Insights from the Office for Civil Rights breach reports analysis

by Chebotarov V

Processed Steps / Data Collection and Validation

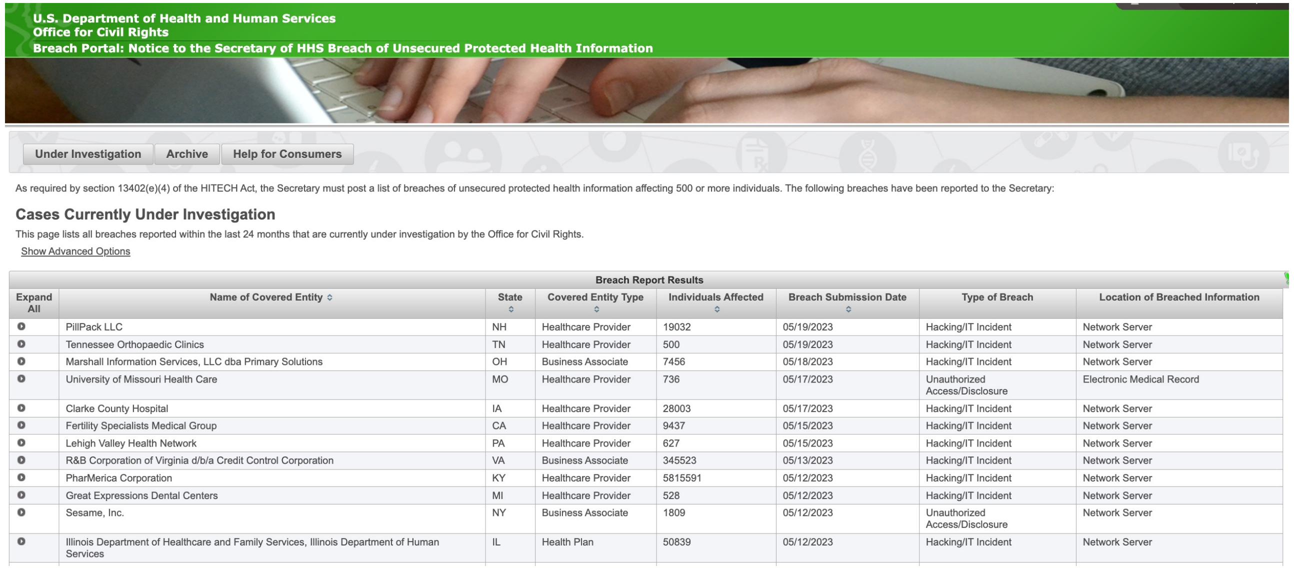
Collection of breach reports* from the U.S. Department of Health and Human Services Office for Civil Rights.

- scraping of current reports (last 24 months)
- scraping of archived reports (all resolved breach reports and/or reports older than 24 months)

Each report data was stored in JSON format and validated.

5384

reports were collected and stored



U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

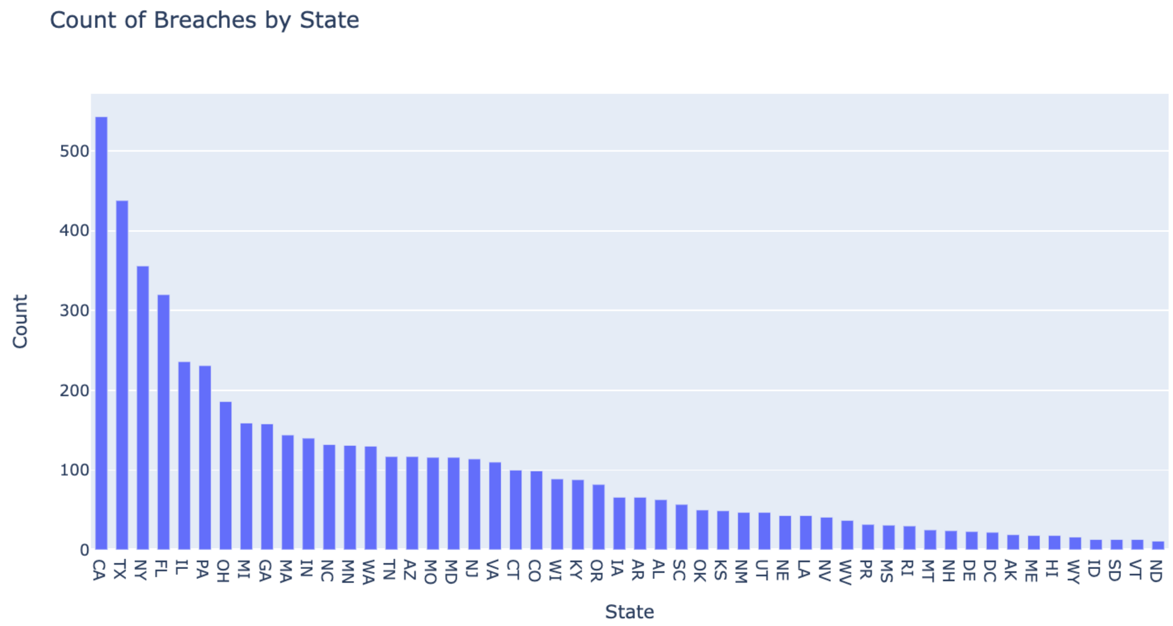
This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

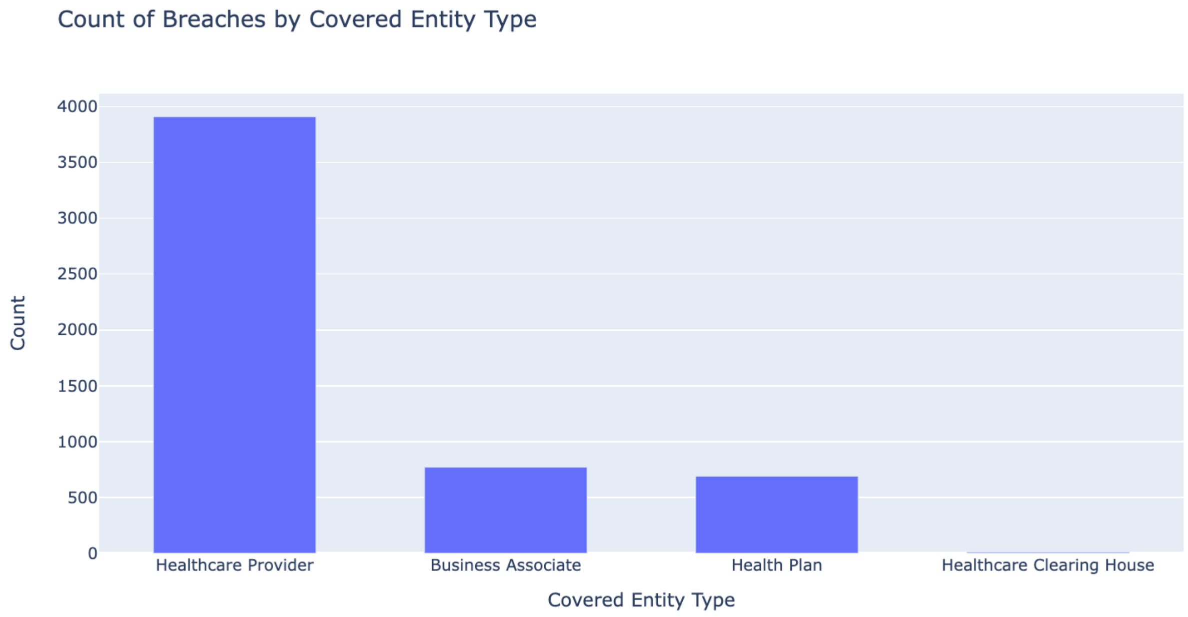
Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
●	PillPack LLC	NH	Healthcare Provider	19032	05/19/2023	Hacking/IT Incident	Network Server
●	Tennessee Orthopaedic Clinics	TN	Healthcare Provider	500	05/19/2023	Hacking/IT Incident	Network Server
●	Marshall Information Services, LLC dba Primary Solutions	OH	Business Associate	7456	05/18/2023	Hacking/IT Incident	Network Server
●	University of Missouri Health Care	MO	Healthcare Provider	736	05/17/2023	Unauthorized Access/Disclosure	Electronic Medical Record
●	Clarke County Hospital	IA	Healthcare Provider	28003	05/17/2023	Hacking/IT Incident	Network Server
●	Fertility Specialists Medical Group	CA	Healthcare Provider	9437	05/15/2023	Hacking/IT Incident	Network Server
●	Lehigh Valley Health Network	PA	Healthcare Provider	627	05/15/2023	Hacking/IT Incident	Network Server
●	R&B Corporation of Virginia d/b/a Credit Control Corporation	VA	Business Associate	345523	05/13/2023	Hacking/IT Incident	Network Server
●	PharMerica Corporation	KY	Healthcare Provider	5815591	05/12/2023	Hacking/IT Incident	Network Server
●	Great Expressions Dental Centers	MI	Healthcare Provider	528	05/12/2023	Hacking/IT Incident	Network Server
●	Sesame, Inc.	NY	Business Associate	1809	05/12/2023	Unauthorized Access/Disclosure	Network Server
●	Illinois Department of Healthcare and Family Services, Illinois Department of Human Services	IL	Health Plan	50839	05/12/2023	Hacking/IT Incident	Network Server

*list of breaches of unsecured protected health information affecting 500 or more individuals.

Data Analysis / The highest frequency of breaches

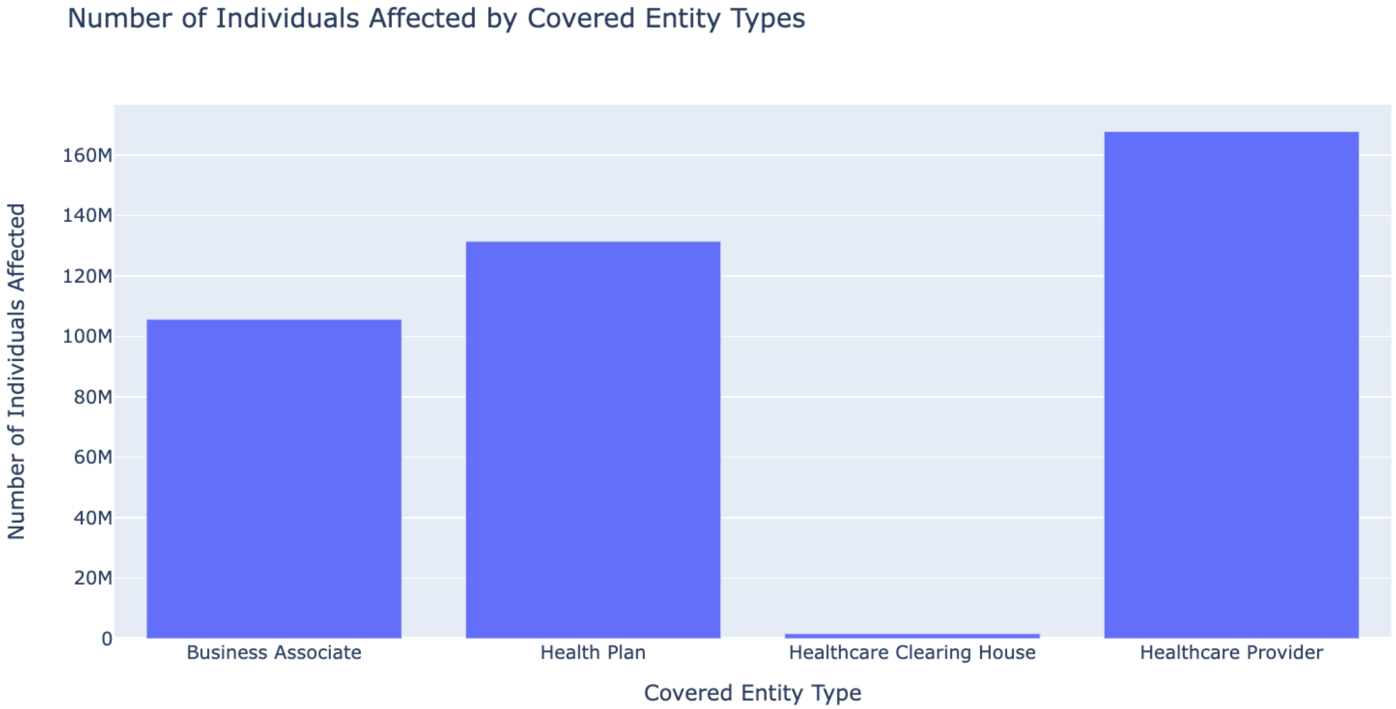




Insights:

- California, Texas, New York, Florida, and Illinois are top 5 regions that require additional cybersecurity measures or regulatory attention.
- Healthcare providers experience a significant number of security breaches, which could potentially impact the privacy and security of patient information.
- Business associates are entities that work with healthcare providers and handle protected health information (PHI) on their behalf. The relatively high count suggests that breaches involving business associates also pose a notable risk to the security of healthcare data.

Data Analysis / Relationship between the number of individuals affected and covered entity types



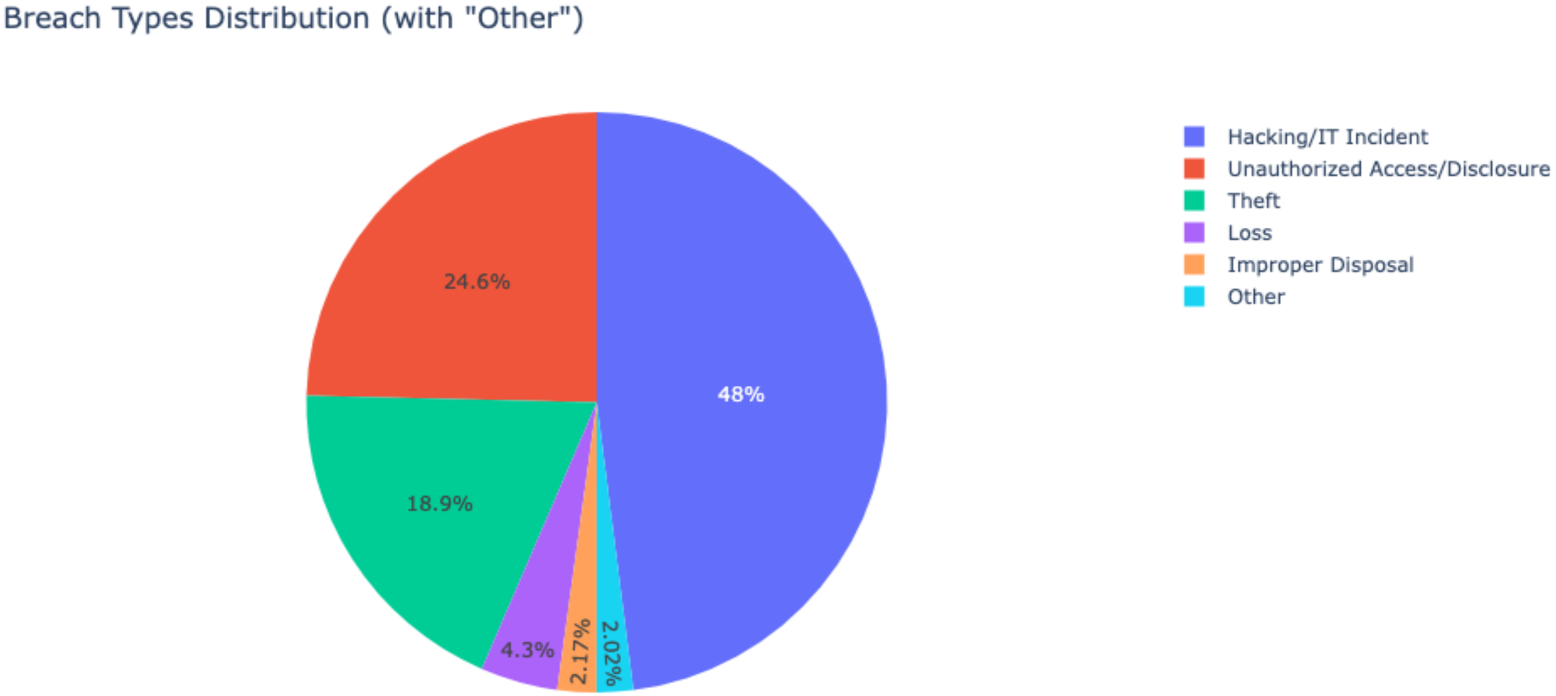
Insights:

- Breaches in healthcare provider organizations have a significant impact on a large number of individuals (167.7 mln). It emphasizes the need for robust security measures, strict access controls, and comprehensive data protection protocols.
- Health Plan entities also have a substantial impact (131.4 mln). This highlights the vulnerability of health insurance providers to breaches.
- Business Associate - 105.65 mln, underscores the need for covered entities to ensure the security and compliance of their business associates to mitigate the risks associated with breaches.

This emphasizes the need for robust security measures, compliance with regulations such as HIPAA, and ongoing efforts to enhance data protection and breach prevention strategies within the healthcare industry.

Collaboration and mutual accountability among covered entities and their business associates are crucial to maintaining the privacy and security of sensitive healthcare data.

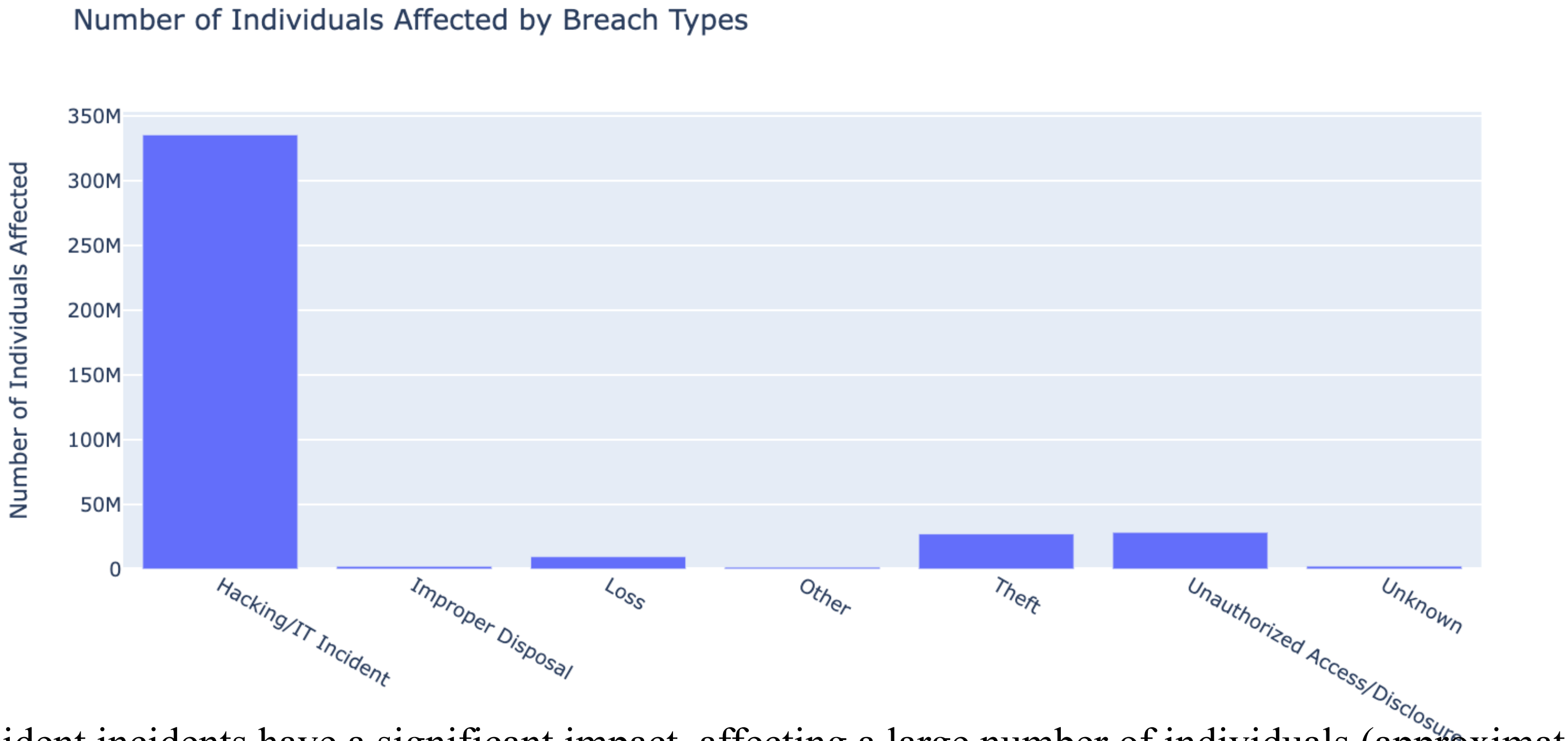
Data Analysis / The distribution of breach types



Insights:

- Hacking/IT Incident is the most common breach type, indicating that unauthorized access, data breaches, or other security incidents involving technology systems are significant concerns.
- Notable risk of individuals gaining unauthorized access to sensitive information or data being disclosed without proper authorization (Unauthorized Access/Disclosure – 24.6%).
- Theft represents a significant portion (18.9%) of the breaches. This indicates the vulnerability of physical assets and the need for comprehensive security measures and proper handling of devices and documents containing sensitive information.

Data Analysis / Relationship between the number of individuals affected and breach types



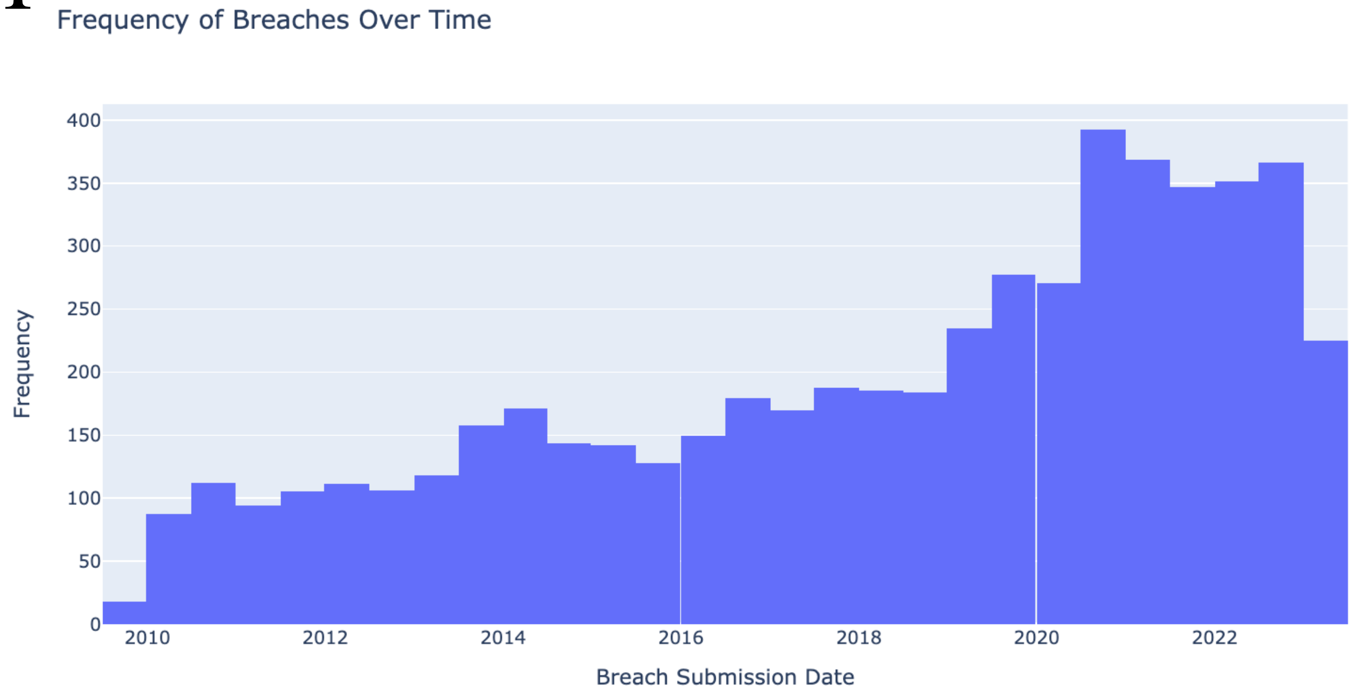
Insights:

- Hacking/IT Incident incidents have a significant impact, affecting a large number of individuals (approximately 335 million). This highlights the prevalence and severity of cybersecurity threats and the need for robust measures to protect sensitive information from unauthorized access.
- Unauthorized Access/Disclosure incidents have a substantial impact (28.3 million) - indicating the importance of implementing strong access controls, authentication mechanisms, and data protection measures.

This analysis of breach type distribution highlights the importance of addressing cybersecurity risks, protecting against unauthorized access, and implementing proper security measures to prevent hacking incidents.

Currently, the system underscores the importance of a multi-faceted approach to security, including robust cybersecurity measures, physical asset protection, proper data disposal practices, and comprehensive employee training on data security and privacy.

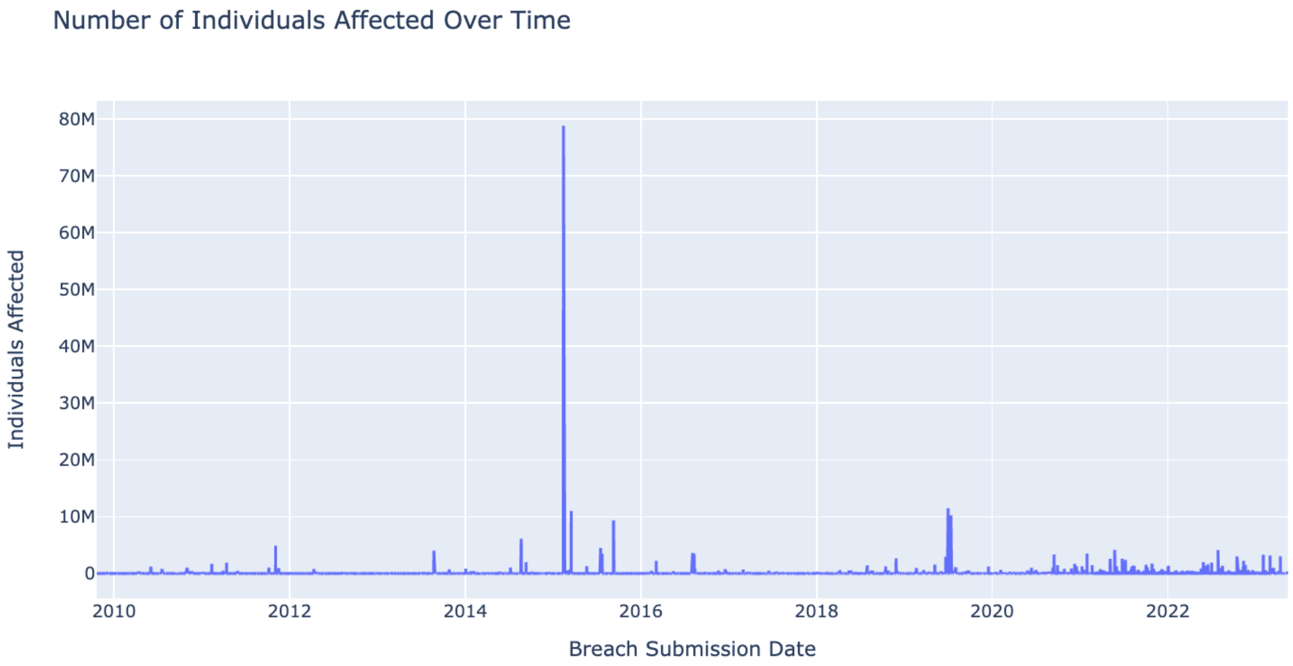
Data Analysis / Frequency of breaches during different periods

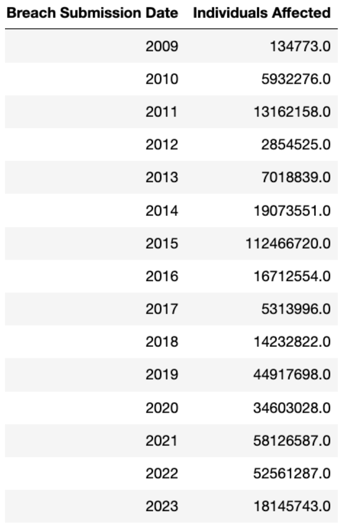


Insights:

- The number of breaches reported during each period fluctuates, indicating variations in the frequency and severity of security incidents over time.
- 2020 witnessed a significant spike in reported breaches. This surge could be attributed to various factors, including the impact of global events such as the COVID-19 pandemic, which created new opportunities for cybercriminals. The increased frequency of breaches in 2020-2023 could also be attributed to heightened awareness and improved reporting practices.
- In 2022 decreased slightly to 718 incidents, indicating a relatively stable level of security incidents compared to the previous year. This highlights the importance of maintaining a proactive and resilient cybersecurity posture.

Data Analysis / Number of affected individuals during different periods





Breach Submission Date	Individuals Affected
2009	134773.0
2010	5932276.0
2011	13162158.0
2012	2854525.0
2013	7018839.0
2014	19073551.0
2015	112466720.0
2016	16712554.0
2017	5313996.0
2018	14232822.0
2019	44917698.0
2020	34603028.0
2021	58126587.0
2022	52561287.0
2023	18145743.0

Insights:

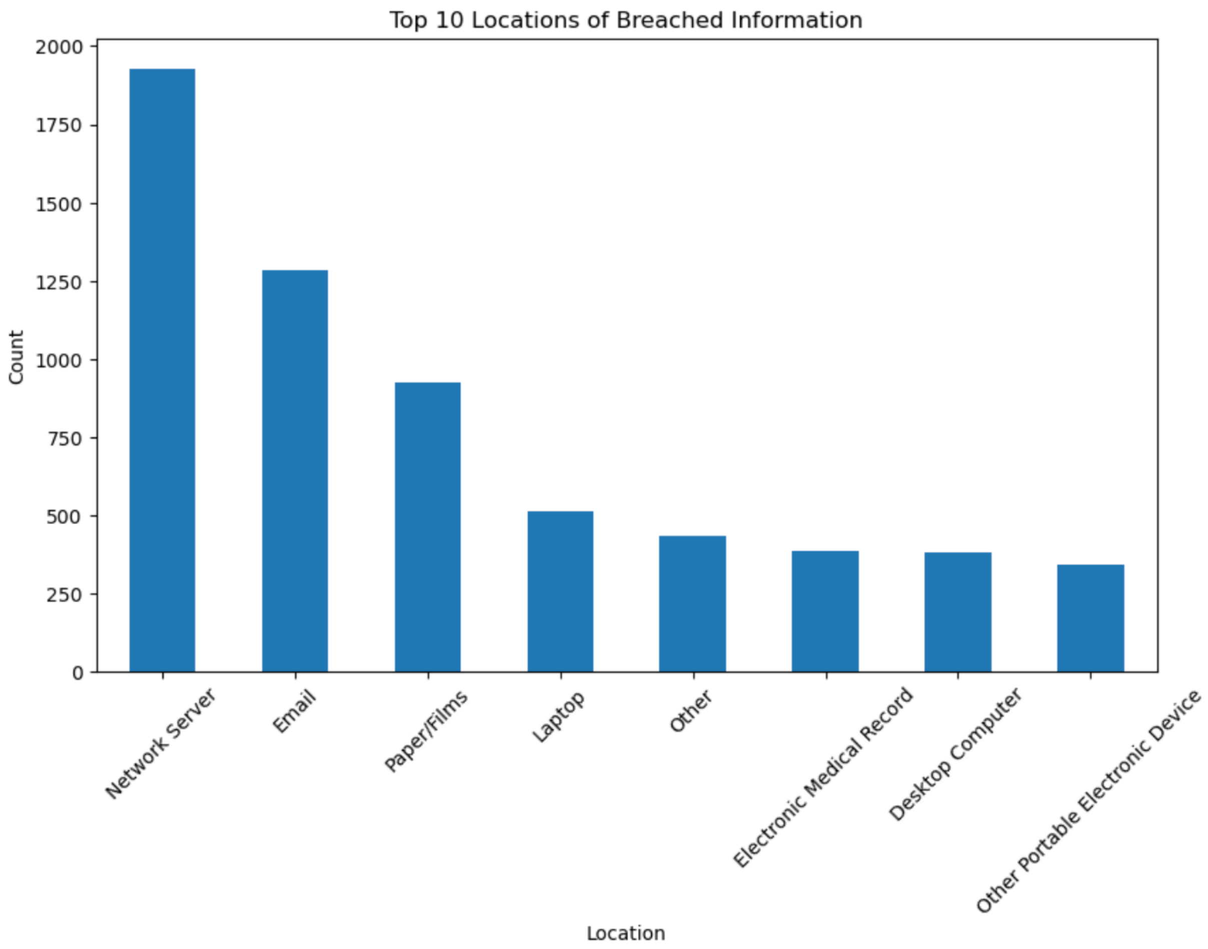
- The number of individuals affected by breaches has been steadily increasing over the years. From 2009 to 2023, there has been a significant rise in the number of affected individuals, indicating the growing impact and scale of security breaches.
- The year 2015 stands out as a particularly significant period, this suggests a major breach on 13.02.2015 Hacking/IT Incident (78.8 mln), series of cyberattacks led to the largest U.S. health data breach in history .
- The years 2020 to 2023 show a mixed pattern in terms of the number of affected individuals. However, in 2022 and 2023, the number of affected individuals decreased again. This fluctuation emphasizes the dynamic nature of breaches and the ongoing efforts required to mitigate their impact.

The data highlights the ongoing and persistent challenge of data security. Emphasizes the increasing frequency and impact of breaches over time, the need for continuous improvement in cybersecurity measures, and the importance of proactive and vigilant approaches to protect individuals' data.

Data Analysis / The location of breached information

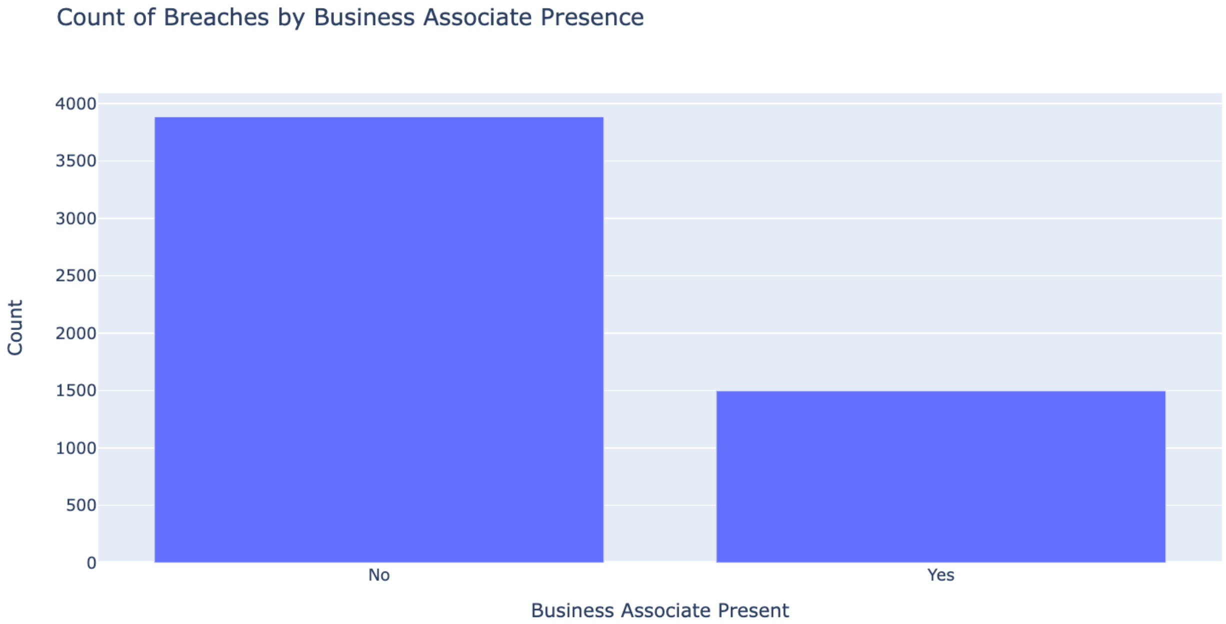
Insights:

- Network servers are frequently targeted for breaches, indicating that they may have vulnerabilities in their security infrastructure or configuration. Strengthening network server security measures is crucial to protect sensitive information.
- Breaches involving email can occur due to phishing attacks, weak passwords, or compromised email accounts. Improving email security practices, including training users on identifying phishing attempts and implementing strong authentication measures, can help mitigate risks.
- The presence of paper/films as a common location for breached information suggests that physical security measures may be lacking.
- Breaches involving laptops and desktop computers may be attributed to stolen or lost devices, malware attacks, or weak security configurations. Implementing full-disk encryption, strong passwords, and remote data wipe capabilities can help mitigate the impact of such breaches.



Chebotarov

Data Analysis / Correlations between breaches and the presence of business associates

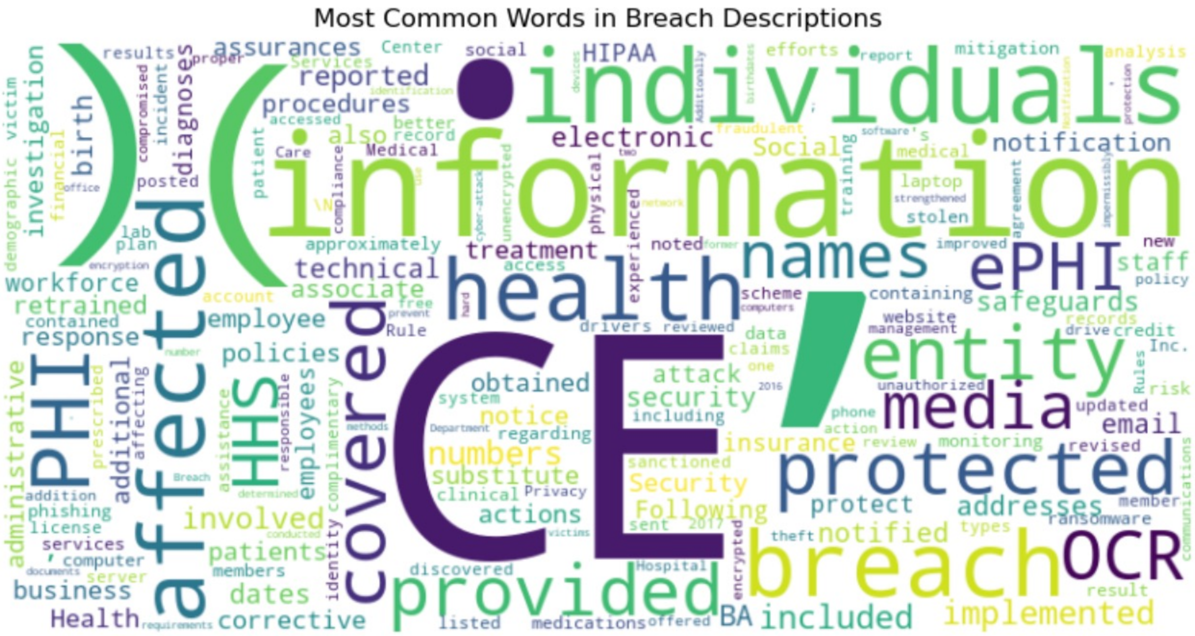


Insights:

This analysis can shed light on the role of business associates in breaches and the need for stricter oversight or contractual obligations.

- Significant number of breaches happened in the absence of a business associate.
- Organizations should pay attention to the management of their relationships with business associates, as breaches can occur regardless of their presence.
- The higher count of breaches in the absence of business associates may indicate that organizations need to be particularly cautious when handling data internally. This includes implementing robust security measures, training employees on data protection best practices, and regularly monitoring and auditing internal systems and processes.

Data Analysis / The textual descriptions of breaches



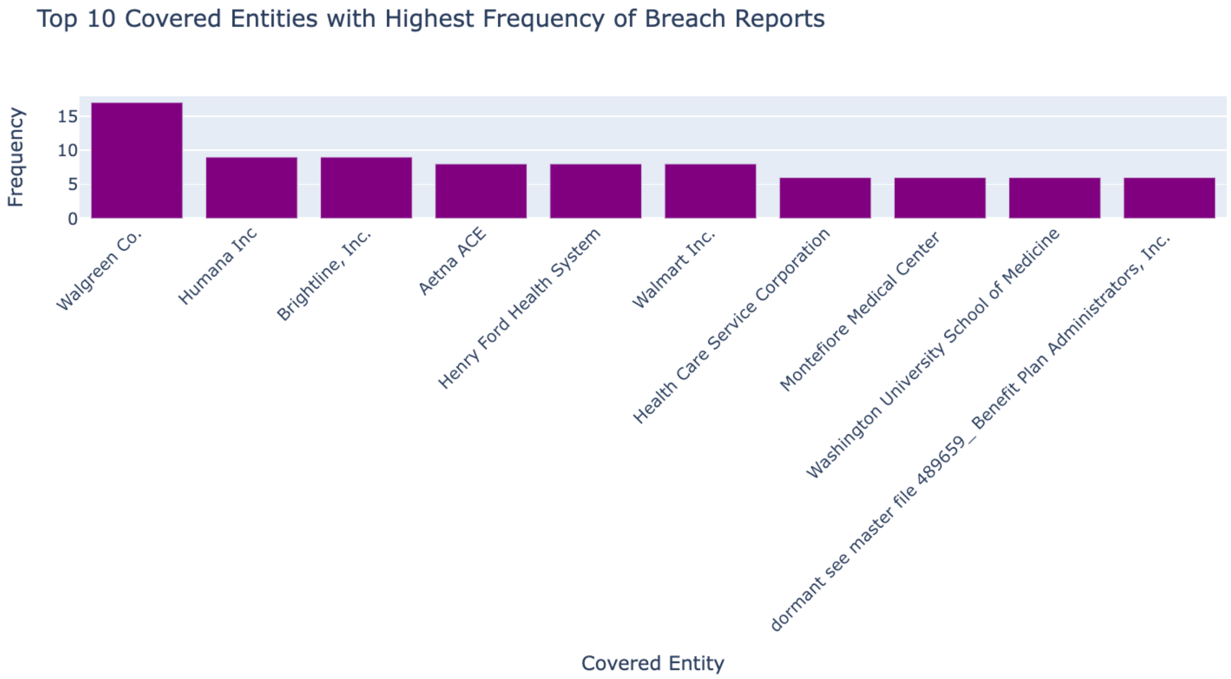
Most Common Words in Breach Descriptions

Insights:

To identify common themes, attack vectors, or recurring patterns. These common words provide insights into various aspects of breaches in the healthcare sector.

- Focus on protecting individuals' information: The frequent occurrence of words like "individuals," "information," and "protected" indicates the importance of safeguarding sensitive data related to individuals' health and personal details.
- Media and electronic breaches: The mention of "media" suggests that breaches may involve the compromise of digital media such as servers or databases containing patient information.
- Protection of PHI: The frequent reference to "PHI" underscores the significance of safeguarding Protected Health Information.
- Involvement of Covered Entities: The presence of words like "CE," "covered entity," and "entity" indicates that breaches often affect organizations or entities that are subject to HIPAA regulations.

Data Analysis / The textual descriptions of breaches



Insights:

Overall, all breach reports occurred in different entities, indicating that multiple organizations experienced security incidents resulting in breaches.

- Walgreen Co. has the highest frequency of breach reports with 17 occurrences. This indicates that the organization has experienced a relatively higher number of security incidents resulting in breaches. It may suggest the need for additional measures to strengthen their cybersecurity defenses and protect sensitive information.
- Humana Inc., Brightline, Inc., Aetna ACE, Henry Ford Health System, Walmart Inc.: These covered entities have reported breaches with a frequency of 9 occurrences each. This suggests that these organizations have also experienced a significant number of breaches and should focus on enhancing their security measures to mitigate future incidents.

What should be done?

1. Implement Robust Cybersecurity Measures: Healthcare organizations should strengthen their cybersecurity measures to protect patient information. This includes regularly updating and patching software systems, utilizing strong encryption, implementing multi-factor authentication, and conducting regular security audits.

2. Enhance Business Associate Oversight: Covered entities should closely manage their relationships with business associates and ensure they have robust security measures in place.

3. Strengthen Physical Security Measures: Organizations should address vulnerabilities related to physical assets, such as paper documents and electronic devices.

4. Foster Collaboration and Mutual Accountability: Covered entities, business associates, and other stakeholders in the healthcare industry should collaborate to maintain the privacy and security of sensitive healthcare data.

Thank you for your attention!

Chebotarov V.
email: hweex7@gmail.com
Linkedin: https://www.linkedin.com/in/halloweex/