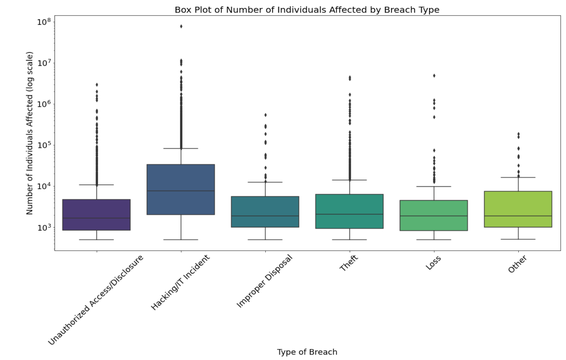


- ***Data breach distribution by State:***

California (CA) and Texas (TX) are the most impacted states, showing high vulnerability.



- ***Impact of data breach types on individuals:***
  - 'Hacking/IT Incident' and 'Other' categories show large variability in impact.
  - 'Unauthorized Access/Disclosure' and 'Hacking/IT Incident' categories include outliers representing breaches with exceptionally high impact.



Results

Human Behavior as a Key Vulnerability:
- Phishing attacks and unauthorized access highlight the significant role of human error in healthcare data breaches.
- Continuous, adaptive training programs are essential to address the vulnerability posed by human behavior.

Socio-Technical Systems in Healthcare:
- Healthcare data systems are socio-technical entities, integrating both technology and human elements.
- Effective breach prevention requires a holistic view, considering both technical flaws and human errors.

Organizational Culture and Security Awareness:
- Breaches involving business associates reveal gaps in organizational culture.
- Cultivating a security-conscious culture across all entities and partners is vital for cybersecurity.

Holistic Approaches to Data Security:
- A comprehensive strategy addressing both technological and socio-technical aspects is crucial for resilience.
- The interconnected nature of breach themes underscores the need for multifaceted cybersecurity solutions.

1 Data Source- **Breach Notification Portal** , frequently termed the **"Wall of Shame."**