Protecting Sensitive Data in Public Services: Tackling Data Silos and Enhancing

Jose Arroyo

California State University, Long Beach

Problem

Public service platforms are responsible for managing vast amounts of sensitive data, ranging from personal identification information to financial and healthcare records. As these platforms increasingly transition to digital systems, the volume and complexity of the data they handle continue to grow. This wealth of information makes them attractive targets for cybercriminals looking to exploit vulnerabilities. Breaches in public service platforms not only compromise individual privacy but can also disrupt essential services, undermine public trust, and result in significant financial and legal consequences for governments. As a result, the protection of this sensitive data has become a critical priority for safeguarding both citizens and the integrity of public services.

Analysis

From January to November 2023, California faced numerous data breaches, continuing its pattern of freFrom January to November 2023, The United State faced numerous data breaches, continuing its pattern of frequent cybersecurity incidents. These breaches affected various government agencies and healthcare organizations. California consistently ranks as one of the top states with the highest number of data breaches, attributed in part to the vast amount of personal information collected by state and local agencies.

The California Department of Justice regularly reports breaches affecting more than 500 residents, and 2023 saw several such events. High-profile cases included breaches in healthcare, where sensitive patient data, including social security numbers and medical records, were exposed. The Kaiser Foundation Health Plan and other organizations reported significant breaches, underscoring the vulnerability of public services in handling large volumes of personal data

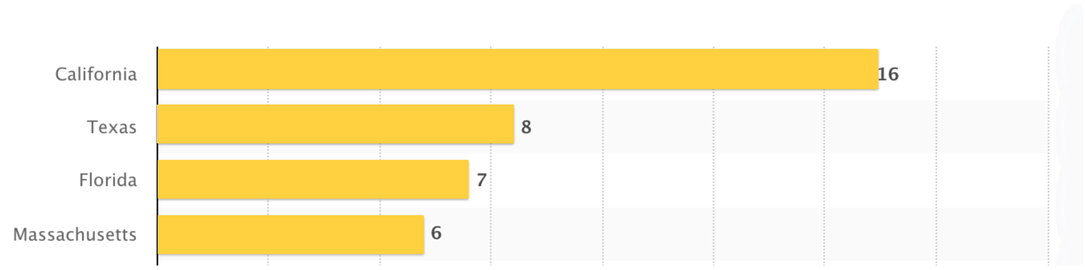

Figure 1: Number of data breach incidents affecting U.S. government organizations from January 2023 to November 2023, by state

These incidents highlight the pressing need for improved security measures, such as encryption and multi-factor authentication, to protect sensitive information from unauthorized access. Furthermore, the state's Attorney General has consistently urged institutions to take proactive steps to safeguard their data and mitigate potential cyberattacks

As cyber threats continue to evolve, California agencies must prioritize bolstering their cybersecurity infrastructure to prevent further incidents.

Challenges

One major challenge for governments is the prevalence of data silos. Data silos occur when departments or agencies store data separately, creating isolated systems that do not communicate with each other. This fragmentation makes it difficult for different parts of the government to share critical information, leading to inefficiencies and vulnerabilities. Legacy IT systems, which many government agencies still rely on, further exacerbate this problem as they are often incompatible with modern technologies. Additionally, strict privacy regulations can limit data sharing between departments, contributing to these silos. When a data breach occurs, these silos make it harder to detect, assess, and contain the damage, as agencies struggle to gain a complete picture of the breach's scope.

Recommendations

To address these challenges, governments should prioritize centralized data management and the adoption of cloud-based solutions. By centralizing data, different departments can more easily share information and monitor data activity, improving overall cybersecurity. Implementing standardized security protocols across all government agencies will ensure that all departments, regardless of their individual systems, maintain strong and consistent protections. Additionally, governments should invest in modernizing their IT infrastructure and consider adopting secure cloud platforms, which provide stronger encryption and access controls while reducing data fragmentation. Data governance policies that encourage cross-departmental collaboration and ensure data is managed responsibly can also help mitigate the risks posed by data silos.

Sources

Published by Ani Petrosyan, & 13, M. (2024, March 13). *U.S. government data breaches by State 2023*. Statista. https://www.statista.com/statistics/1455591/us-gov-data-breaches-by-state/

Uberoi, A. (n.d.). Recent cyber attacks, data breaches & ransomware attacks January 2023. 9ine. https://www.cm-alliance.com/cybersecurity-blog/recent-cyber-attacks-data-breaches-ransomware-attacks-january-2023#DataBreach