Data Breaches Impacting Massachusetts Residents (2024–2025)

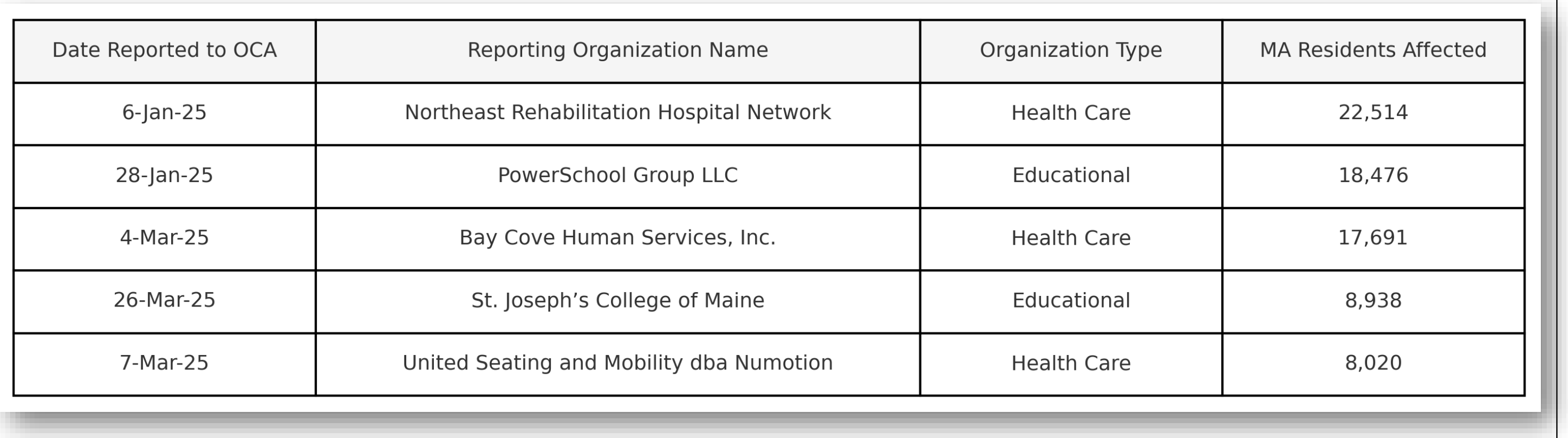
Grace Smalley

Abstract

This project presents a geospatial analysis of data breaches reported across the United States between 2024 and early 2025 that impacted Massachusetts residents. Data was extracted from breach reports published by the Massachusetts Office of Consumer Affairs and filtered for incidents involving healthcare, education, and local government institutions.

Using Python automation and GIS tools, the project geocoded organizational addresses and visualized breach origins nationwide. The resulting map and charts reveal key patterns: Health care organizations reported the most breaches (Figure 4), while SSNs were the most commonly compromised data type (Figure 3). Arkansas and Oklahoma emerged as top contributors to Massachusetts-based exposure (Figure 2). Even a single breach can impact tens of thousands of individuals, as demonstrated by the most detrimental incidents documented in Figure 1. These large-scale exposures underscore the urgency of addressing systemic risks.

This work supports a broader understanding of the spatial dynamics of cyber threats and highlights the urgent need for geographically aware cybersecurity strategies.



Date Reported to OCA	Reporting Organization Name	Organization Type	MA Residents Affected
6-Jan-25	Northeast Rehabilitation Hospital Network	Health Care	22,514
28-Jan-25	PowerSchool Group LLC	Educational	18,476
4-Mar-25	Bay Cove Human Services, Inc.	Health Care	17,691
26-Mar-25	St. Joseph’s College of Maine	Educational	8,938
7-Mar-25	United Seating and Mobility dba Numotion	Health Care	8,020

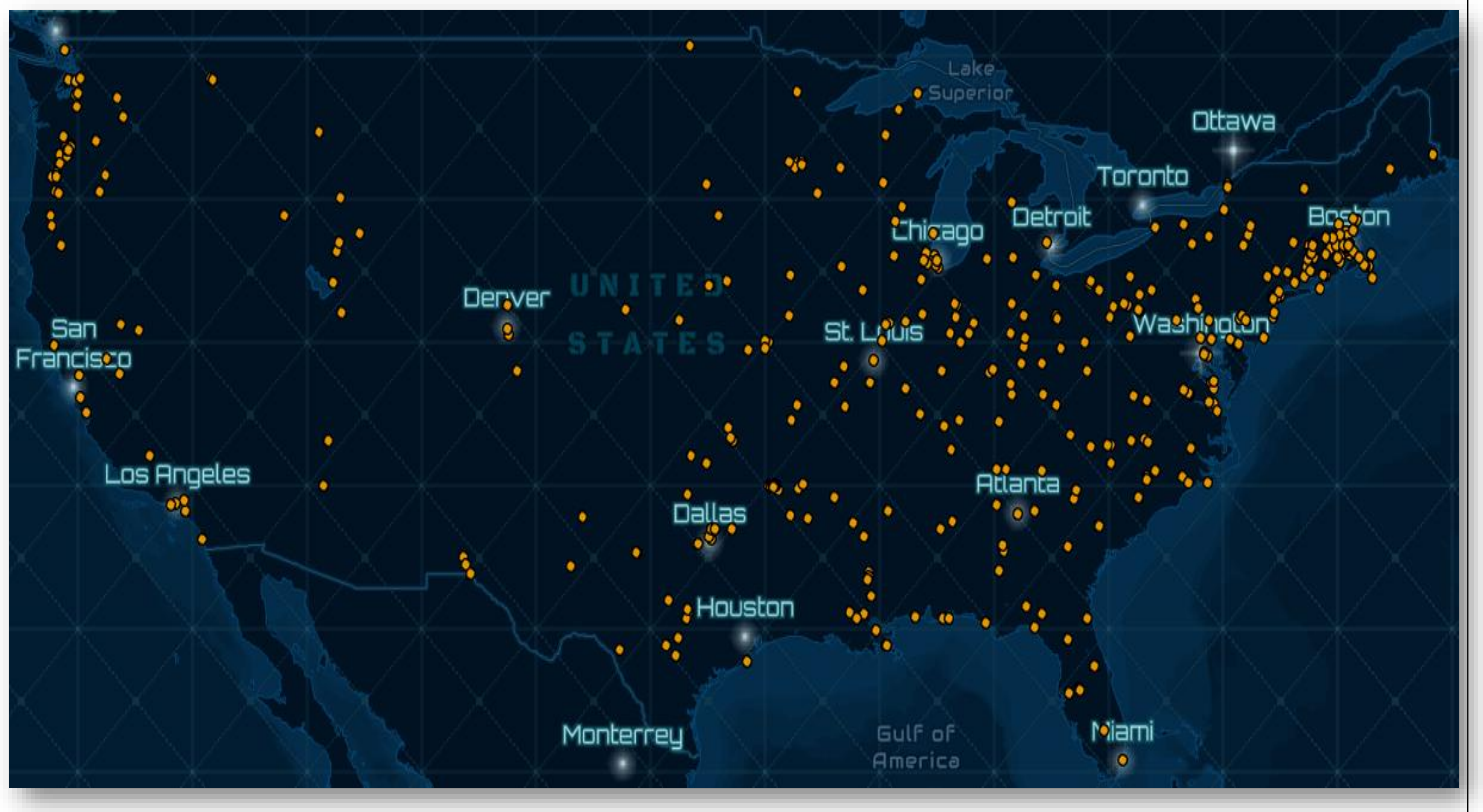
Figure 1: Top 5 Most Detrimental Breaches

The most impactful breaches reported (2024-2025) affected thousands of Massachusetts residents, with healthcare and educational institutions representing the highest exposures.

Process

- Data was extracted from 2024 and 2025 data breach PDF reports published by the MA Office of Consumer Affairs.
- The PDFs were filtered to extract only entries from healthcare, education, and local government sectors. Targeted tables were then converted into Excel sheets for analysis.
- Organization names were geocoded using OpenCage’s API and plotted using the Esri World Geocoder for final location mapping.
- Python was used to automate data cleaning, address processing, and geocoding error handling.
- Summary statistics and spatial comparisons were conducted using ArcGIS analysis tools as well as Python programming.

Results



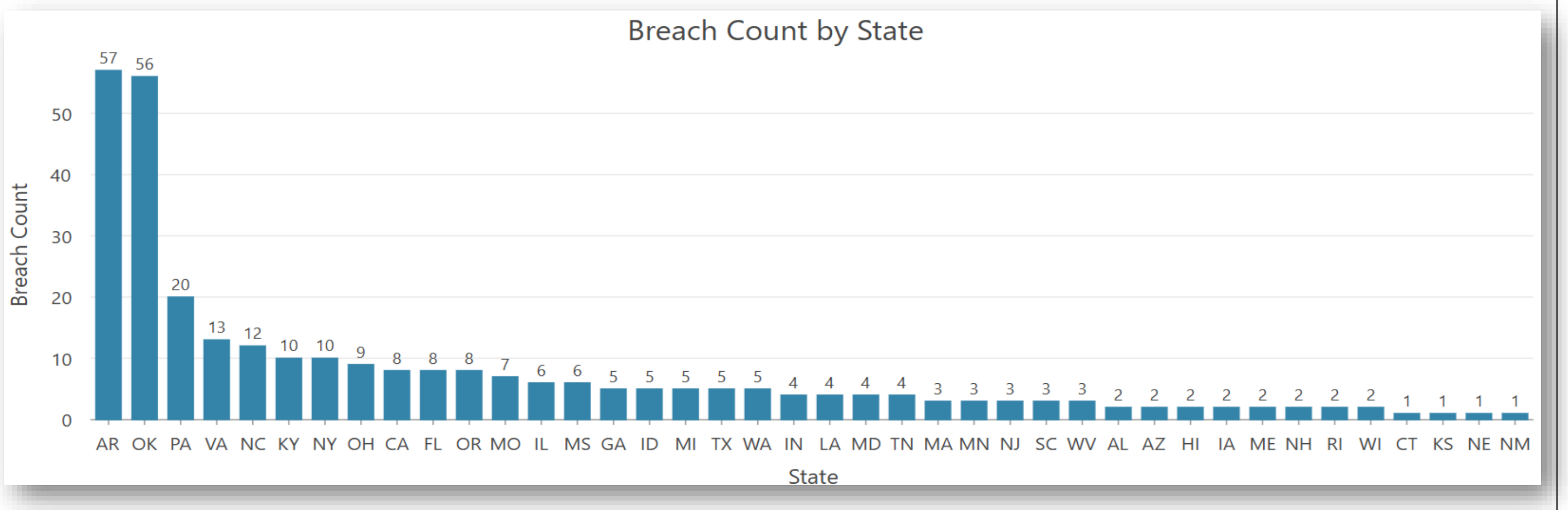


Figure 2: Breach Frequency by State

Arkansas and Oklahoma had the highest number of breaches impacted Massachusetts residents.

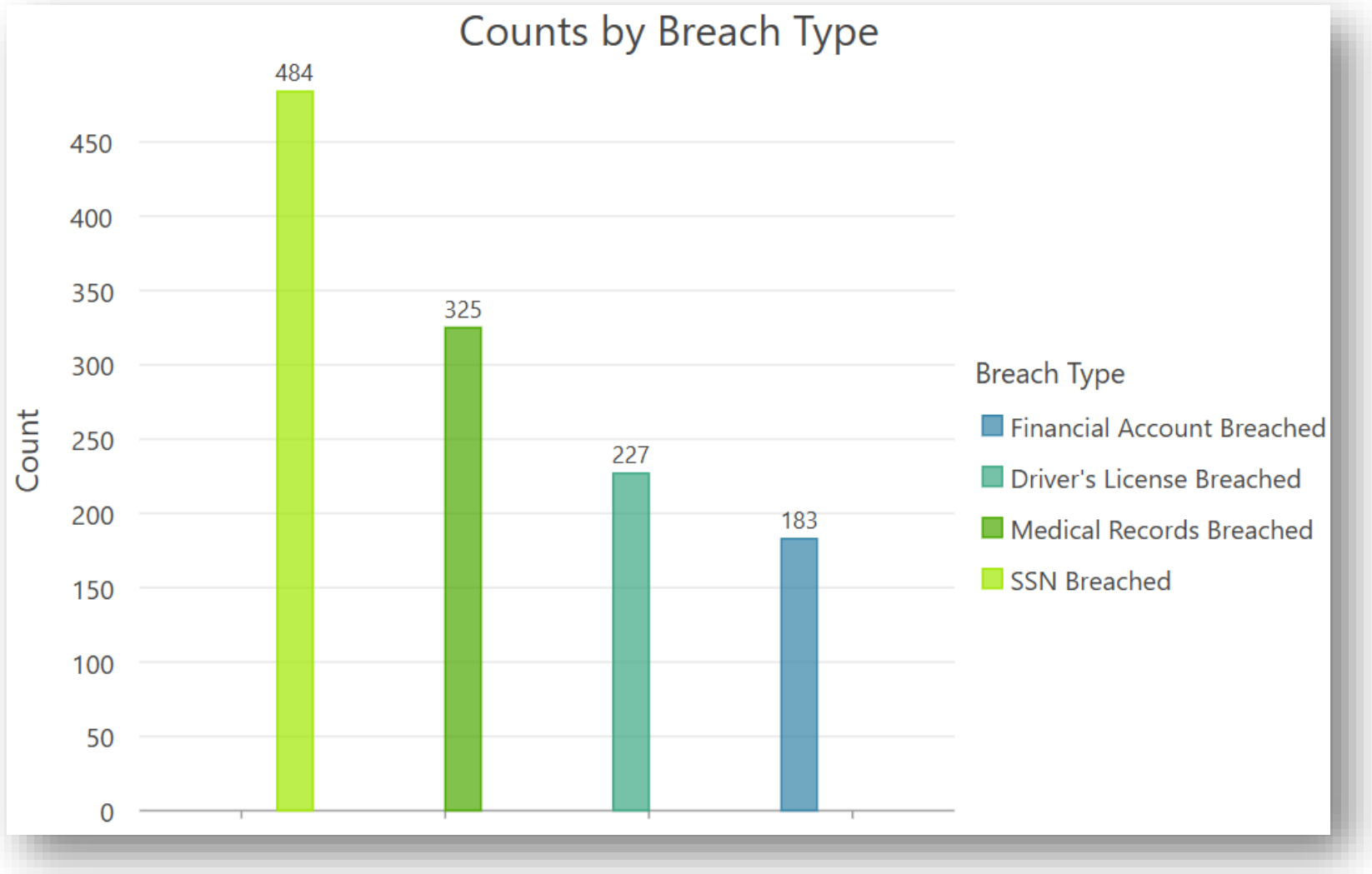


Figure 3: Breach Type Frequency

SSNs were the most frequently breached.

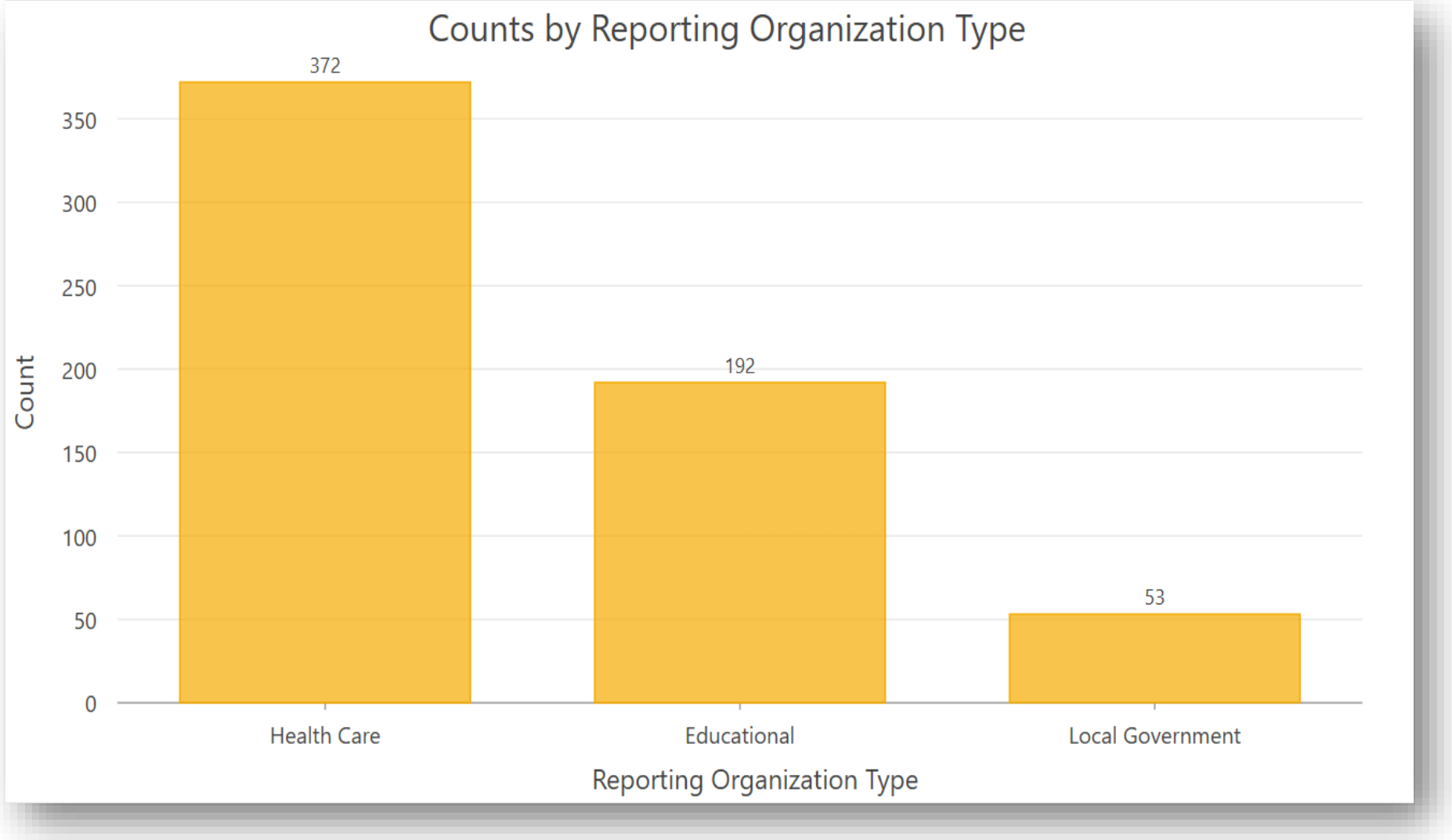


Figure 4: Organization Type Frequency

Health care organizations reported the most breaches.

Significance

The results of this analysis highlight the importance of incorporating spatial awareness into cybersecurity strategy and planning. While breach reports typically present incident data without geographic context, this project reveals that the origins of attacks often span far beyond state borders. States such as Arkansas, Oklahoma, and Pennsylvania (Figure 2) emerged as top sources of data breaches affecting Massachusetts residents, illustrating the distributed nature of digital threats.

Understanding where breaches originate enables a more proactive approach to cybersecurity posture. Geospatial analysis allows policymakers and institutions to identify patterns, prioritize response efforts, and direct resources to regions or sectors most at risk. For example, the high frequency of breaches in health care and education (Figure 4) suggests long-standing structural vulnerabilities that could benefit from targeted investments or revised security protocols.

As data breach volume continues to grow each year (Figure 5), tools like GIS can support broader cyber awareness initiatives and strategic risk modeling. Integrating spatial analysis into cybersecurity planning equips decision-makers with the insight needed to build resilience not just at the organizational level, but across interconnected regions and systems. This approach strengthens the foundation for future policy-making aimed at addressing both immediate threats and long-term digital infrastructure challenges.

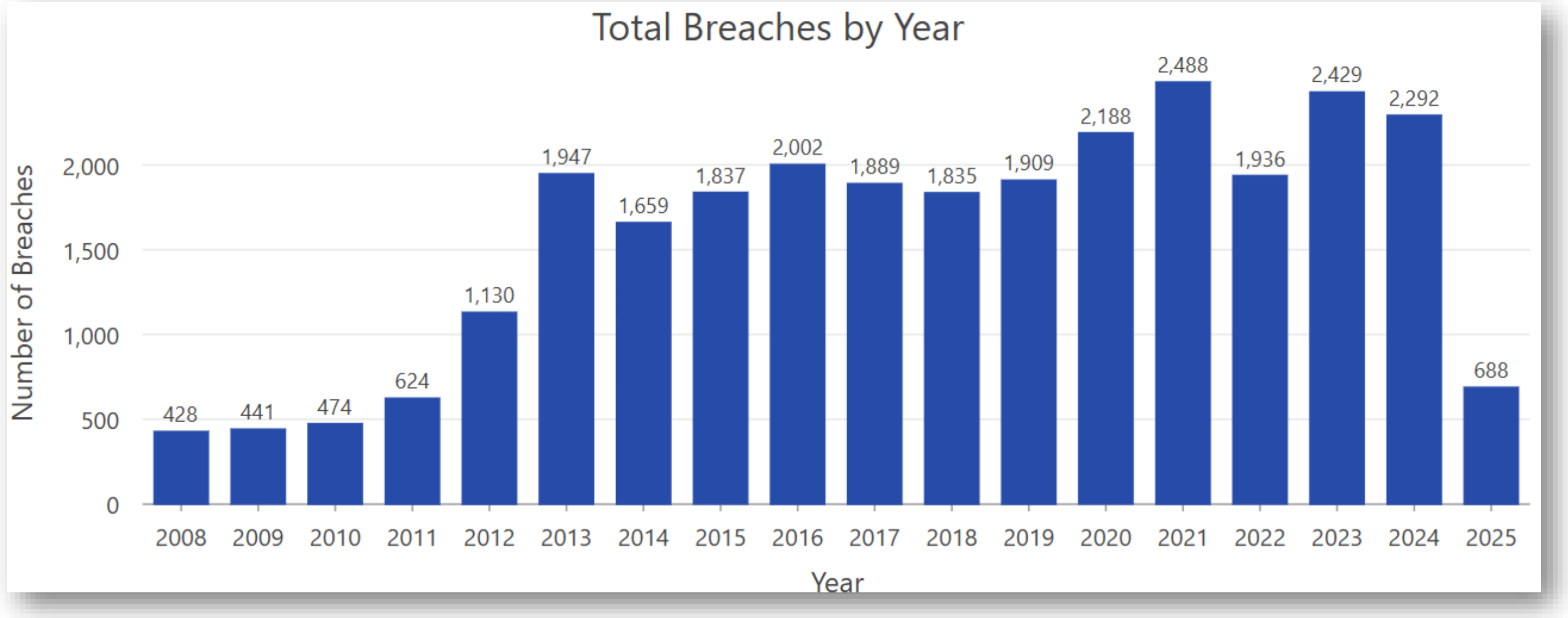


Figure 5: Breach Frequency by Year

The number of breaches impacting Massachusetts residents has steadily risen over the last decade, peaking in 2021. The 2025 count reflects partial-year data as of April.

Acknowledgements & References

This project was made possible thanks to the mentorship of Professor Darcy Boellstorff and the Geography Department at Bridgewater State University. Special thanks to the Massachusetts Office of Consumer Affairs for public breach data access.

1. Massachusetts Office of Consumer Affairs and Business Regulation. (n.d.). *Data breach notification reports*. Mass.gov. https://www.mass.gov/lists/data-breach-notification-reports