**Data Breach Affecting Washington State Residents**

**Research Design**

**Introduction**

Over the past 25 years the internet created new ways of doing business which has brought increase in data across various applications. Digital Marketing has been a main driver to increase the rate of consumer data collection. These initiatives have generated significant online activities and transactions between consumers and businesses. Consumers are actively participating on social media, health care portals to schedule online doctors’ appointments, requesting direct and indirect loans to meet their financial needs. The current economic environment and the usage of IoT internet of things has raised concerns as the shared data becomes accessible to other devices and companies that represent a risk for potential data breaches. Private information stored in company data bases is vulnerable to hackers. (Markos et al., 2023).

We are now part of the big data era as the numbers continue to increase exponentially creating an alarming rate. The growth of data is now moving from terabytes to petabytes. (Horner, 2020). implemented the concept of the V’s which is directly associated with big data. The terms are known for Volume, Velocity and Variety. There is a fourth V which is veracity. These data breaches can come from inside the companies. Employee might be tempted by financial rewarded by selling data on the dark web or feel resentment toward the company for different purposes. Other employees may just commit a mistake that can result on data breach, such as including the wrong person by sending an email, attaching the incorrect email or losing a laptop.(Dominik Molitor, Wullianallur Raghupathi, Aditya Saharia and Viju Rahgupathi., n.d.)

The purpose of our research is threefold and explores the following:

1. The number of residents in Washington State impacted by the Data Breach. 2- Days to identify the breach 3- Days elapsed before notification. To achieve this, we utilize the datasets regarding data breach from 2015 to present published in the Washington state portal on September 2024. (data.wa.gov) This data was provided by the Washington State Attorney General’s Office Protection Division.

**Literature Review**

The development and widespread use of network technologies has created critical security problems. Various attempts have been made to provide a cyber security environment to protect assets, of the different institutions, organizations and individuals. (El Amin et al., 2024). In today’s digital transformation world, privacy has converted into a fundamental human right into a multifaceted challenge. (Aiello, 2024). As the technology enables the exchange of information, the need to protect personal data has grown to reshape how personal information is collected, stored and utilized. Nearly half breaches involved customer personal identifiable information (PII), which can include tax identification (ID) numbers, emails, phone numbers and home addresses. According to previous research the cost-benefit analysis is not always accurate, because consumers cannot determine how their privacy may be impacted when shared with a third party. Research does consistently find that online privacy violations lead to decreased trust in a company or website and trustworthiness and perceived information safety determine a consumer’s willingness to share personal information with a business. (Markos et al., 2023).

It is required for Consumers to make online purchases, interact on social media platforms, or connect with health care providers, information like name, date of birth, and health background information to complete the process. The growth that e-commerce and the smartphone has generated concerns about online data security as breaches continue to rise. E-Commerce expansion surged due to social distancing measures changing consumer to spend more time online. (IBISWorld, August 2024). Consumers feel unprotected when a social contract is disrupted by a data breach, resulting in the loss in personal information. Digital transformation, and connectivity, and intelligent systems, digital breaches have become an area of concerned. The lack of strong cybersecurity measures has proven to cause increasing losses and can range from financial damages, highlighting the critical need for robust cyber risk management. Despite substantial investments in cybersecurity many organizations lack preparation and awareness. My research is based on the Data Breach notifications affecting Washington Residents. (Dominik Molitor, Wullianallur Raghupathi, Aditya Saharia and Viju Rahgupathi., n.d.). The goal is to assess the impact of breaches on the number of residents affected in Washington State. Washington Law requires entities impacted by a data breach to notify the Attorney General’s Office (AGO) when more than 500 Washingtonians personal information was compromised as a result of the breach.

**Hypotheses**

H1. The data lost in a breach will affect consumers’ satisfaction.

H2. The days to identify breach will affect revenue

H3. The days elapsed before notification will affect revenue

H4. The number of Washingtonians will be financially impacted

Research Questions:

1. What is the average number of Washingtonians affected by data breaches during the past 7 years?
2. What are the average days that it takes to identify the breach?
3. What are the average days that it takes to notify Washingtonians about the data breach?
4. How do the data breaches impact Washingtonians Financially?

Dependent Variable (DV):

The main focus of my research is on data breaches affecting Washington residents as the dependable variable. Through the research I want to measure and assess the impact of data breach. The measurement will be based on an ordinal scale based on the numbers of Washingtonians affected by the data breach.

Independent Variable (IVs):

Through the research I want to measure and assess the impact of data breach. The measurement will be based on an ordinal scale based on the numbers of Washingtonians affected by the data breach, days to identify data breach and days elapsed to notify the residents about the data breach incidents.

Unit of Analysis:

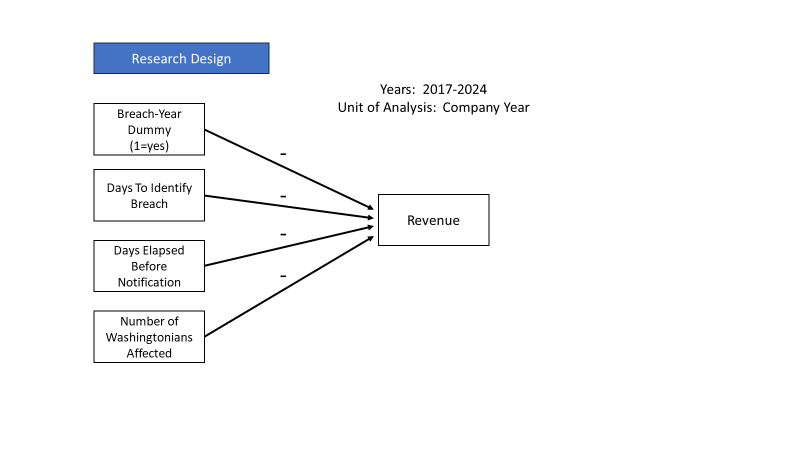
The unit of analysis is the individual residents.

Samples of Population:

The estimated or known number of Washington residents whose information was affected by the data breach. (Figure 2. Model Variable illustrates the description).

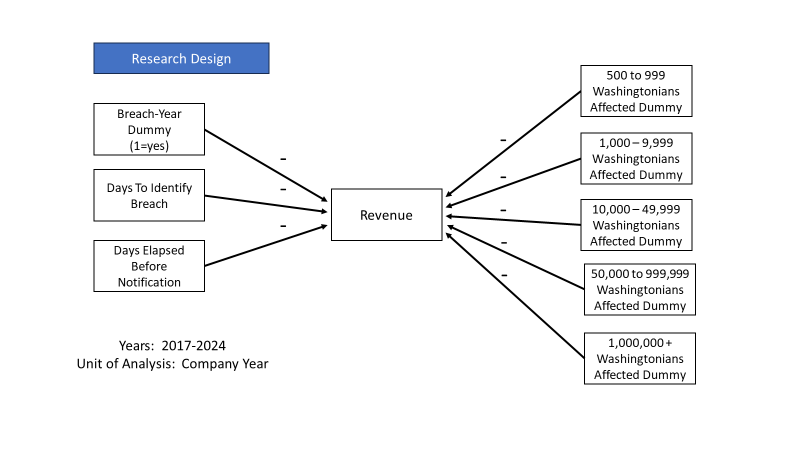
Figure 1 illustrates the theoretical model and Research Design

**Methodology**

****

**Fig. 1**. **Model Variable**

Figure 2 illustrates the theoretical model and Research Design

****

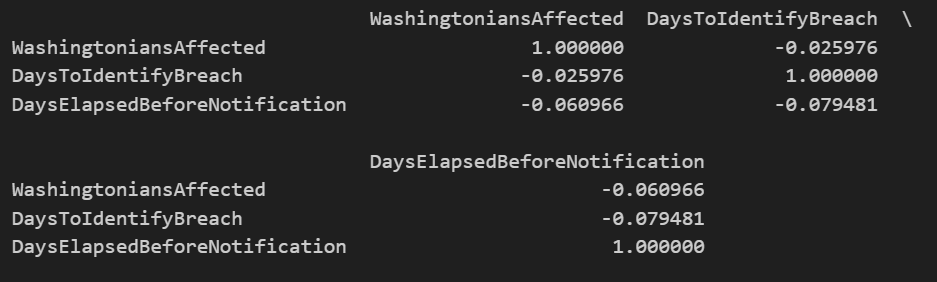
**Fig. 2. Model Variable**

Statistical Tables:

Descriptive statistics

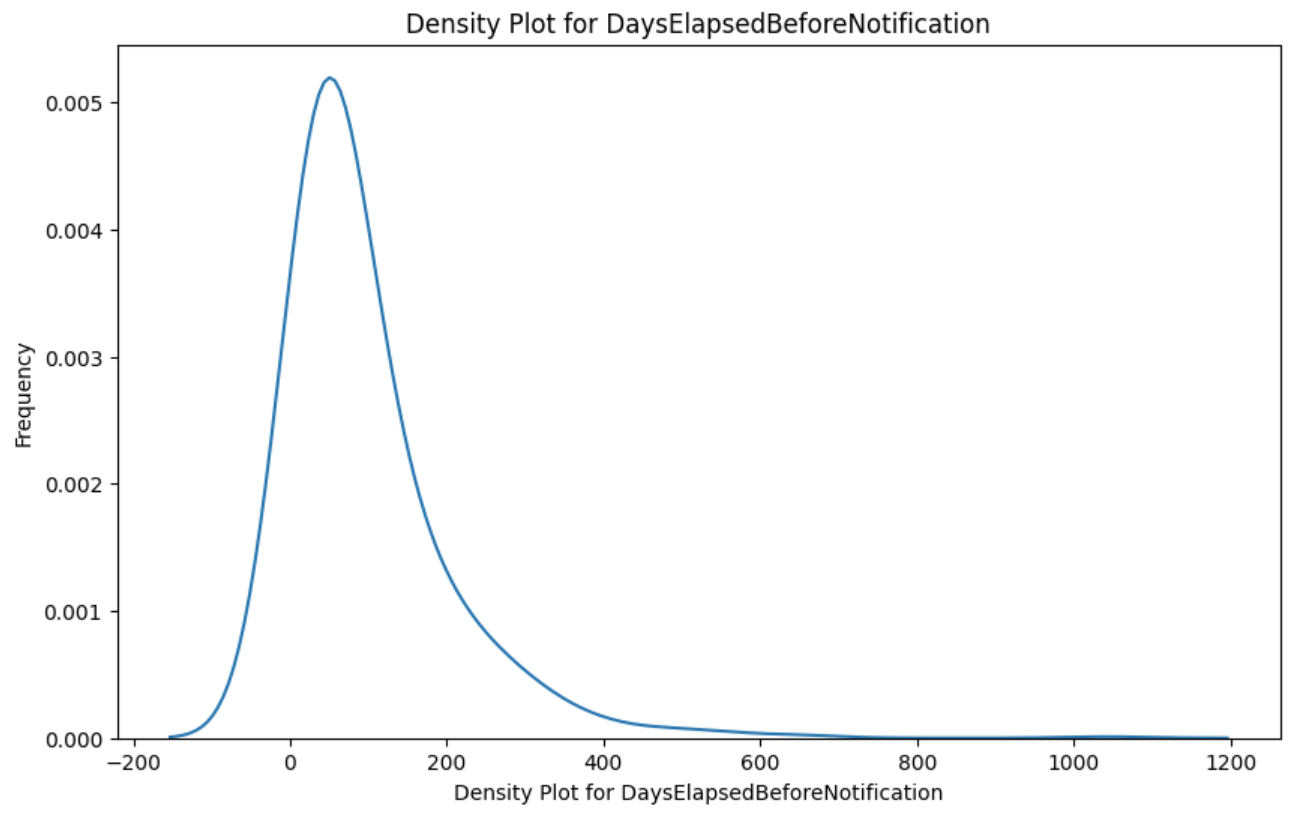
We turn to the Washington Residents affected by the data breach.

Correlations.



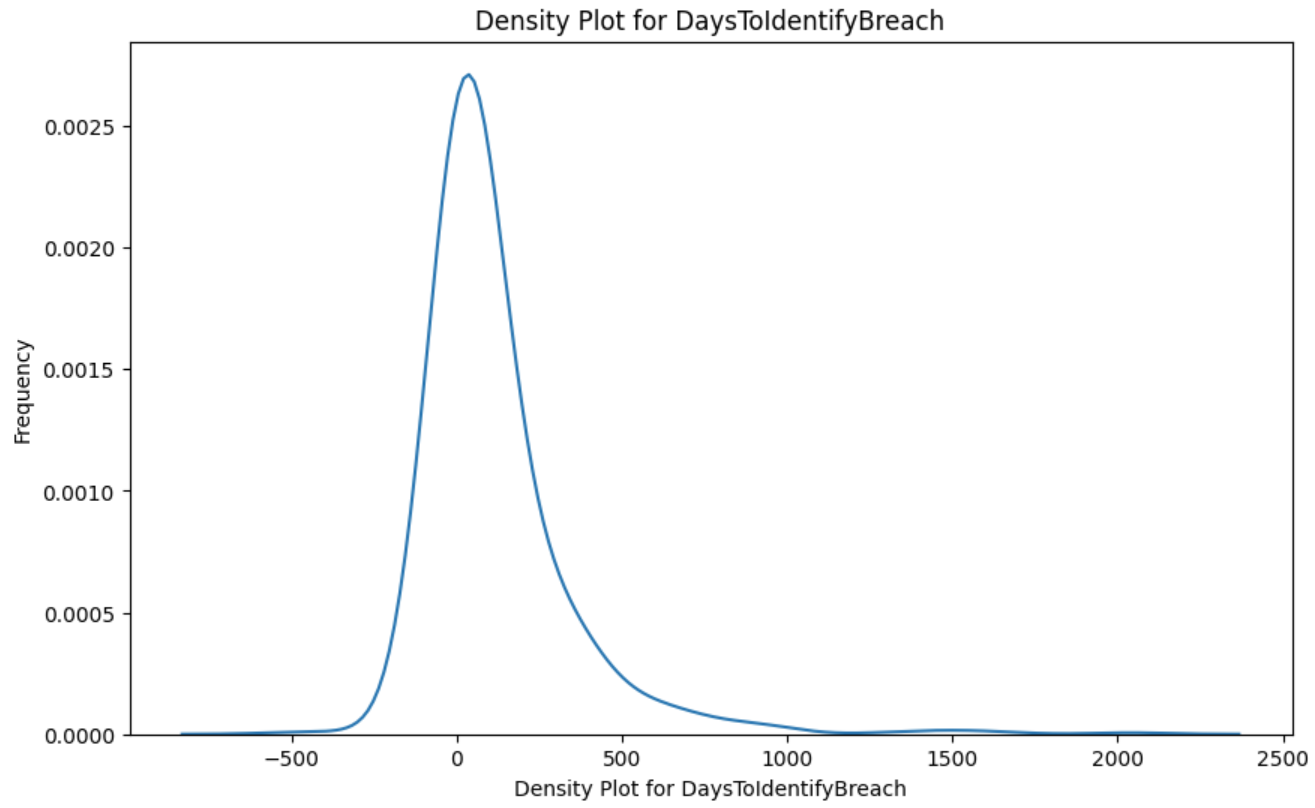
There is a strong positive correlation coefficient on more individuals affected which corresponds to more days to identify. There is a negative correlation (more affected individuals to days to identify and days Elapsed before notification.

**Distributions.**

****

The X-axis (Days Elapsed Before Notification): This represents the number of days taken to notify residents after the breach.

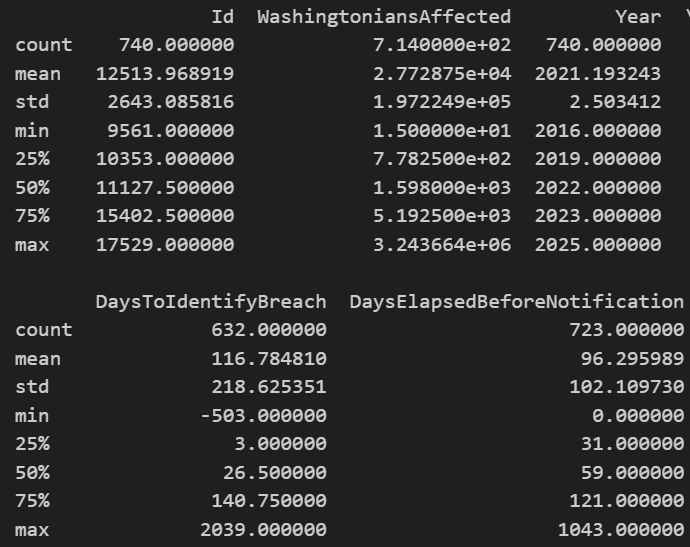
Y-axis (Frequency): This indicates how often different values of days elapsed occur in the dataset. A higher density means that more breaches had a similar number of days before notification.

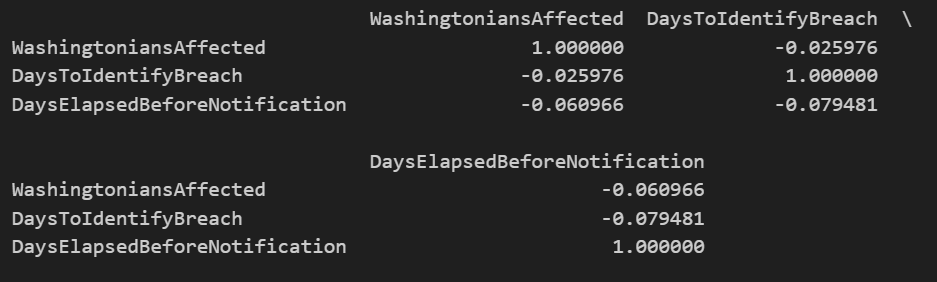


The X-axis (Days to identify breach): This represents the number of days taken to notify residents after the breach.

Y-axis (Frequency): This indicates how often different values of days elapsed occur in the dataset. A higher density means that more breaches had a similar number of days to identify breach.

**Analytical Methods**





**APPENDIX**

**Table 1.**

*Descriptive Statistics.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Variable | Mean | Std | Min | Q1 | Median | Q3 | Max |
| Washingtonians Affected | 12513.968919 | 2643.085816 | 9561.000000 |  |  |  |  |
| Days to Identify Breach | 116.784810 | 218.625351 | -503.000000 |  |  |  |  |
| Days Elapsed Before Noti. | 723.000000 | 102.109736 | 0.000000 |  |  |  |  |

**Table 2.**

*Correlations.*

|  |  |  |  |
| --- | --- | --- | --- |
| Variable | (1) | (2) | (3) |
| Washingtonians Affected | 1.000000 | -0.025976 | -0.60966 |
| Days to Identify Breach | -0.025976 | 1.000000 | -0.079481 |
| Days Elapsed Before Noti. | -0.060966 | -0.079481 | 1.000000 |
|  |  |  |  |
|  |  |  |  |

**Figure 1.**

*Distributions of the variables.*

|  |  |
| --- | --- |
| Days to Identify Breach | Long trails shift toward the right- Indicating that it takes more time to identify the breach. |
| Days to Elapsed Before Notification | Trails are shifting towards the right- Indicating significant delays in the notification process. |
|  |  |

References