How Effective is Zero Trust in Securing Databases

By: Tyra Baxter, Marcus Davis, Reginald Williams

Introduction

Zero Trust is a modern cybersecurity approach built on the principle of “never trust, always verify”, requiring strict identity checks and least-privilege access. We want to evaluate how effective is Zero Trust Framework. We focused on data breaches that occurred between 2014 and 2025

Research Questions

1. Which states has the most breach activity?
2. What are the most common type of data breach events?
3. What are the most common motives of security breaches in the U.S?
4. What are the most attacked industries in the U.S?
5. What is the difference in breach frequency before and after zero trust was implemented?

Dataset Ingestion

year	month	actor_type	industry	motive	event_type	country	state
2014	01	Criminal	Educational Services	Undetermined	Exploitive	United States of America	Florida
2014	01	Criminal	Professional, Scientific, and Technical Services	Undetermined	Exploitive	United States of America	Texas
2014	01	Hacktivist	Professional, Scientific, and Technical Services	Protest	Disruptive	United States of America	Washington
2014	01	Criminal	Information	Undetermined	Exploitive	United States of America	California
2014	01	Undetermined	Information	Undetermined	Disruptive	United States of America	California
2014	01	Undetermined	Information	Undetermined	Disruptive	United States of America	Undetermined
2014	01	Undetermined	Information	Undetermined	Disruptive	United States of America	Washington
2014	01	Undetermined	Information	Undetermined	Disruptive	United States of America	California
2014	01	Undetermined	Information	Undetermined	Disruptive	United States of America	California
2014	01	Undetermined	Information	Undetermined	Disruptive	United States of America	California
2014	01	Criminal	Information	Undetermined	Disruptive	United States of America	Washington
2014	01	Undetermined	Information	Undetermined	Disruptive	United States of America	Undetermined
2014	01	Criminal	Information	Financial	Exploitive	United States of America	California
2014	01	Criminal	Information	Undetermined	Exploitive	United States of America	Illinois
2014	01	Hacktivist	Educational Services	Protest	Disruptive	United States of America	Massachusetts
2014	01	Criminal	Retail Trade	Financial	Exploitive	United States of America	Undetermined
2014	01	Hacktivist	Information	Protest	Disruptive	United States of America	Washington
2014	01	Hacktivist	Information	Undetermined	Disruptive	United States of America	Washington
2014	01	Hacktivist	Information	Undetermined	Disruptive	United States of America	Washington
2014	01	Criminal	Administrative and Support and Waste Management and Remediation Services	Undetermined	Exploitive	United States of America	Washington
2014	01	Criminal	Manufacturing	Financial	Exploitive	United States of America	Ohio
2014	01	Criminal	Other Services (except Public Administration)	Undetermined	Exploitive	United States of America	Undetermined
2014	01	Hacktivist	Public Administration	Protest	Exploitive	United States of America	Undetermined
2014	01	Hacktivist	Public Administration	Protest	Disruptive	United States of America	California
2014	01	Criminal	Public Administration	Undetermined	Exploitive	United States of America	Undetermined

Full Name: Cyber Events Database

Collection Organization: Center for Internal & Security Studies at Maryland

Data Wrangling

Country:USA

Originals Instances: 14,651 Breaches

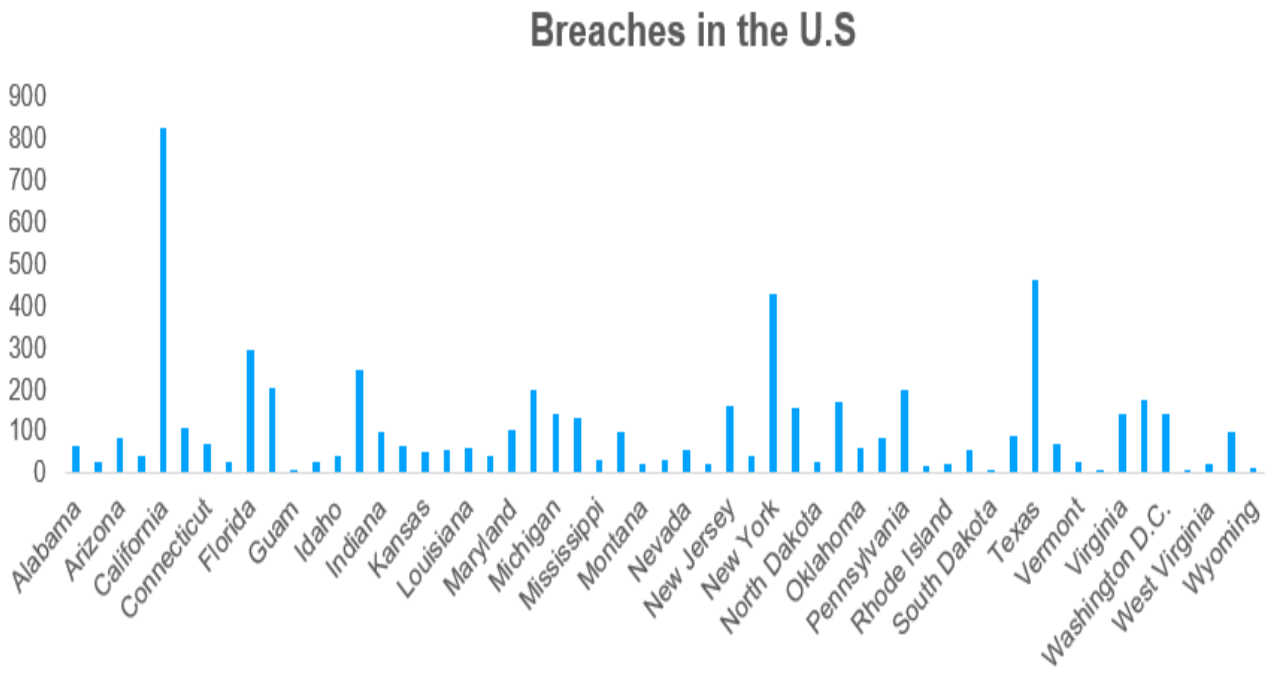
Final Instance: 7,142 Breaches

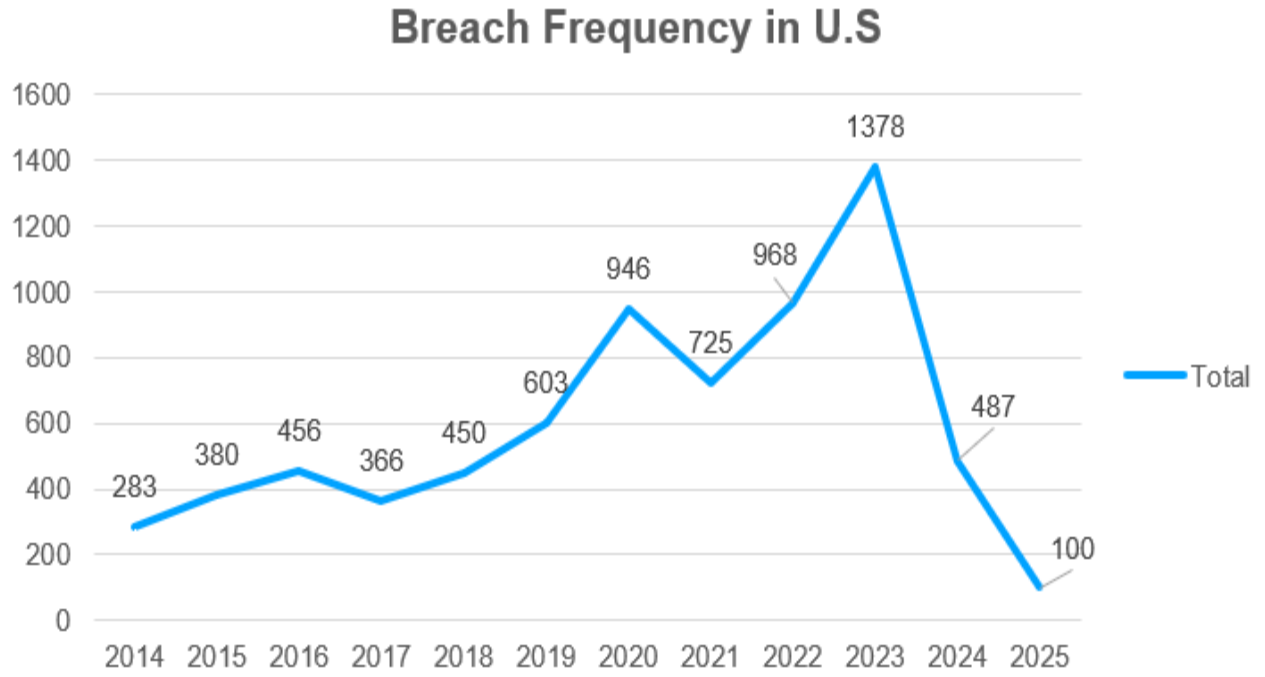
Years: 2014-2025

Original Features:36 Categories

Final Features:8 Categories

EDA

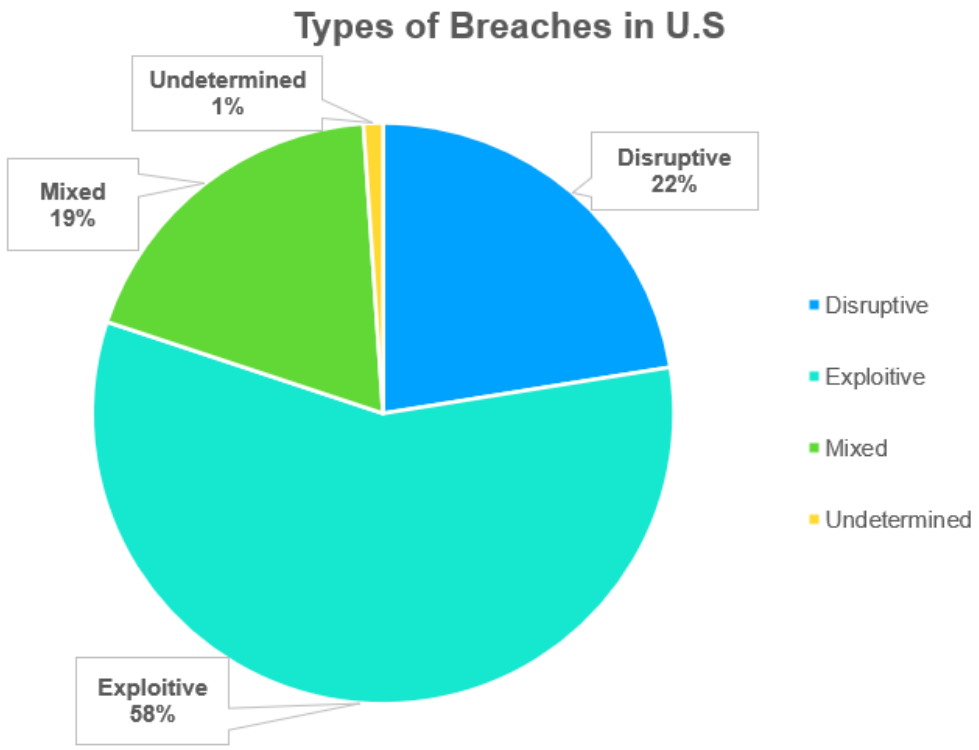




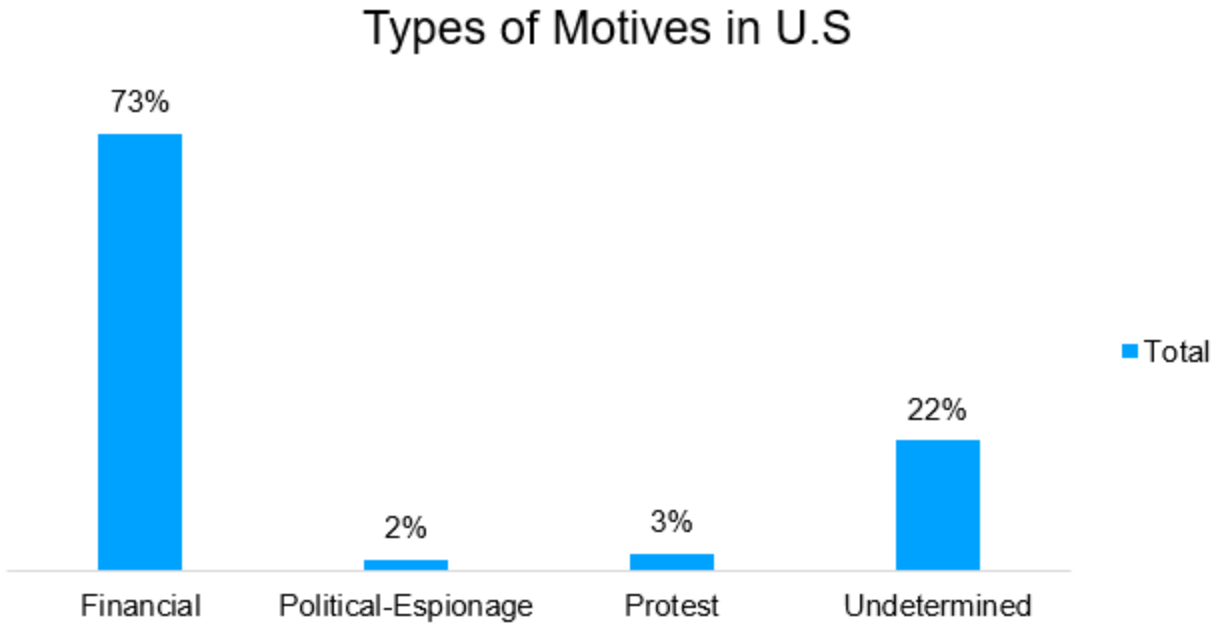
The states that experienced the most breaches are California (14%) , Texas (8%), and New York (7%)

Between 2014- 2015 there where noticeable spikes in 2020 (13%) and again in 2022-2023 (19%). Then followed by drops in 2021 (10%) and once again in 2024-2025(7%)

EDA

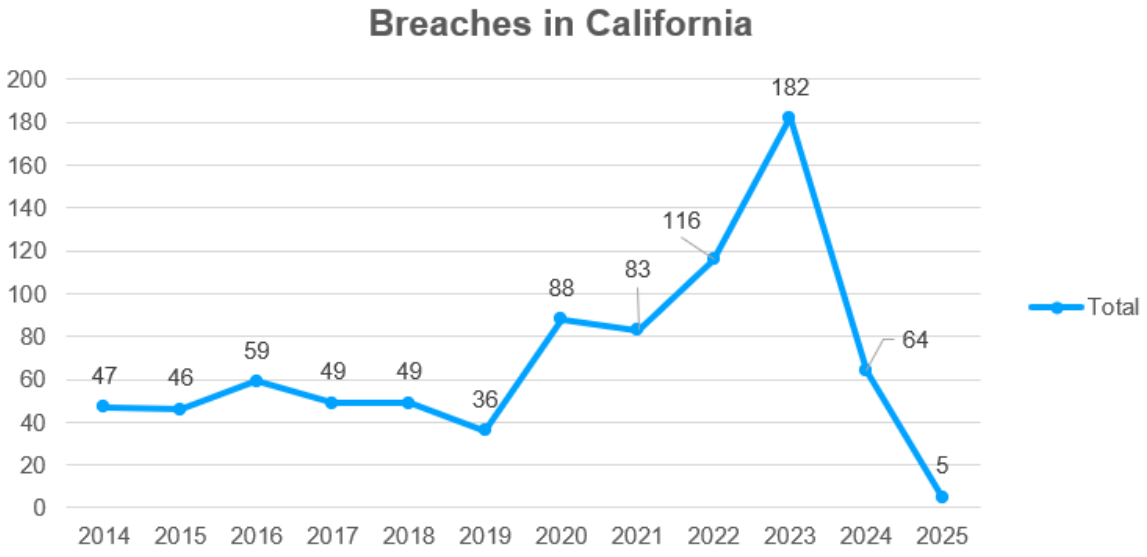


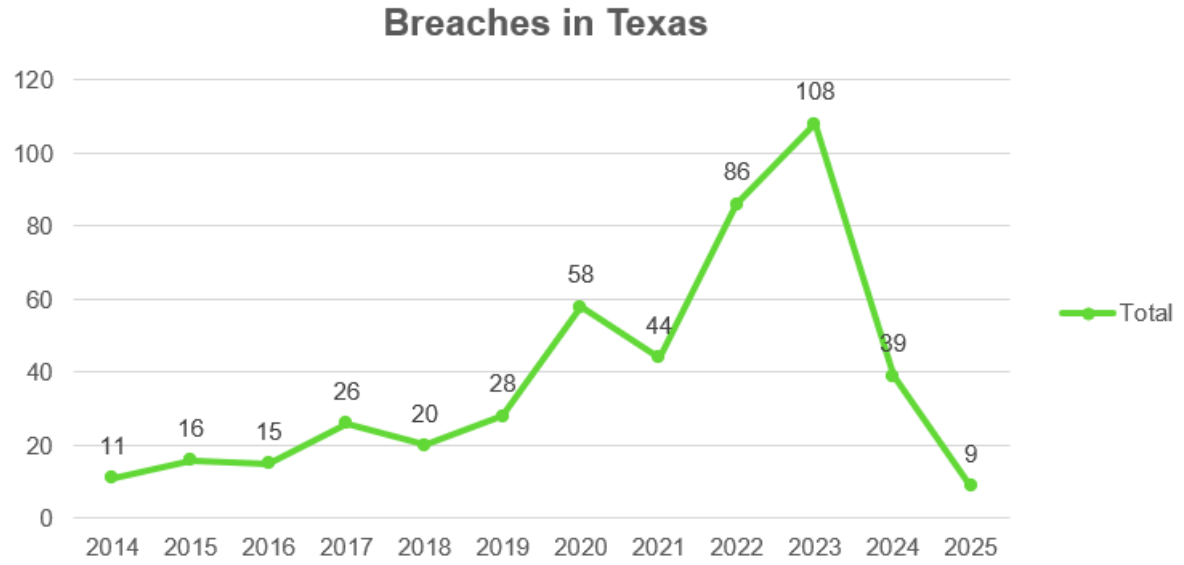
A majority of breaches were exploitive (58%), meaning threat actors gain access to confidential data.

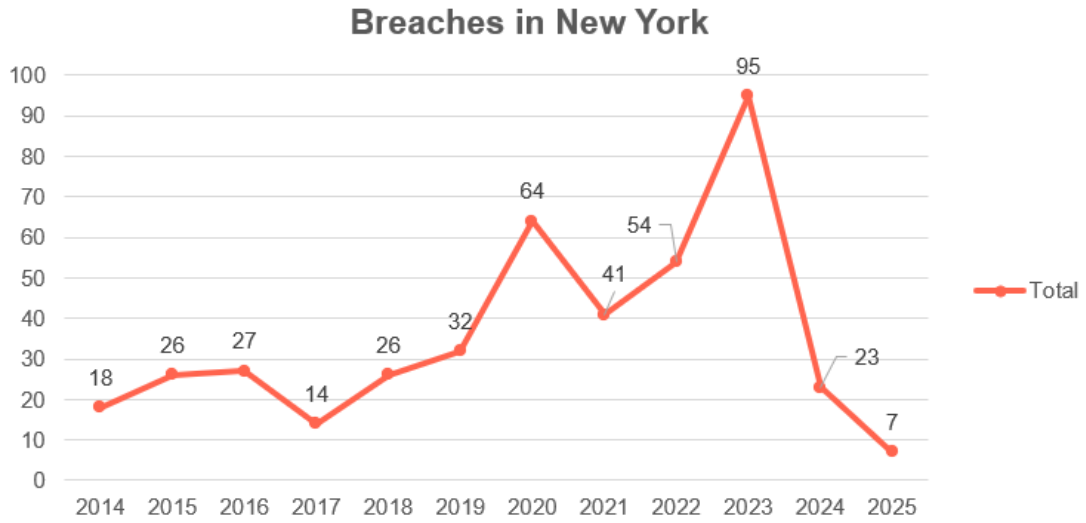


Motives behind most breaches in the U.S are financial, 73% fall under this categories.

EDA

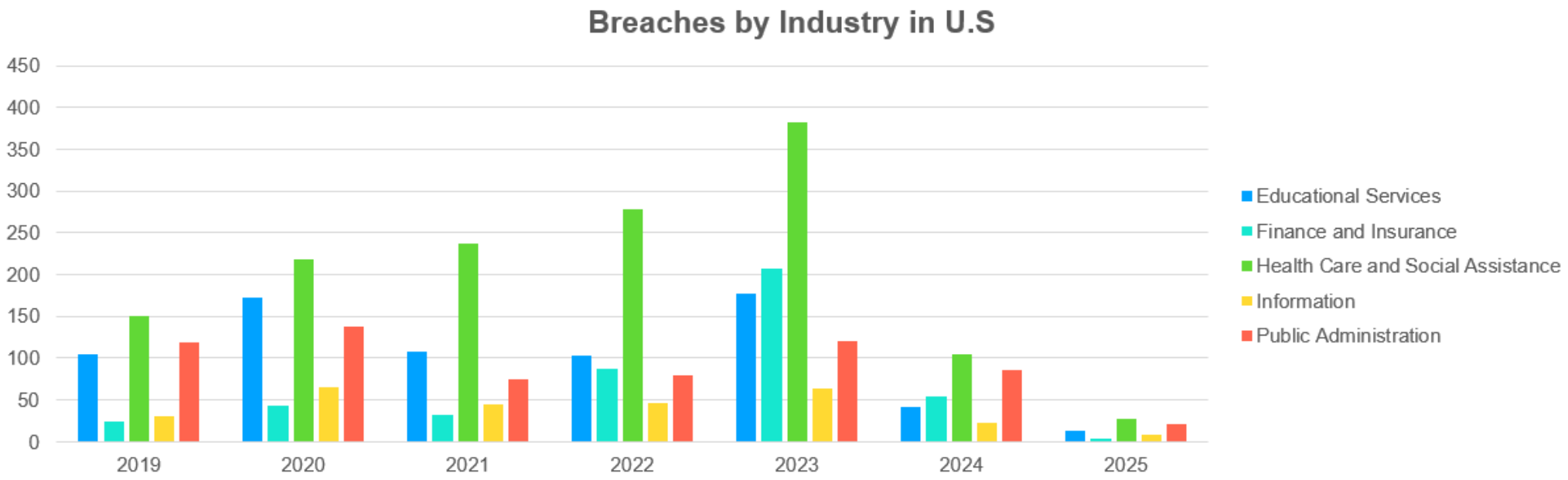






In all the top 3 states, they follow the same pattern of data breach spikes in 2020. Then dropped slightly or staying consistent through 2021-2022. Also, all states saw a hugged spike breaches during 2023 and a drastic decline in 2024.

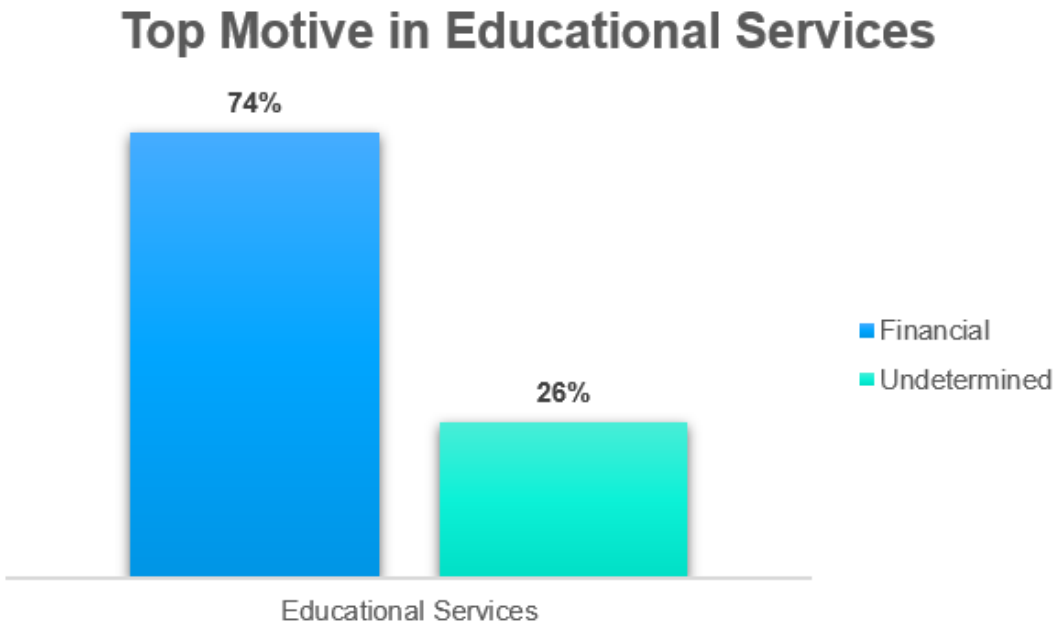
EDA



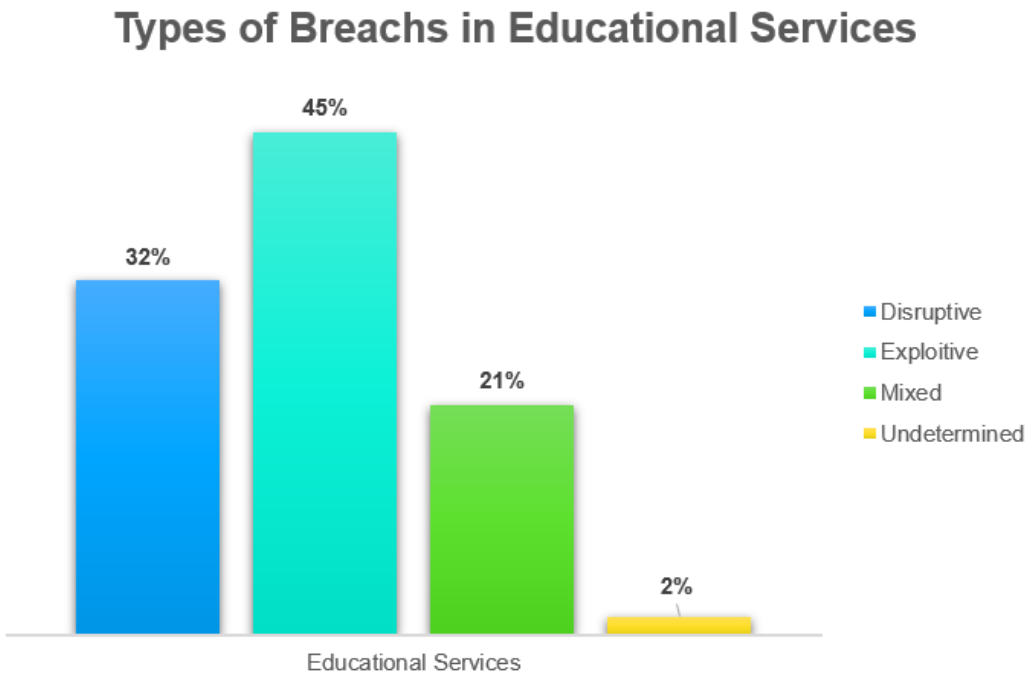
Top 5 Industries

1. **Heath Care and Social Assistance- 40%**
2. **Educational Services- 20%**
3. **Public Administration- 18%**
4. **Finance and Insurance- 12%**
5. **Information-8%**

EDA (Education Services)

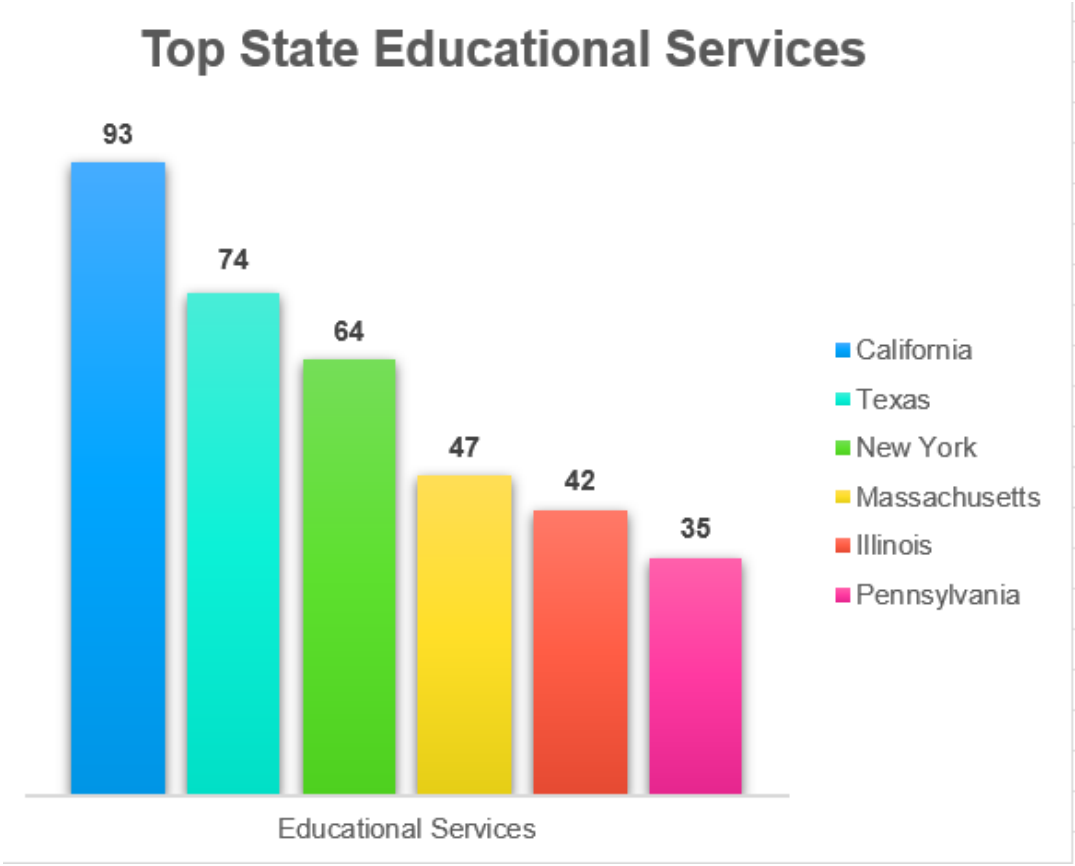


The motive behind majority of Educational Service breaches are financial (74%).



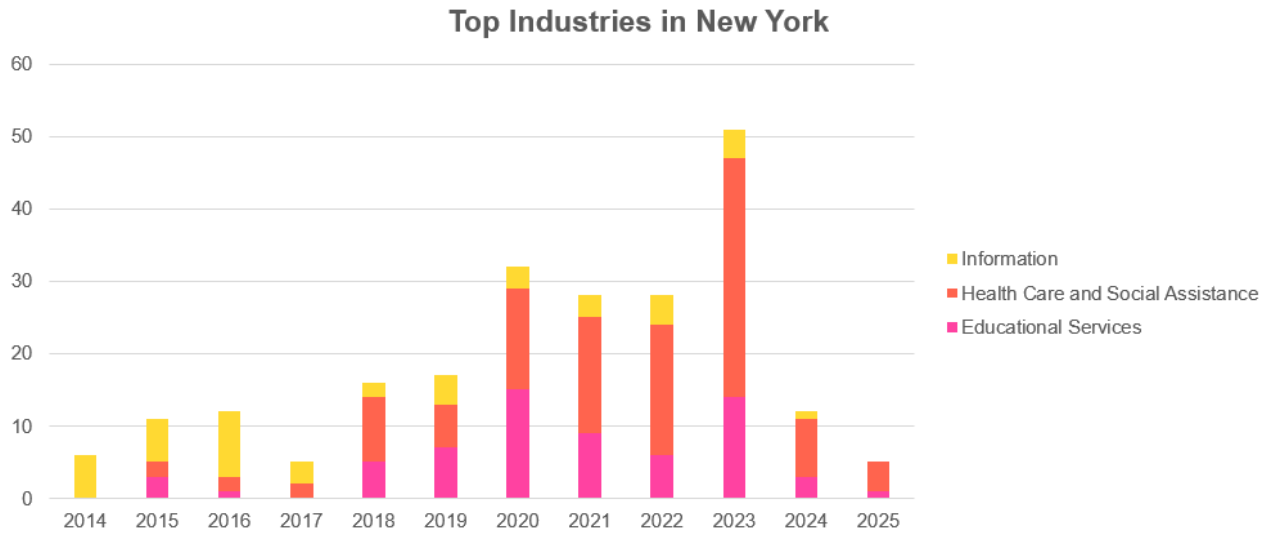
Majority of breaches in Educational Services are exploitive (45%). But 32% of breaches are disruptive which is higher than the overall average. Meaning that this industries face data theft but also significant operational disruption

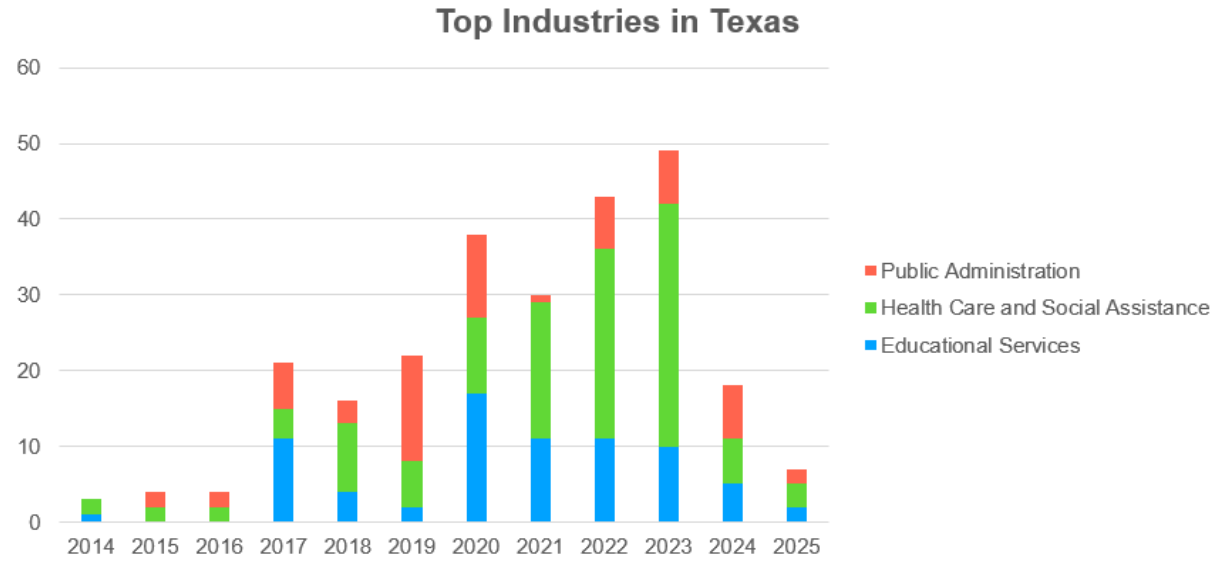
EDA (Educational Services)

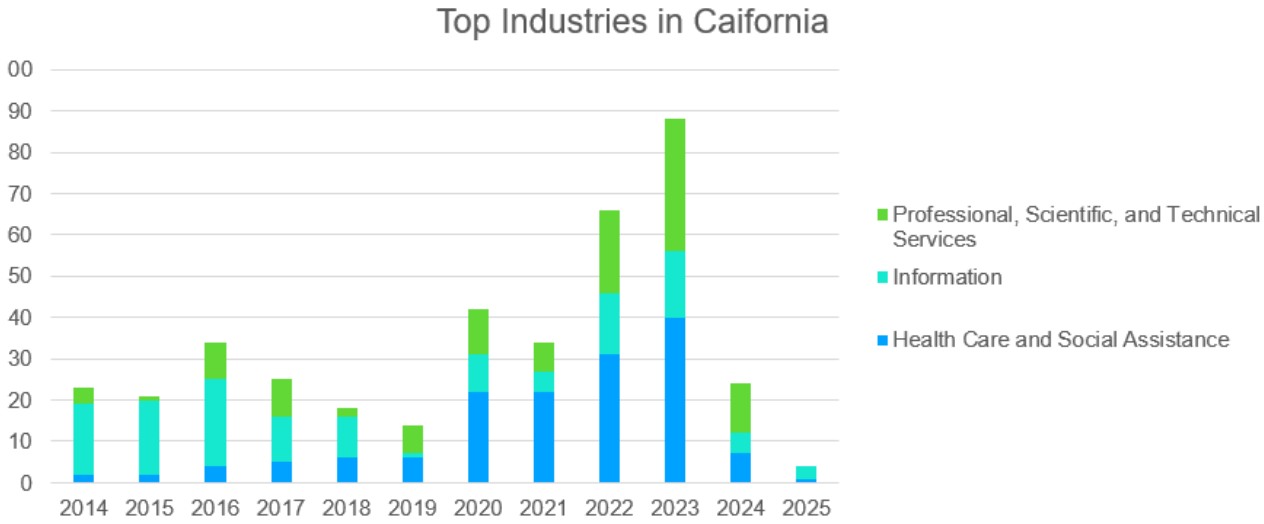


The top states that breaches happened in educational services are California, Texas, and New York. Meaning these states are hot spots for breaches that affect Educational Services

EDA







In New York, Texas, and California the leading industries who face breaches are Heath Care, Educational Services, and Information

Insights

1. The shifts in breach frequency suggest that early deployment had mixed result. But once Zero Trust has been fully implemented breach incidents can be reduced

2. Healthcare, Educational Services, and Public Administration are frequently attacked by threat actors.

3. The motive behind majority of breaches are for financial gain.

Challenges & Future Work

1. Dataset was primarily qualitative so we not able to use descriptive statistics tools
2. There is not a feature that counts each data breach so we were not able to create maps to showcase breaches
3. Limited time to explore the different industries like public administration.

Sources

1. Cyber Events Database Home | Center for International and Security Studies at Maryland
2. Cyber Events Database | Center for International and Security Studies at Maryland