Individual Practical Assignment: MIS781

Student Name: Anh Khoi Vo
Student ID: 223262778

Table of content

1. Introduction

This report provides an analysis of the current state of data breaches across various entities, as monitored by the U.S. Department of Health and Human Services Office for Civil Rights. The report is divided into four distinct dashboards, each providing valuable insights for a specific role. The Secretary's dashboard offers a macro-overview of the breach landscape, including total breaches, cost implications, the number of individuals affected, and breach distributions across states and entities. The Chief Information Security Officer's (CISO) dashboard has a deeper into breach specifics such as type, location, threat level, source, and response times. Besides, the CFO's dashboard offers a detailed financial perspective, illustrating the cost of breaches over time, the cost incurred by source and type of breach, and cost by entity type. These insights are useful for effective budgeting and resource allocation. Lastly, the Compliance Manager's dashboard focuses on compliance standards status, detailing non-compliance by entity type and state, and highlighting the correlation between breaches and compliance status. This data is support for risk management and prevent attack ability in the future. By using the insights provided in this report, these key stakeholders can collaboratively develop more effective strategies to prevent data breaches and protect the individuals and entities through the U.S states.

1.1 Objectives of your BI Dashboards

- Objective 1 THE Secretary of U.S. Department of Health and Human Services Office for Civil Rights
- Objective 2 Chief Information Security Officer of U.S. Department of Health and Human Services Office for Civil Rights
- Objective 3: CFO of Information Security Department
- Objective 4: Compliance Officer of Security Department

1.2 Benefits/Advantages of your BI Dashboards

- Provides an overview of the attack/breach between 2021-2023.
- Analyse the attack sources, thereby improving methods to prevent cybersecurity attacks.
- Improve the financial viability in cybersecurity investment.
- Enhance the protection of compliance status in cybersecurity.

1.3 Assumptions

Table 1 Assumptions

Assumption 1: A covered entity is attacked many times.
Assumption 2: Not entity no cybersecurity compliance standard is attacked
Assumption 3: In the long term, number of cybersecurity attacks on healthcare institutes increasing
Assumption 4: Ransomware takes about 18% of the number of attack sources.

1.4 Description of business rules and of variables used in this report

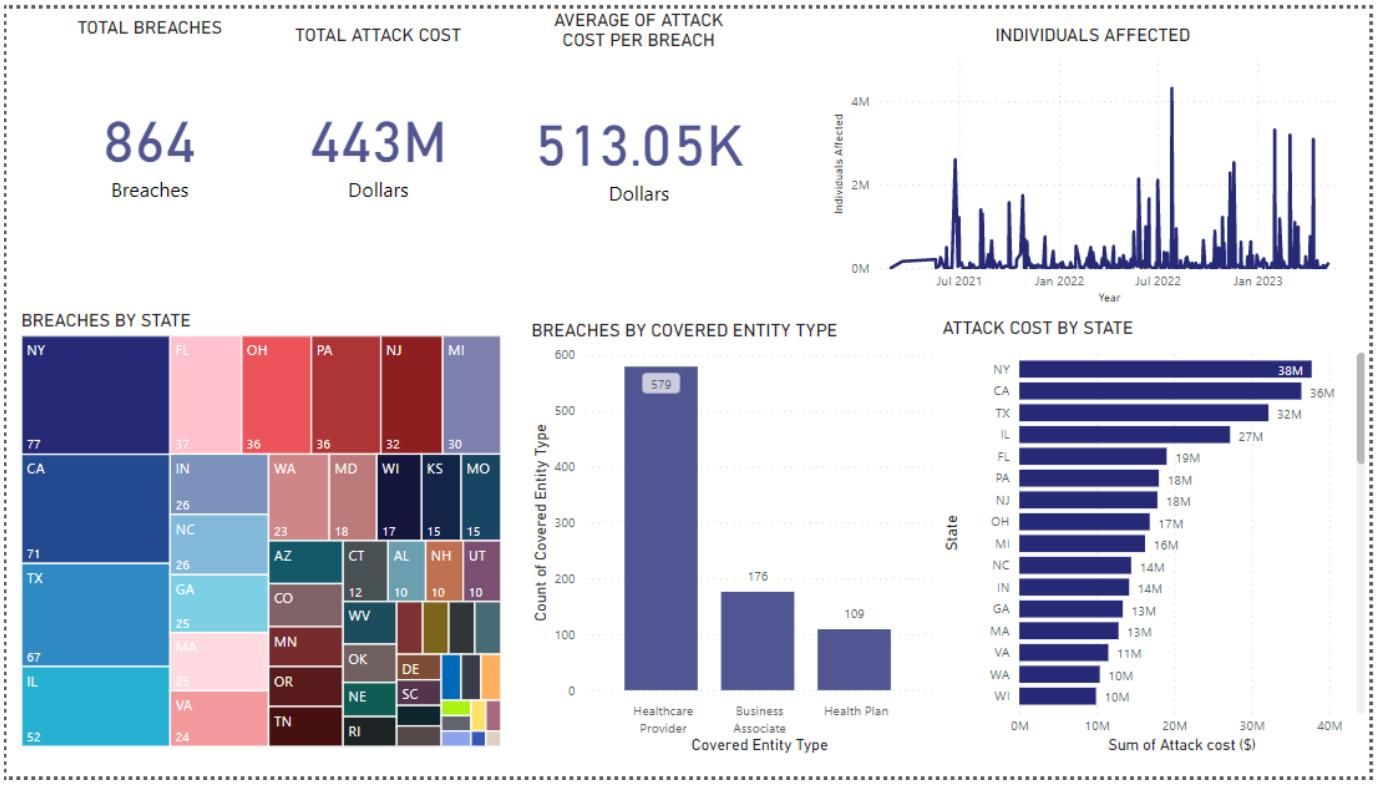
Table 2. Business Rules and final variables used for analysis

Variables	Description
Attack cost ($)	Amount of dollar cost damaged for an attack
Breach submission date	Date the attack/breach occurred
Compliance status	The cybersecurity standard used by entity
Individuals affected	Number of individuals that affected by breach
Level of threat	Level of threat of each attack
Location of Breached Information	The location of information, where the information is affected or attacked
Name of covered entity	Name of all covered entities, which are protected by the HHS
Source of breach	Origins of the breaches
State	The state in U.S that had the breaches
Time from detect to respond (mins)	The amount of time that counted form detect the breach to respond to it
Type of breach	The specific way in which a data breach or security incident has occurred
Business Associate Present	Third party was involved or present in the context of a data breach or security attack
Covered entity type	A classification of all entities

2. BI Dashboards

2.1 Dashboard 1: THE Secretary of U.S. Department of Health and Human Services Office for Civil Rights

The Secretary's dashboard provides a broad summary of the current data breach scenario. It includes an aggregate count of breaches, associated financial impacts, the total number of individuals impacted, and the distribution of breaches across various states and entities. overview of the data breach landscape, reflecting a



total of 864 breaches with a total attack cost of $443 million. This means that the average attack cost per breach is $513K. These numbers underline the seriousness and financial implications of the data security problem.

Chart 1

This chart shows the relationship between the number of individuals It is easy to see that the number of individuals affected by effectiveness increases over time from 2021 to 2023. In 2021, over 2 million individuals are affected, then there is a decrease. By July 2022, it will increase dramatically to more than 4 million individuals. After that, the number has decreased and remained above 2.5 million in 2023. Although there are times of increase and sometimes decrease, in general the gap of individuals between time points is increasing. Proved to be more widespread and affect more individuals in the future.

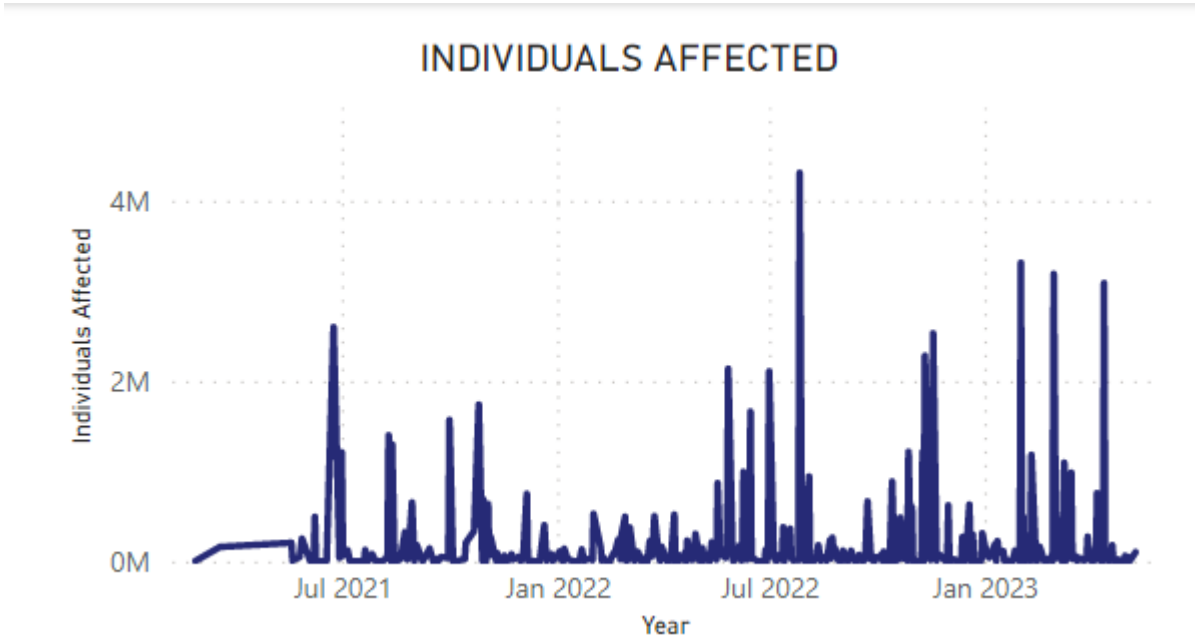


Chart 2

This graph illustrates the breakdown of profits by location, with New York (NY) leading the way with a total of 72. Following New York are California (CA), Texas (TX), and Illinois (IL). The graph suggests a correlation between the high number of profits and the larger populations in these states Undeniably, New York (NY) needs more scrutiny as it is the most frequently violated location. California (CA) and Texas (TX) also need more focus due to their significant number of violations. While these states are currently the most affected, it

is important to acknowledge that less affected states are not immune to similar threats in the future. Lessons learned from the hard-hit states must be applied broadly to prevent similar scenarios in less-affected states.

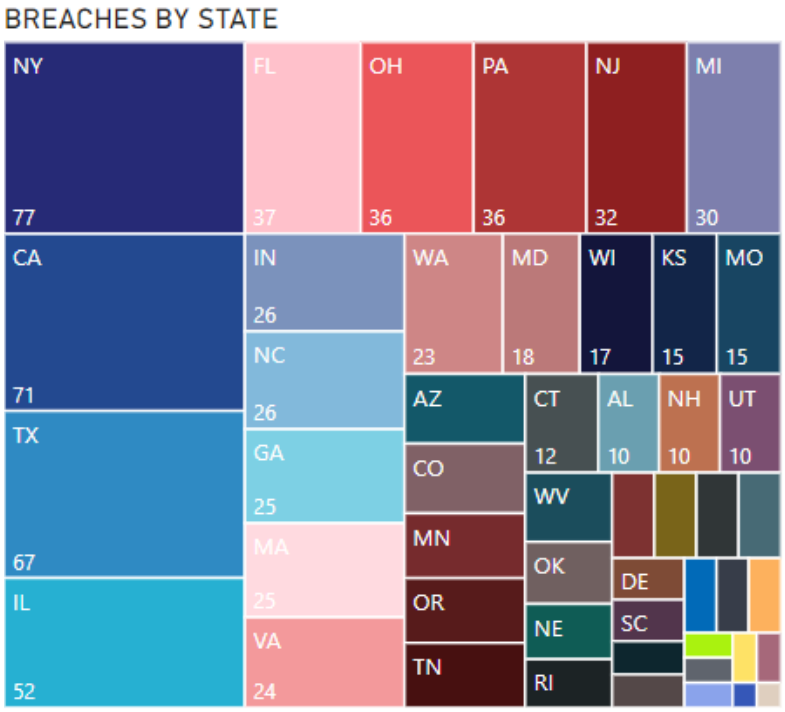


Chart 3

This graph displays the spread of covered entities according to their type. While all types of entities experience some degree of involvement, healthcare providers top the list with almost 579 breaches. Business associates follow in second place with close to 176 breaches, and health plans bring up the rear with slightly more than 100. This data suggests that healthcare providers are the most target and should therefore be the focus of increased vigilance.

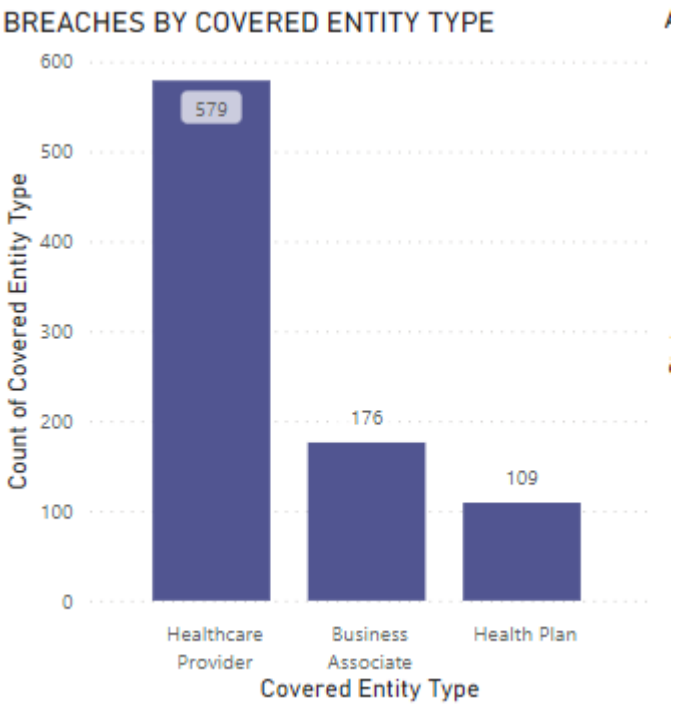
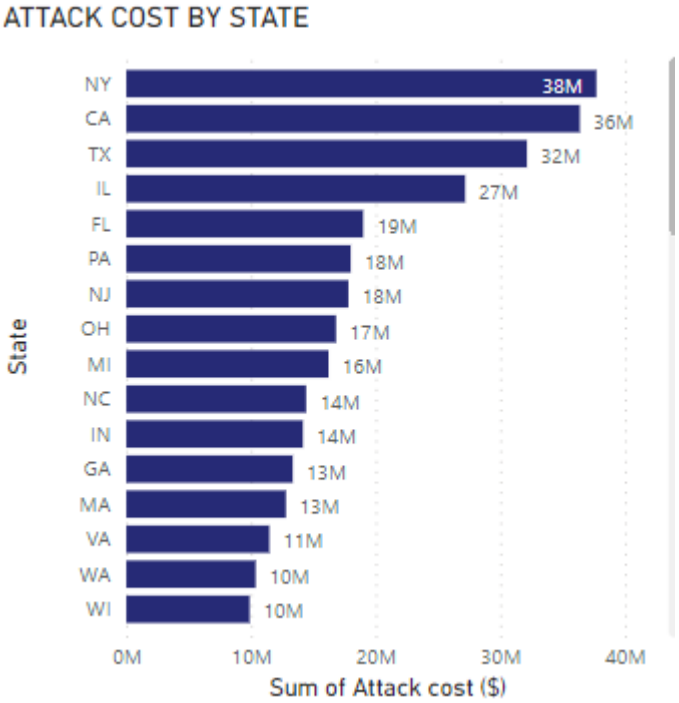


Chart 4

This graph illustrates the comparison of attack costs across various states. Consistent with the previous observation, the top four states in terms of profits are also the ones with the highest attack costs. New York (NY) is at the forefront with an attack cost of $38 million, followed closely by California (CA) at $36 million. Texas (TX) incurred costs of $32 million and Illinois (IL) accounted for $27 million. Wisconsin (WI), at the lower end, experienced attack costs of $10 million, which is almost a quarter of the cost faced by New York.



2.2 Dashboard 2 Chief Information Security Officer of U.S. Department of Health and Human Services Office for Civil Rights

This dashboard presents a real-time overview of security breaches over time, detailed breakdowns of breach types, and the locations where these breaches most commonly occur such as network servers and emails. Further, it illustrates the threat level distribution to help prioritize risk management efforts. It also provides valuable insights into breach sources and the average time taken from breach detection to response, crucial for enhancing our incident response strategy.

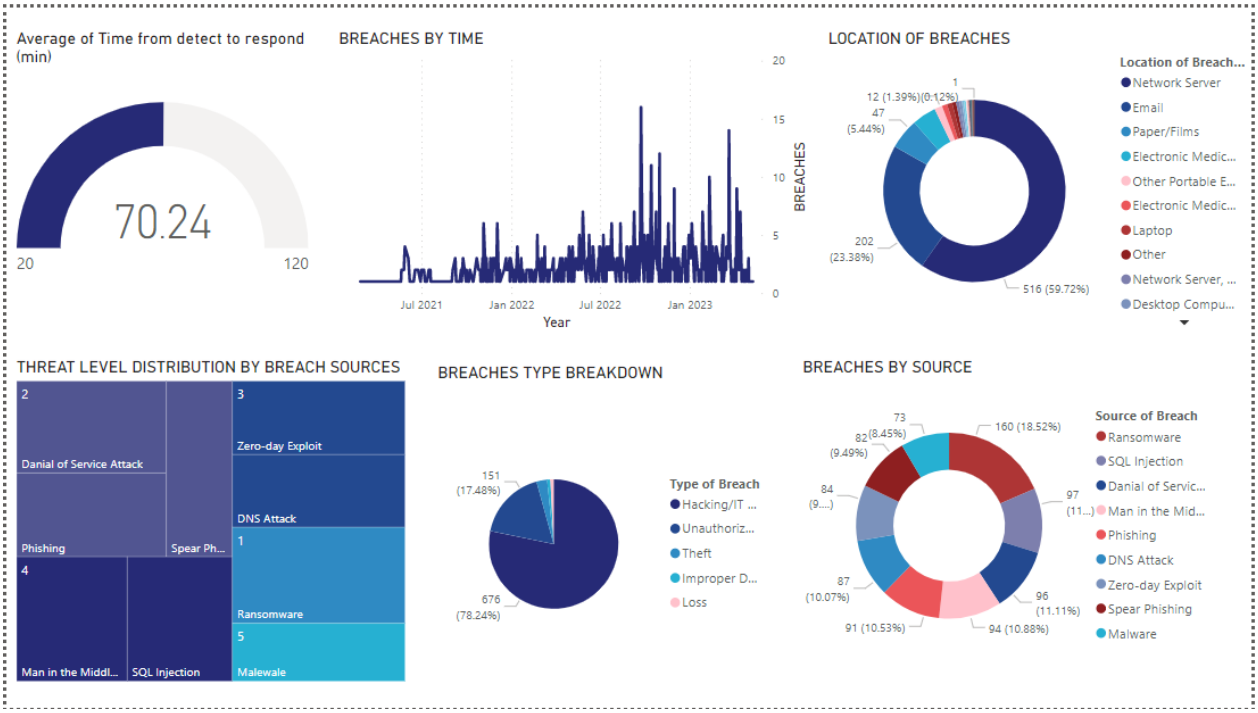


Chart 1

This chart depicts the fluctuation in production volume over time. Initially, in July 2021, there were close to 5 breaches per day. By January 2022, this figure saw a slight increase to just above 5 breaches daily. A dramatic surge occurred from July 2022 to January 2023, peaking at more than 15 breaches per day. Following this, there was a downturn; however, the daily volume stabilized and sustained at around 10 breaches per day.

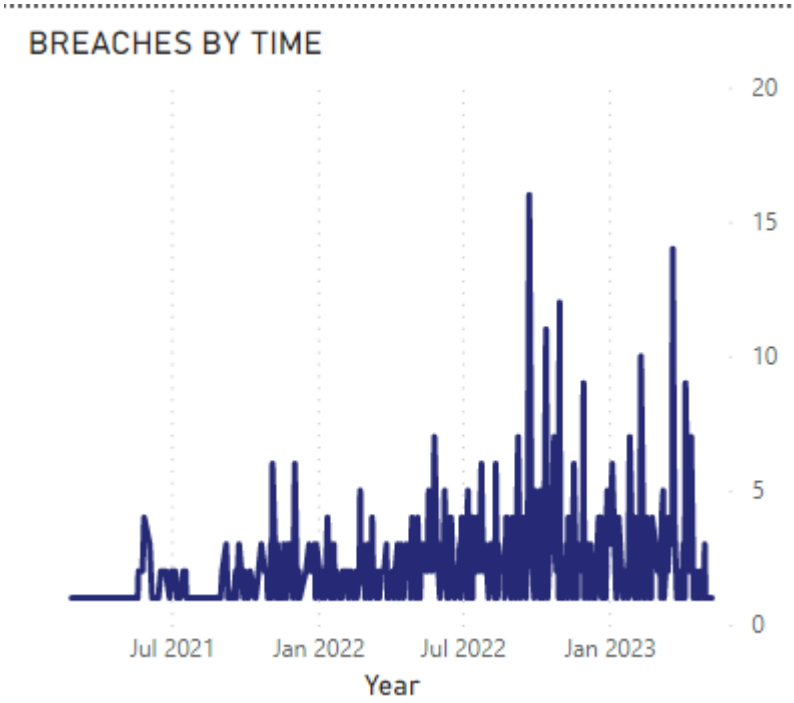


Chart 2

This pie chart shows the distribution of benefits by type. The largest number, accounting for 78.24%, is the type of breach Hacking/IT Incident. Behind is Unauthorized Access/Disclosure accounting for 17.48%. accounted for 2.6% and ranked 3rd is Theft. Together with the lowest percentages are Improper Disposal and Loss with 0.8%. This shows that Hacking/IT Incident is the method most targeted among types of breach.

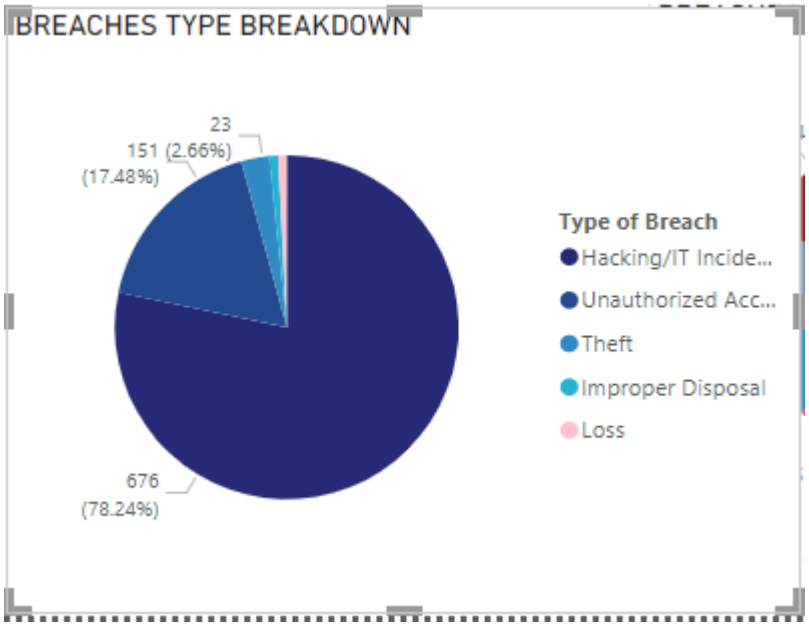


Chart 3

This donut chart shows the location rates at which events occur or penetrate. Topping the list is Network Server, accounting for 59.72%. Email comes in second with 23.38%. In third place is Paper/films with 5.44%. The lowest is Desktop Computer with 1%. The network server is the most vulnerable to attack and it can lead to significant consequences. Next is email, which customers and entity employees can reach every day are at risk of being taken advantage of.

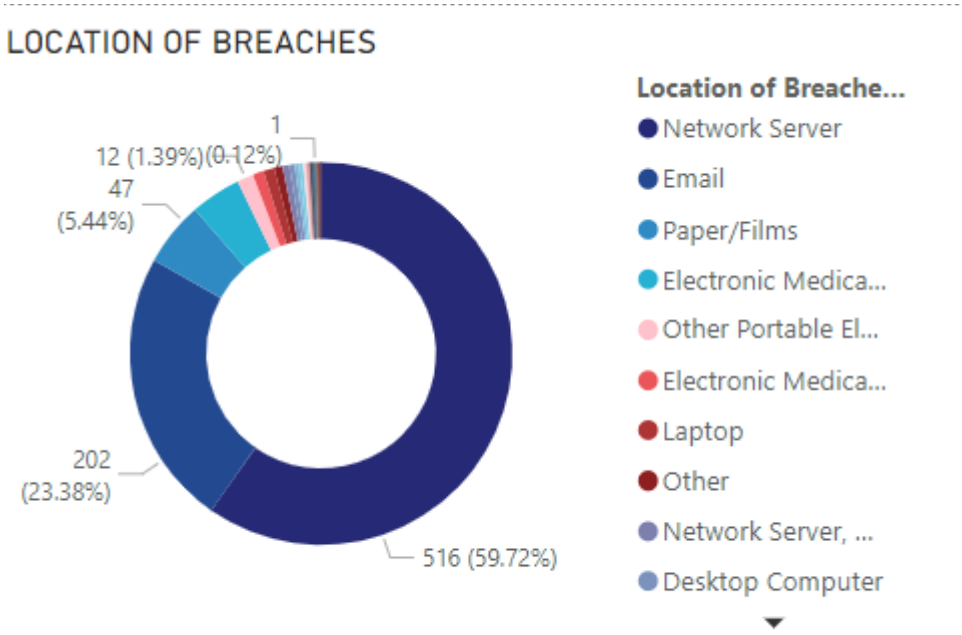
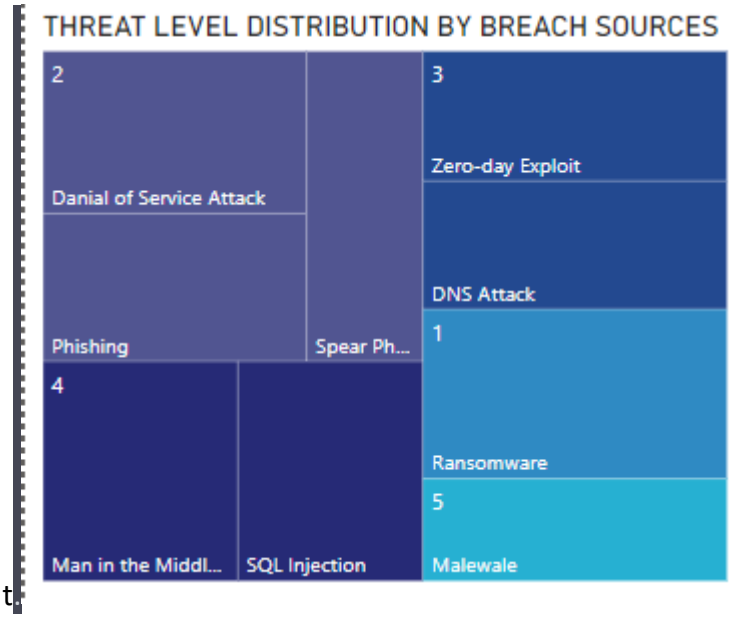


Chart 4

This tree map provides a visualization of the distribution of threat levels across various breach sources, aiding the Chief Information Security Officer (CISO) in formulating response strategies. Denial of Service attacks, Phishing, and Spear Phishing are the primary breach sources, posing a substantial threat level of 2. Following these, Man in the Middle attacks and SQL Injection present a secondary threat level of 4. Zero-day Exploits and DNS attacks represent the third tier with a threat level of 3. Ransomware falls into the fourth category with threat level of 1, and Malware, having the highest threat level of 5, is ranked last.



t.

Chart 5

This gauge visualization provides the average of time from detect to respond. It can be seen that the quickest respond is 20min and the longest is 120 mins. Besides, the average respond time is 70.24 min. This is a long amount of time leading to increased damage. So, it should be fixed in the future. The average response time from detection to action is now 70.24 minutes. This time can give an attacker a generous amount of time to deal significant damage. Efforts should be focused on reducing this response time.

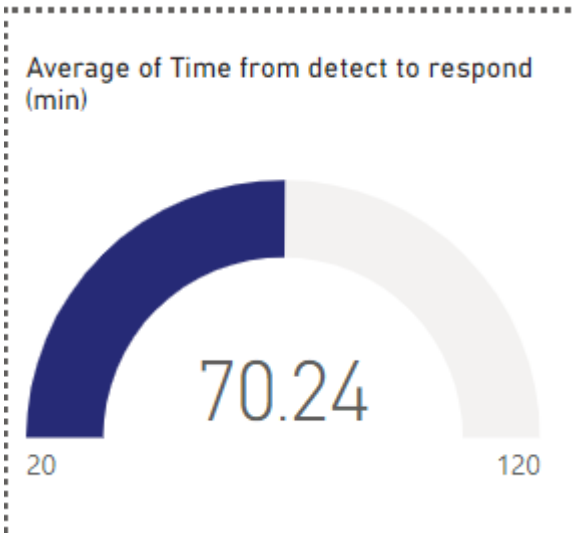
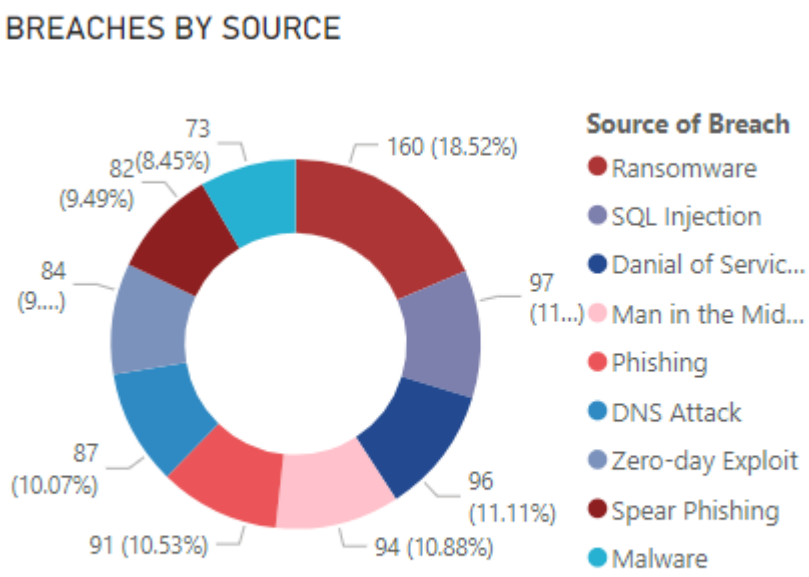


Chart 6

This donut chart represents the percentage of profit by source. Ransomware accounted for the majority with 18.25%. Second is SQL Injection with 11.23%. Coming in third and accounting for 11.11% is the Danial of service attack. Following are Man in the Middle attack, phishing, DNS attack, Zero-day Exploit and Spear Phishing with rates, 10.8%, 10.53%, 10.07%, 9.72%, and 9.49% respectively. Malware accounted for the lowest with 8.45%.



2.3 Dashboard 3: Chief Information Security Officer of U.S. Department of Health and Human Services Office for Civil Rights

The CFO Dashboard presents an invaluable tool for assessing the financial impact of a data breach, critical for strategic financial planning and resource allocation. Its ability to illustrate attack cost trends over time provides a clear view of the financial consequences and helps identify periods of increased vulnerability. In addition, by providing cost breakdown by source of breach, it enables the identification of costly threat vectors, aiding in prioritizing defense mechanisms. Additionally, by categorizing costs by breach type and organization type, the dashboard sheds light on which instances caused the greatest financial harm. This information is important to understand where prevention and mitigation efforts will be most economically profitable. The ability to track these metrics and understand the financial implications is critical for budgeting, risk management, and for making informed decisions about investing in new security technology or training.

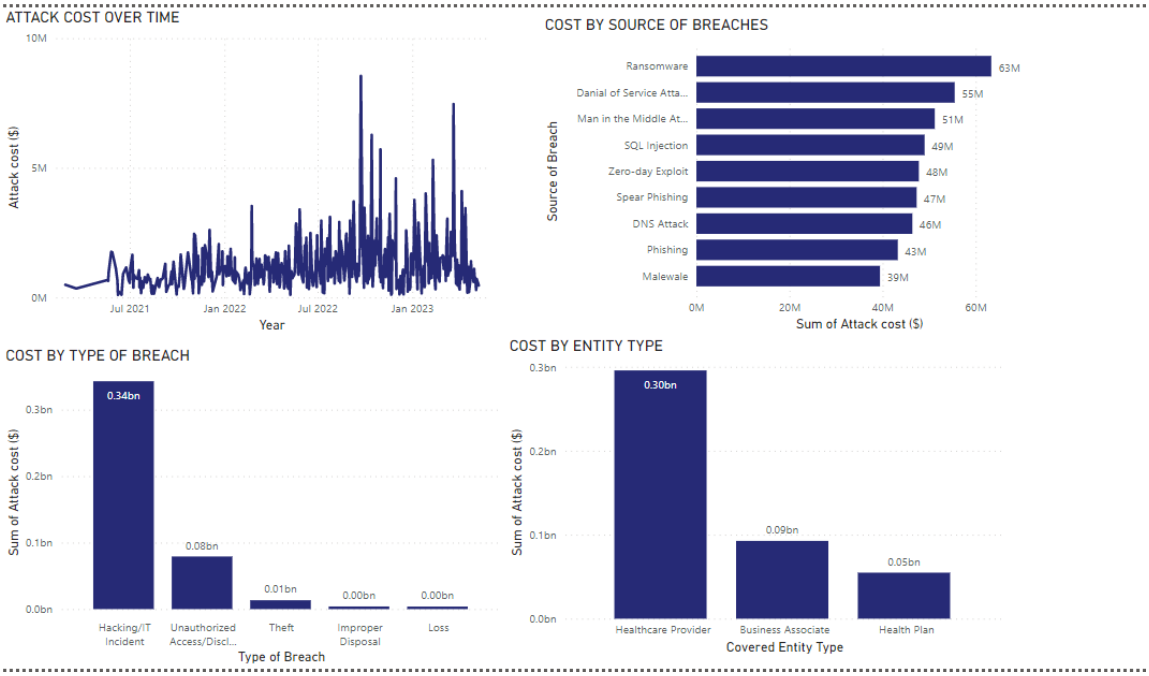


Chart 1

This line chart shows the change of attack cost over time from July 2021 to January 2023. It is easy to see that 2021 starts with 490k ($) attack cost. Then, into 2022, it starts to gradually increase and peaks in July 2022 with 8mil ($) attack cost. After that, the attack cost can decrease and stay between 600k ($) – 1mil6 ($). This is notable because the attack cost increases alarmingly and could increase further.

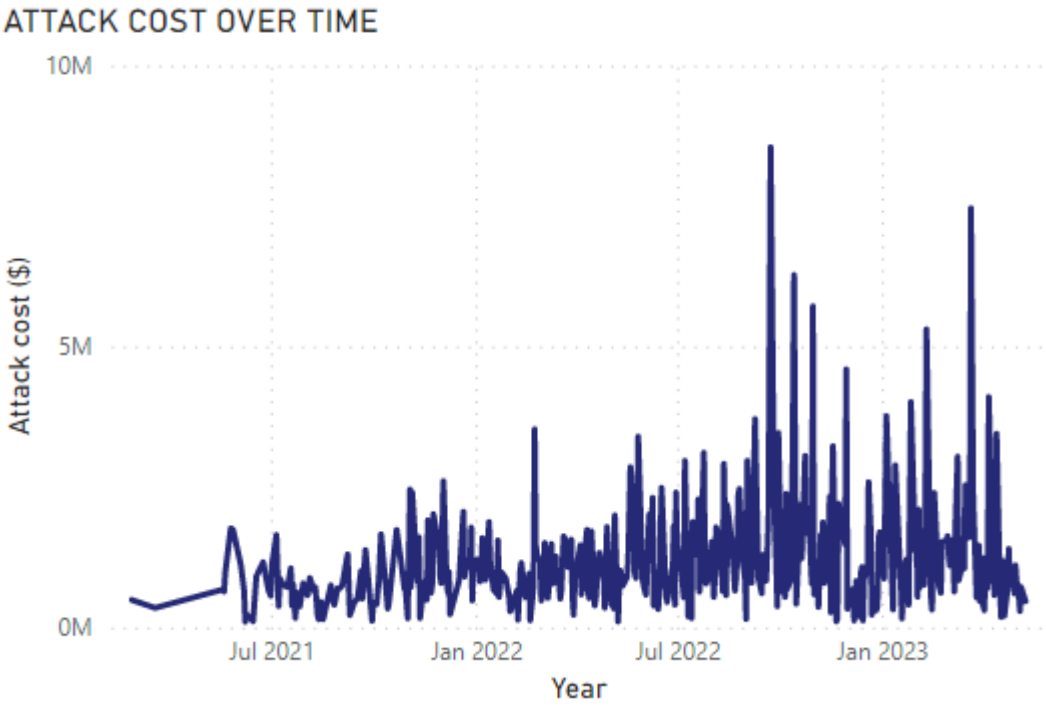


Chart 2

This bar chart depicts cost variations between different sources of violation. Ransomware seems to be the most expensive, worth $63 million. This was closely followed by denial-of-service attacks, which amounted to $55 million. In third place, Man in the Middle Attacks had a budget of $51 million. SQL Injection, Zero-day Exploit, Spear Phishing, DNS Attack and Phishing are in the middle, priced at $49 million, $48 million, $47

million, $46 million, and $43 million, respectively. Finally, Malware, while still substantial, costs as little as $39 million.

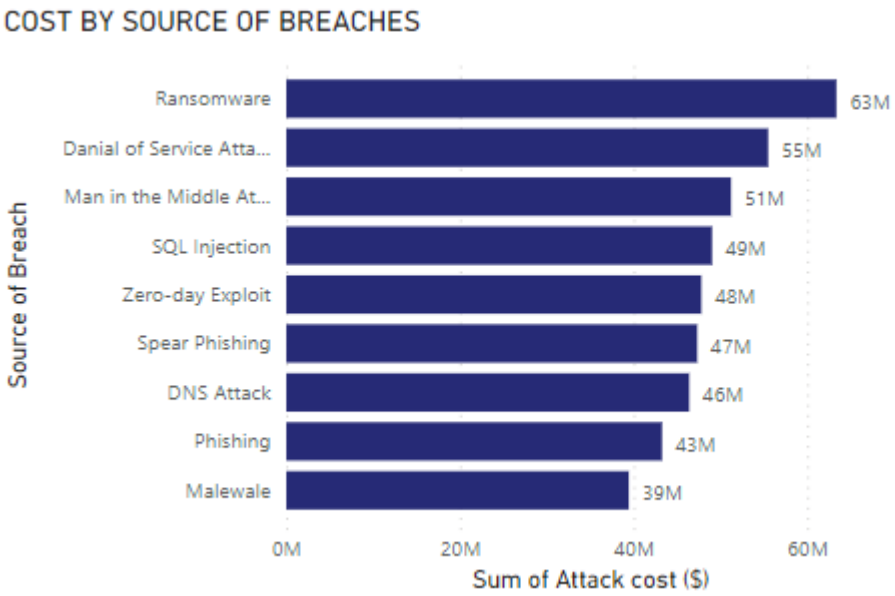


Chart 3

In terms of breach type, Hack/IT Incident was the most expensive, resulting in a staggering $0.34 billion in damages, four times the cost of the next most expensive category, Unauthorized Access/Disclosure , at $0.08 billion. Other categories such as Theft, Improper Handling, and Loss were significantly less expensive, causing $0.01 billion, $3.9 million, and $3.8 million, respectively.

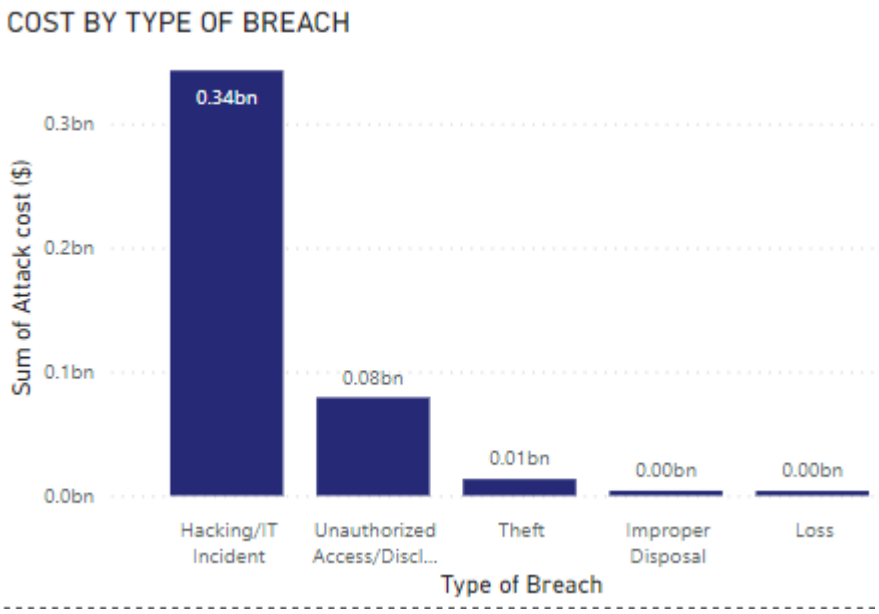
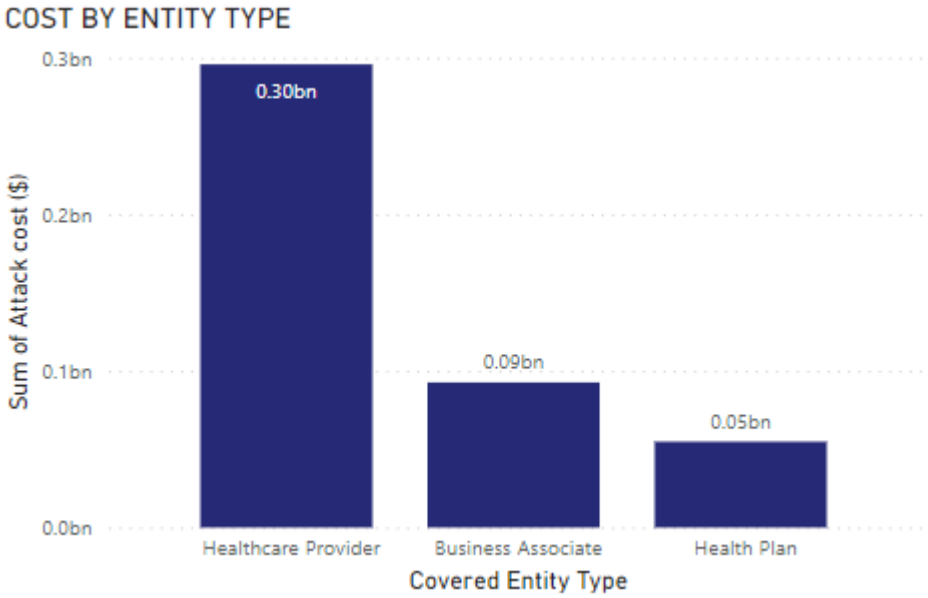


Chart 4

In the context of entity types, the chart clearly shows that Healthcare Providers bear the brunt of the loss, at a cost of nearly $0.3 billion. Business Associates followed in second place with a loss of about $0.09 billion. Health Plans suffered the least financial impact, with a loss of about $0.05 billion. This consequence reflects the prevalence and prominence of Healthcare Providers in this field.



2.4 Dashboard 4: Compliance Officer of Security Department

The Compliance Manager dashboard focuses on compliance status related to security standards. It identifies non-compliance issues by entity type and state, highlighting areas for improvement. It also shows the relationship between breaches and compliance status, allowing to assess how compliance or lack of compliance affects the likelihood and severity of breaches. This critical feature allows for the evaluation of the effectiveness of current compliance measures and highlights the risk posed by non-compliance. Besides, it provides insight into the geographic distribution of noncompliance, thereby supporting a more targeted approach to improvement.

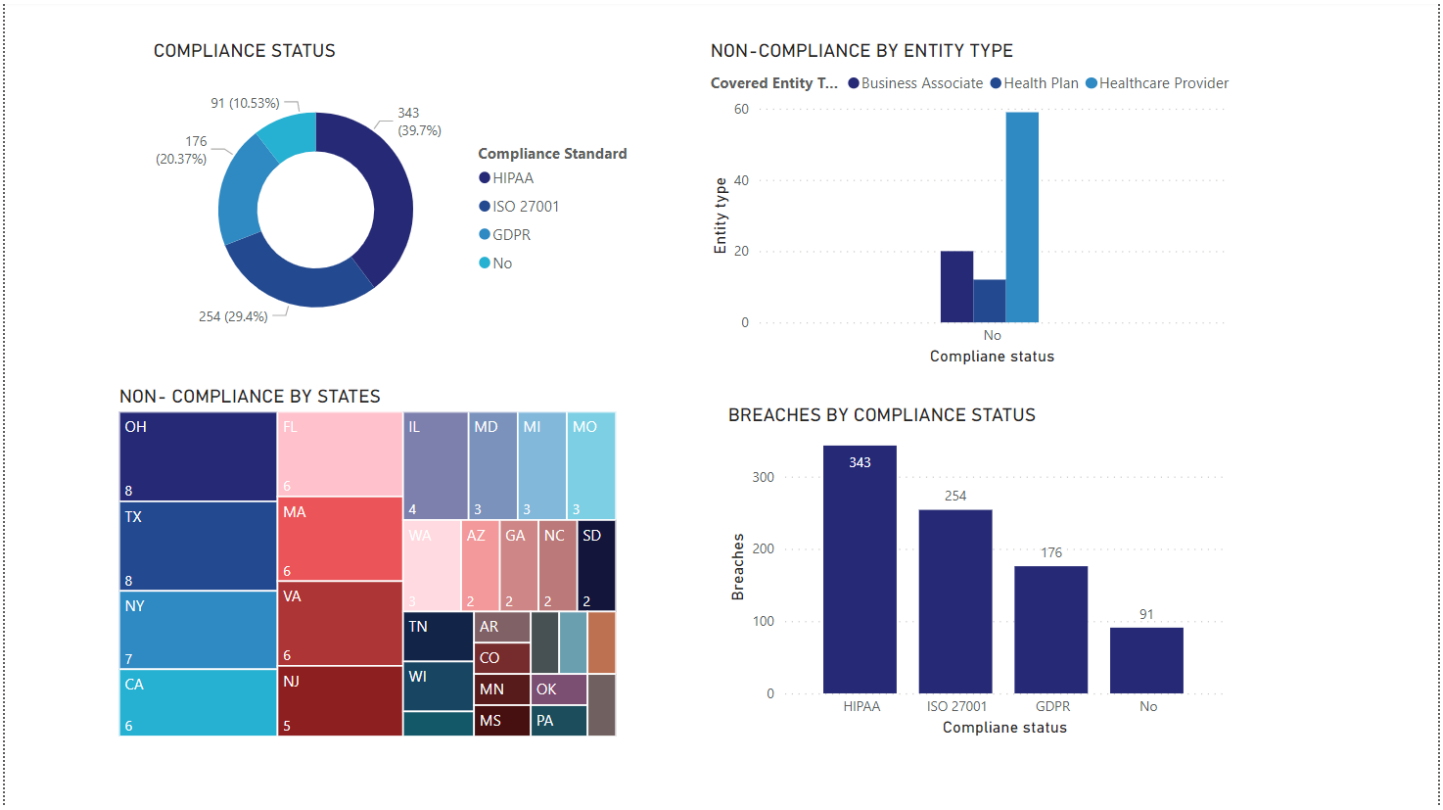


Chart 1

This donut chart initially shows the percentages of entities that are compliant and not compliant with compliance standards. It should be noted that 10.53% of entities do not adhere to any compliance standards. On the other hand, 89.47% of the units are compliant with certain standards, which is broken down as follows: 39.7% HIPAA standard, 29.4% ISO 27001 compliant, and 20.37% GDPR compliant.

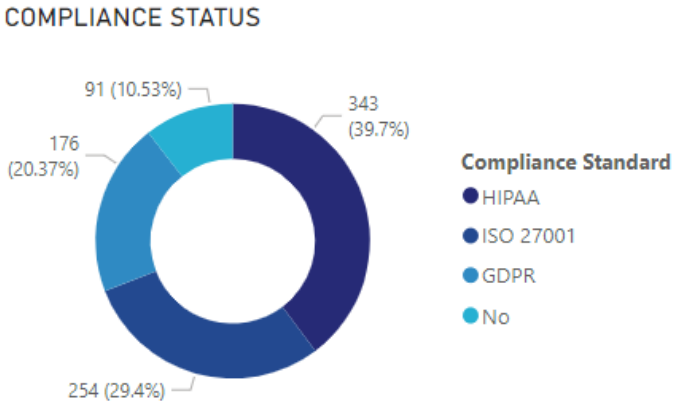


Chart 2

The bar chart visualizes the number of non-conforming entities by type. It is clear that healthcare providers are at the forefront with nearly 60 cases of noncompliance. Business partners follow about 20 cases, while health plans follow the least with about 10 cases. This sample shows that healthcare providers, although most targeted, are not compliant as expected, indicating a potential area for improvement. Enhanced compliance

strategies should be implemented, especially in healthcare providers, to ensure better security.

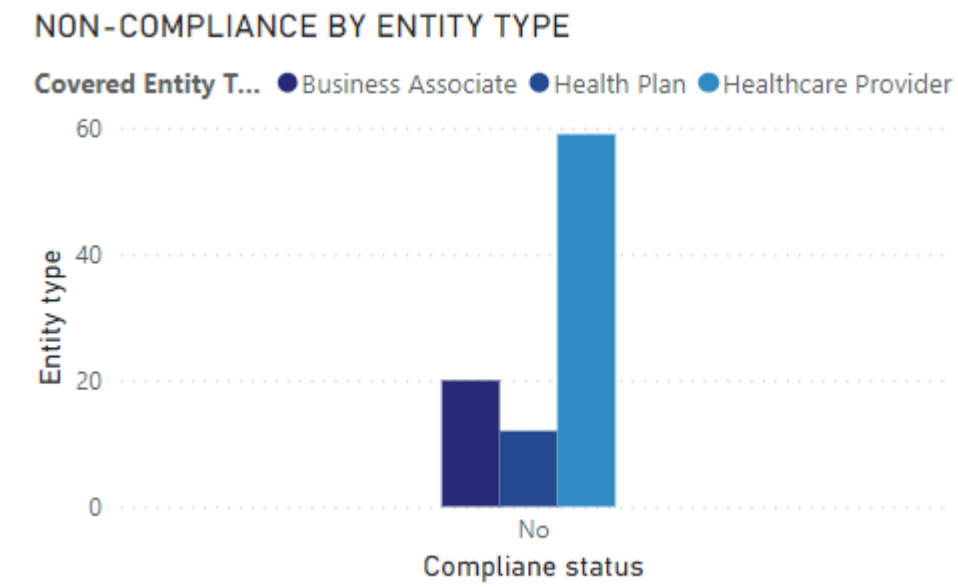


Chart 3

The graph showing non-compliance across states shows Ohio (OH) and Texas (TX) as the leaders, with eight entities each that did not meet any compliance standards. New York (NY) came in second with 7 non-compliant entities. California (CA), Florida (FL), Massachusetts (MA) and Virginia (VA) all had six entities that lacked compliance. The remaining states each have less than 6 non-compliant entities. This model highlights the need for an increased focus on ensuring compliance in states with higher rates of non-compliance, with Ohio and Texas in need of immediate attention. Medical providers, although most targeted, show higher rates of non-compliance. This suggests that these entities may not fully understand the importance of security standards or how to comply with them.

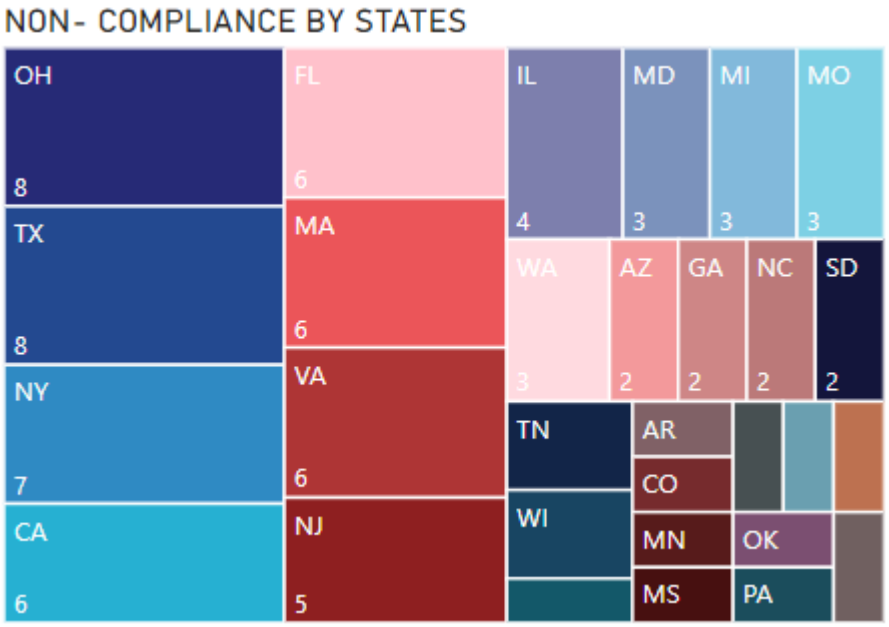
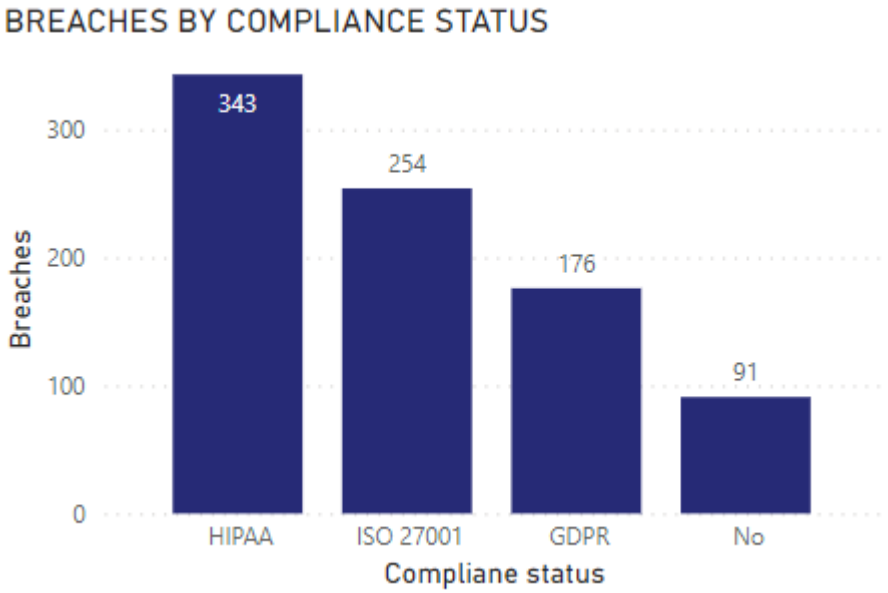


Chart 4

The bar graph regarding compliance status highlights that HIPAA standards-compliant entities make up the majority, represented by 343 entities. In second place are entities that comply with the ISO 27001 standard, which includes 254 entities. Entities that meet the GDPR standard are in third place, with a total of 176

entities. Entities that do not meet any of the compliance standards are at a lower level, with a count of 91. Clearly, HIPAA is the most widely implemented standard among entities and at the same time, it seems most easily violated. This indicates the need to strengthen security measures in HIPAA compliant entities.



3. Recommendations

- First, reducing the number of people affected by the agency is something that each entity should be more responsible for, not just the government. Entities should prioritize strong data governance and proactive cybersecurity measures. This includes regularly updating and fixing cybersecurity systems, implementing multi-factor authentication, and encrypting sensitive data. In addition, regular training for employees on how to recognize and respond to cyber threats such as phishing is also important. Especially the staff who have little knowledge of network security and know a lot of sensitive information of patients or customers. Additionally, regular audits and compliance audits should be conducted to identify and remediate potential vulnerabilities and ensure compliance with privacy regulations such as HIPAA, GDPR or ISO 27001.

- In terms of geographic distribution, New York, California, Texas, and Illinois have consistently reported higher numbers of breaches and, as a result, they also incur the highest cost of attacks. This suggests that these states, due to their large populations, may be more attractive targets for cybercriminals. Centralizing cybersecurity, education, and training resources in these states can help mitigate these attacks. States can form a joint committee to discuss and come up with the best solution. The government can also divide the state into two types: high attack state and low attack state for easier management and better centralization of resources. Another way is that states can divide their resources among other states to reduce the network security workload.

- Healthcare providers stand out as the most vulnerable, with the highest number of breaches. This is likely due to the large amount of sensitive data they manage and the interconnected nature of their systems. The recommendation is to provide specialized cybersecurity training and resources tailored to healthcare providers. In other words, these providers should be more focused on cybersecurity and should build their own protection system that is more personalized. Should healthcare providers create a platform, ecosystem to share solutions and experiences with each other to provide the most appropriate and optimal protection.

- Enhancing network and email server security: Data shows that Network and email servers are the most exploited breach locations, accounting for a significant portion of breaches. To enhance protection for these two, it may include implementing advanced intrusion detection and prevention systems, firewalls, and end-to-end encryption for all communications. The communications of key locations should be secured with multiple layers and must be authenticated by multiple stakeholders. Training employees on safe email methods, recognizing phishing attempts, and reporting them immediately to CISO can also significantly reduce the risk of an email breach.

- The average response time from detection to action is currently 70.24 minutes. This time period can give an attacker a generous amount of time to deal significant damage. In order to reduce this amount of time, agencies that can conduct regular drills and simulations can also be helpful in preparing the team for quick and efficient troubleshooting. Not only in the US but can coordinate with leading countries in cybersecurity such as Russia, China, etc.

- Allocate resources to prevent and mitigate breaches: Data shows a significant increase in the costs associated with breaches, particularly related to ransomware, denial of service, and man-in-the-middle attacks. Invest in advanced cybersecurity tools and technologies, including endpoint protection, intrusion detection systems, and threat intelligence solutions. In addition, providing continuing education and training in cybersecurity for employees or investing in universities, research institutions or competitions to develop and leverage existing resources to create new solutions to save costs as much as possible.

- Strengthen Compliance Education and Training: Workshops, training sessions, webinars, or tutorials may be developed and delivered among these entities, with a particular focus on healthcare providers in states with high rates of health care with higher non-compliance rates like Ohio and Texas.

- Review and Reinforce HIPAA Compliance Measures: Although the HIPAA standard is the most widely adopted, it seems to be violated most often. This indicates that compliance is not simply about applying a standard, but about effectively implementing and maintaining that standard. Review and assess current HIPAA compliance for gaps and develop a comprehensive plan to address them. It can be replaced by other cybersecurity compliance such as SOC 2, NYDFS Cybersecurity Regulation, FERPA, NIST or CMMC (CompTIA, 2023). Furthermore, these units can spontaneously develop a healthcare-specific standard for optimal protection and best fit healthcare characteristics.

- Promoting a Culture of Compliance: Compliance should not be viewed as a strict obligation, but as a fundamental component of operational integrity and confidentiality. This culture should be maintained and there are rewards in keeping this culture. Entities can exchange employees with each other to learn from each other. In addition, severely penalize entities that intentionally do not comply or ignore warnings. This penalty is intended as a reminder rather than a penalty for cost.

4. Reference

CompTIA. (2023.). *What Is Cybersecurity Compliance | CompTIA*. Default. https://www.comptia.org/content/articles/what-is-cybersecurity-compliance#:~:text=At%20its%20core,%20cybersecurity%20compliance,availability%20(CIA)%20of%20information.

5. Appendix (Certificate of Completion for Power BI & Dataset)

LinkedIn Learning

Power BI Essential Training (2020)

Course completed by Kane Khoi Vo
May 15, 2023 at 03:04PM UTC

Top skills covered

Microsoft Power BI

Head of Content Strategy, Learning

Instructional Delivery Method: QAS Self Study
In accordance with the standards of the National Registry of CPE Sponsors, CPE credits have been granted based on a 50-minute hour.
LinkedIn is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

Field of Study: Computer Software & Applications
Program: National Association of State Boards of Accountancy (NASBA)
Registry ID: #140940
Continuing Professional Education Credit (CPE): 7.40
Certificate ID:
9a36b4f5a728f1e658a26dc20e2bbd5aadc41f1ebfefab1eeadb224c33b18282

	Name of Covered Entity	State	Covered E	Individuals	Breach Submission Date	Source of	Source of	Type of Br	Location o	Attack cos	Time from	Business A	Level of th	Compliane status
2	Uintah Basin Healthcare	UT	Healthcare	103974	5/10/2023	Malware	11	Hacking/IT	Network S	466291	82	No	5	ISO 27001
3	ASAS Health, LLC	TX	Healthcare	25527	5/6/2023	Ransomwa	12	Hacking/IT	Desktop C	717301	114	No	2	HIPAA
4	People Incorporated of Sequoya	OK	Healthcare	8725	5/5/2023	SQL Injecti	13	Hacking/IT	Network S	290339	35	No	4	ISO 27001
5	New Mexico Department of Hea	NM	Healthcare	49000	5/4/2023	Ransomwa	14	Unauthori	Other	582915	53	No	1	ISO 27001
6	Methodist Family Health	AR	Healthcare	5259	5/3/2023	DNS Attac	15	Hacking/IT	Network S	765205	48	No	3	GDPR