AN ANALYSIS OF THE RELATIONSHIP BETWEEN RECENT ELECTRONIC DATA BREACHES AND ENACTED DATA SECURITY AND PRIVACY LEGISLATION IN THE UNITED STATES

by

Christian M. Wilson

Honors Thesis

Appalachian State University

Submitted to the Walker College of Business
and The Honors College
in partial fulfillment of the requirements for the degree of

Bachelor of Science

May 2020

Approved by:

Beverly Dawn Medlin

Beverly Dawn Medlin, Ed.D., Thesis Co-director

Sandra A. Vannoy

Sandra A. Vannoy, Ph.D., Thesis Co-director

Austin Eggers, J.D., Second Reader

Lorilee Medders

Lorilee Medders, Ph.D., Walker College of Business Honors Director

Jefford Vahlbusch, Ph.D., Dean, The Honors College

Abstract

The widescale adoption of electronic records in businesses and organizations has been a boon to entities throughout the world by simplifying the process of collecting, retrieving, and analyzing data. As some of the most prevalent industries in the United States, the industries of healthcare, finance, government, and education in particular make frequent use of electronic data system to increase operational efficiency. The impacts of this digitalization of organizations are not all beneficial, however, as data breaches represent a major threat to information security. Incidents of cyberattacks targeting healthcare, financial, governmental, and educational data are well-documented, and it is clear that the danger remains. Indeed, state and federal agencies regularly enact laws and legislation seeking to combat the rise of data breaches.

Research was conducted in order to compare the occurrences of data breaches with the enactment of state data security and privacy legislation. The methodology used to perform the research largely consisted of collecting press releases and news reports ranging from 2010 to 2019 that announced a data breach incident. All relevant records were then categorized by industry. Likewise, state bills from the same time period were consulted to analyze enacted legislation that pertain to electronic data privacy and security.

The findings of this study indicate that the healthcare industry has been the largest target of data breaches of the past decade, followed by the financial, governmental, and educational industries, respectively. Interestingly, the number of cyberattack trends impacting healthcare and government is shown to have decreased over time while those affecting finance and education has no clear pattern. A comprehensive view of data breaches across the four industries, however, suggest an inverse relationship with the enactment of relevant legislation. Indeed, with some variation, as the number of passed legislation increased over the decade, the number of breaches decreased.

Keywords: Cyberattack, data, data breach, education industry, finance industry, government industry, healthcare industry, legislation, personal information

An Analysis of Recent Electronic Data Breaches and Enacted Data Privacy and Security Legislation in the United States

INTRODUCTION

In the modern age, digitalization has affected virtually all aspects of life. Businesses, homes, vehicles, jobs, and activities are now all enabled or enhanced by technology. Such progress would not be possible without the utilization of big data. Big data, as the name suggests, refers to the sheer amount of data collected and made available. According to Gordon (2014), big data is characterized by five qualities: volume, variety, velocity, value, and veracity. These characteristics present as many challenges as they do solutions. Indeed, properly maintaining data is a daunting task, particularly given the risk of data breaches.

As increasing amounts of data are being stored in electronic formats, new security vulnerabilities have emerged. Much of these vulnerabilities come in the form of data breaches, which now present a major threat to virtually every industry. A data breach can be defined as the prohibited or otherwise unauthorized access to confidential personal data, stored primarily in an electronic format (Sen & Burle, 2015; Solove & Citron, 2017). Items such as names, contact information, Social Security numbers, account credentials, financial records, and health information are all susceptible to data breaches.

In the United States, the healthcare, financial, governmental, and educational industries are among the largest collectors of data in the nation. It seems probable, then, that each industry would be an ideal target of data breaches. In an effort to prevent the occurrence of data breaches and mitigate the potency thereof, many pieces of legislation have been proposed over the years. Such data privacy and security legislation exists on federal, state, and local levels consists of both comprehensive data regulation and regulation of a specific industry. Data breaches and data

laws have thus become the industrial norm, and careful consideration of each is essential for organizational operations. It therefore seems worthwhile to study data breaches, information security laws, and the relationship between the two. The conclusions drawn from this research will allow for a better understanding of the prevalence of data breaches in various industries as well as the associated laws. Additionally, the implications may be used by organizational and governmental entities to better assess the importance of information security.

The study of this topic was conducted by collecting news releases on data breach occurrences in the industries of healthcare, finance, government, and education from 2010 to 2019 in the United States. The quantity of collected incident reports was then grouped by year according to industry in order to better assess data trends. Specifically, the compiled data were analyzed for implications of growth or decline in data breach events over the past decade. Records of relevant state laws and legislation enacted during this time period were likewise gathered from official sources and compared to the number of data breaches occurrences. Pieces of state legislation designed to safeguard personal information, as compiled by the National Conference of State Legislatures, were included in this study, and consist of civil and criminal laws related to the protection of personal information and the notification of data loss incidents. Finally, an analysis was conducted to identify any potentially significant relationship between the quantity of data breaches and the enactment of relevant legislation.

LITERATURE REVIEW

There is a strong concentration of data breaches impacting the industries of healthcare, finance, government, and education. As such, a fair number of studies have been conducted and documented in research literature. In the sections that follow, an overview of current literature detailing data breaches is presented in order to emphasize the prevalence of this issue. Data

security and privacy threats have been an ongoing issue and require a close understanding and analysis.

Healthcare

The healthcare industry is among the largest and most complex in the world, and it is consequently the target of many cyberattacks. The vast amount of personal data collected, stored, and transmitted by healthcare providers are viewed as a goldmine by potential bad actors. Data breaches and related attacks are realistic and increasingly common in this industry. Angst, Block, D'arcy, & Kelley (2017) note that electronic health records (EHRs), due to their low-cost incentives, have been a boon to the quality of the industry. Despite the benefits, however, the widespread practice of storing health records electronically has made this information particularly vulnerable to illegal access and misuse (Bai, Jiang, & Flasher, 2017; Patil & Seshadri, 2014). According to Liu, Musen, and Chou (2015), over 23 million individual health records were affected in targeted breaches between 2010 and 2013.

It is estimated that an average of 18,000 records are breached in any given incident (Khan & Latiful Hoque, 2016). Furthermore, as shown by Huq (2015), the number of data breaches affecting HIPAA-compliant healthcare organizations seems to be rising, particularly from 2005 to 2013. Indeed, Collier (2014) agrees, stating that 2013 saw a 137% healthcare breach increase in just a single year.

Research on HIPAA has shown that the law has had considerable impact on many healthcare institutions. The impact of HITECHA was considerable: according to Collins, Sainato, and Khey (2011), the likelihood of a breach being reported within the healthcare industry increased dramatically from 18.9% in 2009 to 30.8% by the conclusion of 2010. Health information sources that are not protected under HIPAA are also the subject of attacks. Glenn

and Monteith (2014) note that entities such as fitness centers and medical researchers are not necessarily covered by HIPAA; likewise, the majority of mobile applications that collect health information including heart rate are not bound by HIPAA regulations and may not be publicly reported at all. Notable data breaches impacting the healthcare industry have been documented throughout the years. Some of the recent breaches are detailed in Table 1 below.

Table 1

Instances of Healthcare Data Breaches

Date	Entity	Magnitude	Additional Details
06/03/2019	Quest Diagnostics	11,900,000 records	Potentially exposed SSNs, medical information, and financial data
02/04/2015	Anthem	78,800,000 records	Exposed SSNs and other personal information
09/10/2015	Excellus Blue Cross Blue Shield	10,000,000 records	Exposed SSNs and other personal information
08/18/2014	Community Healthcare Systems	4,500,000 patients	Exposed SSNs and other personal information

Note. Individual examples of data breaches targeting the healthcare industry are shown. The announcement date, entity name, incident magnitude, and noteworthy additional details are included for each entry. The data were retrieved from Identity Theft Resource Center (idtheftcenter.org).

As shown in Table 1, vast amounts of records, primarily those belonging to patients, were compromised in each incident. In these events, Quest Diagnostics, Anthem, Excellus Blue Cross Blue Shield, and Community Healthcare System were the victims of targeted attacks, and sensitive data were exposed. The stolen data consisted of Social Security numbers (SSNs), financial or insurance information, and other protected health information (PHI). The existing

research literature therefore clearly demonstrates the severity of data loss affecting the healthcare industry.

Finance

Due to the nature of the financial industry, organizations operating within the sector are often stewards of exceedingly valuable and sensitive consumer information. Credit and debit card numbers, credit scores, and banking information are among the most sensitive pieces of information held by these companies. As a result, account takeovers and other forms of data theft are not uncommon in the industry (Peretti, 2008). It has been observed that large multinational financial entities are often impacted by cybercrime; however, in a study of breaches affecting accounting firms in Maryland, Cheng, Flasher, and Higgins (2019) wrote that the vast majority of firms targeted were relatively smaller in size. The current research thus seems to indicate that data breaches may affect financial organizations regardless of scope. Table 2 contains examples of relatively recent data breaches within the financial industry. The severity of the breach targeting each entity is noted.

Table 2

Instances of Financial Data Breaches

Date	Entity	Magnitude	Additional Details
07/29/2019	Capital One	100,000,000 records	Less than one percent of SSNs were compromised
09/07/2017	Equifax	143,000,000 users	Exposed SSNs, financial data, and other personal information
01/02/2016	TaxSlayer	8,000 users	Exposed account information
10/02/2015	Scottrade	4,600,000 records	Primarily exposed contact information

Note. Individual examples of data breaches targeting the financial industry are shown. The announcement date, entity name, incident magnitude, and noteworthy additional details are

included for each entry. The data were retrieved from Identity Theft Resource Center (idtheftcenter.org).

As shown in Table 2 above, Capital One, Equifax, TaxSlayer, and Scottrade have been targets of cyberattacks, indicating that larger companies operating on national or international levels were frequently targeted over the years. Perhaps due to the largescale nature of these organizations, these events affected a substantial quantity of users and compromised vast amounts of data. In each of these instances, sensitive personal information, including financial records and SSNs, was commonly exposed.

Government

Current literature demonstrate that federal, state, and local governments are plagued by cybercrime. In addition to confidential internal data, the government collects and stores an enormous amount of data on its citizens. Much of this data is personally identifiable information (PII), making the governmental industry another prominent target of data breaches. According to Froomkin (2009), it is estimated that nearly 530 million PII records were breached between 2000 and 2008. It has been emphasized that every United States federal agency has been affected by a data breach at some level, and many incidents were due to the physical theft of electronic devices (Jones, 2007). According to Rhoda (2017), much of the data breaches affecting these agencies target sensitive or even classified government data, presenting a major threat to national security. In 2012 alone, federal governmental agencies reported 22,159 data breaches, representing a major increase from the 15,584 incidents reported in the year prior (Catalano, 2014).

There appears to be a strong correlation between the yearly number of government breaches and the data protection policies enacted. A greater number of policies are implemented following years with many government data breaches (Huq, 2015). Perhaps the most notable policy implemented to secure and protect PII at the federal level is the Federal Information

Security Management Act of 2002 (FISMA). According to Catalano (2014), FISMA sets forth rules and regulations for the prevention and detection of cyberattacks and the required response procedures. Catalano goes on to note that after a major 2006 data breach targeting the United States Department of Veteran's Affairs, an executive order was quickly enacted to establish the Identity Theft Task Force, designed to assist agencies in protecting PII from unauthorized access. The government industry has been the target of many large-scale data breaches over the years. Some of these are documented in Table 3 below.

Table 3

Instances of Government Data Breaches

Date	Entity	Magnitude	Additional Details
11/21/2018	United States Postal Service	60,000,000 users	Exposed account and contact information of usps.com users
02/08/2016	Department of Homeland Security	20,000 employees	Exposed contact information and other personal information
06/17/2015	Office of Personnel Management	21,500,000 records	Exposed personal information of employees
10/19/2018	The U.S. Centers for Medicare & Medicaid Services	93,689 records	Exposed SSNs and other personal information

Note. Individual examples of data breaches targeting the government industry are shown. The announcement date, entity name, incident magnitude, and noteworthy additional details are included for each entry. The data were retrieved from Identity Theft Resource Center (idtheftcenter.org).

As shown in Table 3, the United States Postal Service, the Department of Homeland Security, the Office of Personnel Management, and the United States Centers of Medicare & Medicaid Services, have been targets of data breaches in years past. Personal information is shown to have been especially vulnerable to breaches within government agencies, and large

quantities of contact details were stolen in each incident. The enormous scope of these federal agencies resulted in a substantial quantity of information being compromised per breach.

Education

Prior research literature has closely explored cybercrime in the education industry. As observed by multiple studies, there is a high incidence rate of hacking and data loss within the education sector (Posey & Ncube, 2011; Collins, Sainato, & Khey, 2011). Cybercriminals target educational institutions presumably to obtain student records. According to Tech & Learning (2018), as much as 70% of educational sector cyberattacks have some sort of financial motivation, such as stealing student loan information. Perhaps because of this monetary incentive, Sareel (2006) reports that the educational industry was the single largest target of data breaches in 2005: it is estimated that nearly 46 percent of total breaches targeted the sector that year. In Table 4 below, recent data breach incidents affecting educational industry entities are recorded.

Table 4

Instances of Education Data Breaches

Date	Entity	Magnitude	Additional Details
02/04/2016	University of Central Florida	63,000 users	Exposed SSNs and other personal information
02/26/2016	University of California Berkeley	80,000 users	Exposed financial data and other personal information
02/19/2014	University of Maryland	309,079 users	Exposed SSNs and other personal information
12/17/2010	Ohio State University	760,000 users	Exposed SSNs, financial data, and other personal information

Note. Individual examples of data breaches targeting the education industry are shown. The announcement date, entity name, incident magnitude, and noteworthy additional details are included for each entry. The data were retrieved from Identity Theft Resource Center (idtheftcenter.org).

As shown above in Table 4, local universities, including Central Florida, California Berkley, Maryland, and Ohio State, were impacted by cyberattacks exposing data in recent years. These incidents are relatively small in scale, impacting a fewer number of users per incident when compared to the selected healthcare and financial breaches detailed in Table 1 and Table 2. However, the data breaches targeting the education industry in Table 4 all exposed sensitive personal information, such as SSNs and financial data, and are therefore quite severe.

It is evident that data breaches have been a prominent topic of research throughout the years. Despite the attention, data breaches continue to be a problem even today. For this reason, it seems appropriate to conduct further research on the issue. The contents of the research presented below consist of an analysis of trends in data breaches that have occurred in the United States over the last decade.

RESEARCH METHODOLOGY

The severity of data breaches in the modern age demands additional research. The research described here will be useful in identifying potential patterns among breaches that have occurred in some of United States' largest industries. In order to conduct this research, data were collected from various sources including press releases and news articles detailing breaches impacting organizations within the healthcare, financial, governmental, and educational industries. The data range from 2010 to 2019 and include records of breaches that occurred throughout the United States. Breaches of various severity levels were identified; that said, due

to the nature of the press, it is likely that breaches of greater severity were more commonly reported on than those of lesser severity. Upon compilation, the data were analyzed according to industry in order to detect trends over time and were scaled to a ten-point scale of frequency to better exhibit these trends. As will be shown, a relative frequency rating of ten indicates the year of largest estimated occurrences during the observed timeframe within each industry.

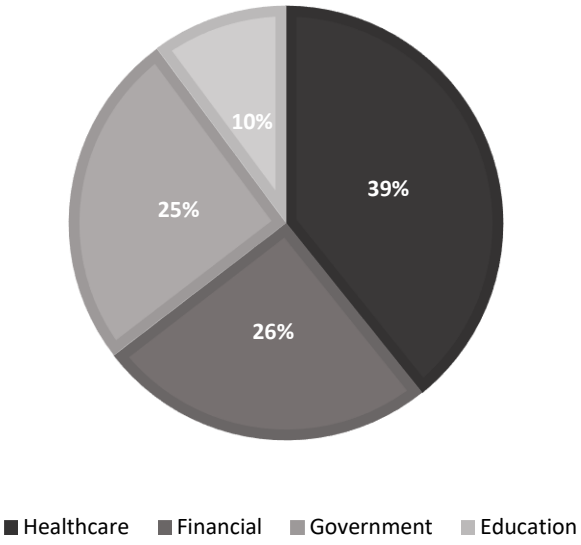
Information on legislation designed to combat data breaches and enacted during the 2010 to 2019 timeframe was likewise collected. Data security and privacy laws enacted in the United States at state levels were of primary focus, and the pieces of legislation studied establish data security standards or expand on existing laws thereof. To obtain the relevant data, records compiling government bills were consulted. The number of data protection laws and legislation passed in the past decade were then analyzed for any potentially significant relationship to data breach frequency.

The sample data consist of news article, press releases, and electronic sources that announced data breach events. The affected organizations or institutions were categorized and recorded by industry. Some individual data breach cases may possess characteristics of multiple industries; in such cases, an incident was recorded for each industry. Ultimately, the sample data were collected to describe the prevalence of data breaches each year, sorted by industry. Although the severity of the breaches was not a discriminatory factor during the data collection process, it seems likely that press sources would have a bias towards reporting more severe data breaches. Indeed, in some circumstances, a severity threshold must be met before an organization is required by law to report on data exposure, resulting in potential underrepresentation of lesser data breach events.

Among the largest industries in the United States are healthcare, finance, government, and education. These industries together represent a significant proportion of total data breaches. The sample data from each of the four industries were analyzed over the aforementioned timespan. As shown in Figure 1, of the four industries studied, healthcare represents the most prominent target of data breaches with 39% of observed breaches affected a healthcare entity. Financial organizations and governmental agencies possess a nearly identical incident rate of 26% and 25%, respectively. The education sector follows with a significantly less frequent rate of only 10%.

Figure 1

Estimated Data Breaches by Industry, 2010 – 2019



Note. The estimated proportion of data breaches affecting each of the observed industries from 2010 to 2019 is shown. These percentages are based on only on data breaches that have occurred in the healthcare, financial, government, and education industries.

These findings may be explained by multiple external factors. Interestingly, the rank of data breach incidents seems to be correlated to the value of the data the industries maintain. The

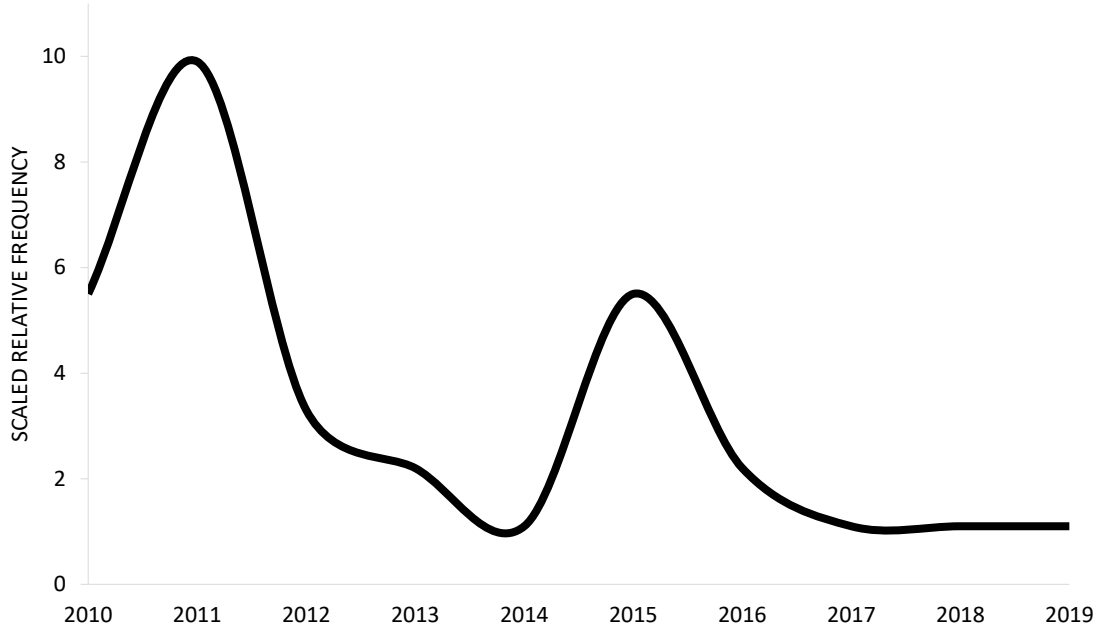
healthcare industry, which is shown to have the greatest number of incidents, is responsible for protecting vast quantities of sensitive data, including electronic protected health information (ePHI), Social Security Numbers (SSNs), and insurance or payment information. Although the financial and governmental industries likewise offer valuable information—such as SSNs, financial records, and, in the case of the government agencies, classified information—the absence of personal health records or ePHI is likely to make them targets of lesser value. The educational industry, enduring a substantially smaller percentage of data breaches, is primarily responsible for storing student records. While SSNs, payment information, and other sensitive data are oftentimes kept by schools and universities, they are not as commonly utilized – SSNs, for instance, may be substituted with student identification numbers. It therefore seems reasonable that educational institutions would be less popular targets. The noted trends may also be due in part to the nature of the reporting process. Incidents involving healthcare organizations are likely to receive a larger public reaction because of the high sensitivity of the stolen data, resulting in increased press attention. Educational data breaches, on the other hand, generally affect a smaller community that is limited to a particular area and therefore may receive less attention.

Healthcare Industry

A trend graph of the number of reported data breaches affecting healthcare organizations is shown to possess a moderate relationship between incident rate and time. Based on the findings in Figure 2, it appears that data breaches within the healthcare industry have largely decreased over the past decade. During the selected time interval, there was a dramatic spike in breach incidents in 2011. Since that time, the frequency has leveled out to a more consistent rate.

Figure 2

Estimated Frequency of Healthcare Data Breaches, 2010 – 2019



Note. The estimated frequency of data breaches in the healthcare industry over time is shown. The number of incidents each year were scaled to better indicate change over time.

The indicated pattern of decrease in data breaches present in the healthcare industry is likely due to the implementation of increased security measures for patient data. It is reasonable to assume that organizations would implement additional protections in years following large numbers of incidents. This may explain why the number of incidents is shown to have decreased significantly following the large spike that occurred in 2011. Increased enforcement of existing laws, particularly HIPAA, may further explain the trend.

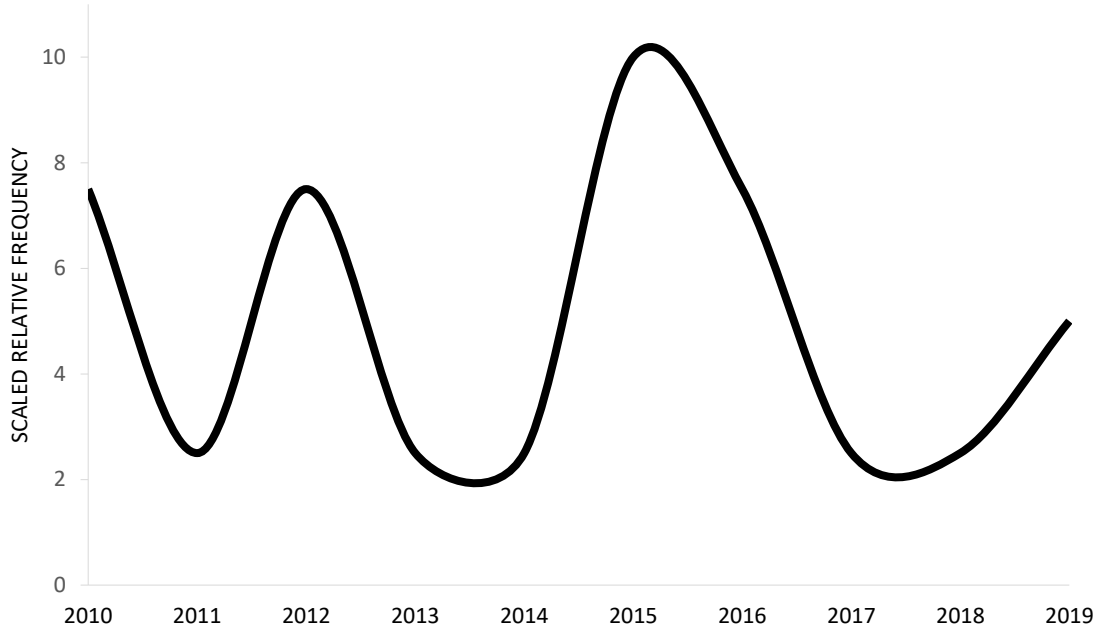
Financial Industry

The findings within the financial industry possess a less significant relationship. Indeed, there appears to be virtually no correlation between the rate of data exposure and time. Instead, an analysis of the data suggests that breach occurrences fluctuate by year—a year of high

incidents is often followed by a year of low incidents, as indicated by Figure 3. The year 2015 represents the most frequent events of unauthorized data exposure, but this rate is only slightly higher than those of other years.

Figure 3

Estimated Frequency of Financial Data Breaches, 2010 – 2019



Note. The estimated frequency of data breaches in the financial industry over time is shown. The number of incidents each year were scaled to better indicate change over time.

Figure 3 indicates no significant trend in data breach occurrences over the observed timeframe within the financial industry. The incidents spikes in 2010, 2012, and 2015 are all immediately followed by years or fewer occurrences. Interestingly, this pattern—or rather lack thereof—cannot be conclusively explained by any particular event. There is no obvious reason for the frequency of financial data breaches to be larger in these years over others. It is therefore likely that the stark changes in incident rates are due to random variation. Perhaps surprisingly,

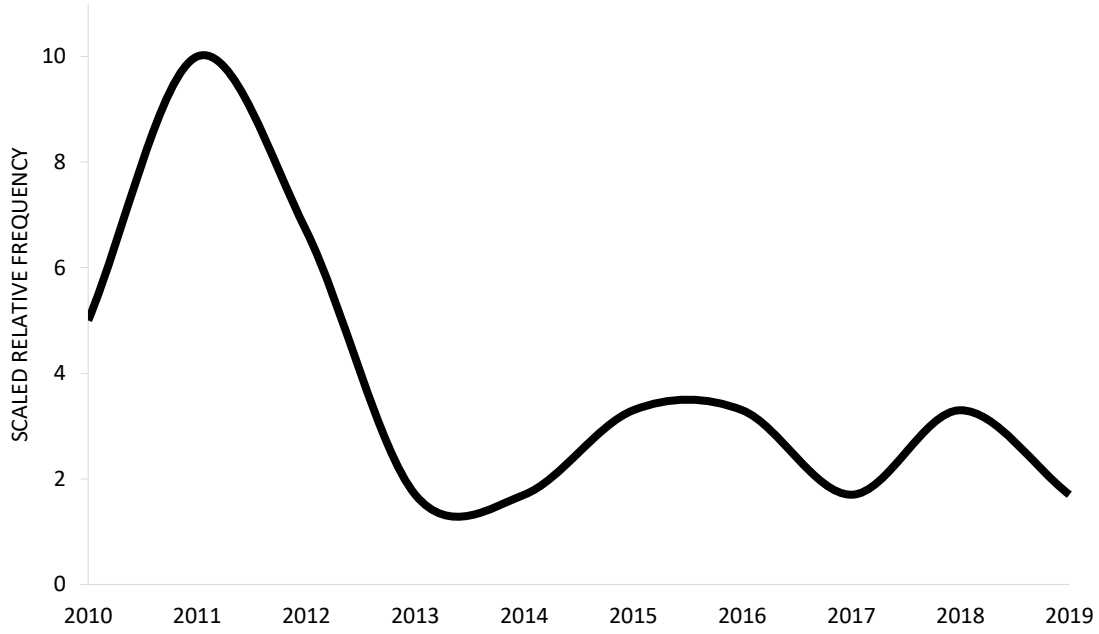
the sudden rise and fall of incidents over the years may indicate that data security legislation has had no significant impact on the reduction of breaches in the industry.

Government Industry

The findings within the government indicate a negative relationship between data breach incidents and time. Like organizations within the healthcare industry, governmental agencies had a clear spike in data exposure during the 2011 year. In the years that follow, the breach rate has fallen significantly, with only minor fluctuation, as seen in Figure 4.

Figure 4

Estimated Frequency of Government Data Breaches, 2010 – 2019



Note. The estimated frequency of data breaches in the government industry over time is shown. The number of incidents each year were scaled to better indicate change over time.

The dramatic decline in estimated data breaches targeting government agencies displayed in Figure 4 may indicate that safeguards were implemented following the major quantity of incidents recorded in 2011. The vast number of breach events in 2011 is consistent with the

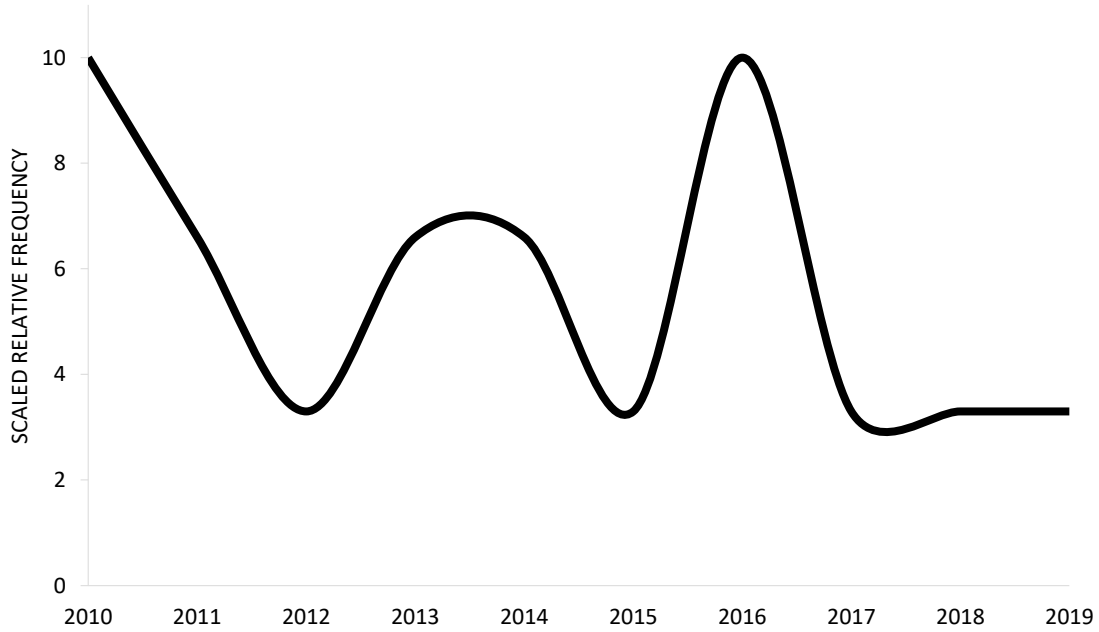
National Conference of State Legislatures' assertion that 2011 is among the worst years for data security breaches (NCSL, 2011). It seems probable that the passing of new laws and legislations, or simply a stricter adherence to existing protocols, would explain the lesser frequency of data security incidents in the years following 2011.

Education Industry

An analysis of the data findings suggests that there is not a strong pattern in data breach incidents over time within the education industry. The rate of breach impact strongly fluctuates by year, and there is no obvious trend. As shown in Figure 5, there is overall pattern of increase or decrease in data breach incidents affecting educational institutions.

Figure 5

Estimated Frequency of Education Data Breaches



Note. The estimated frequency of data breaches in the education industry over time is shown. The number of incidents each year were scaled to better indicate change over time.

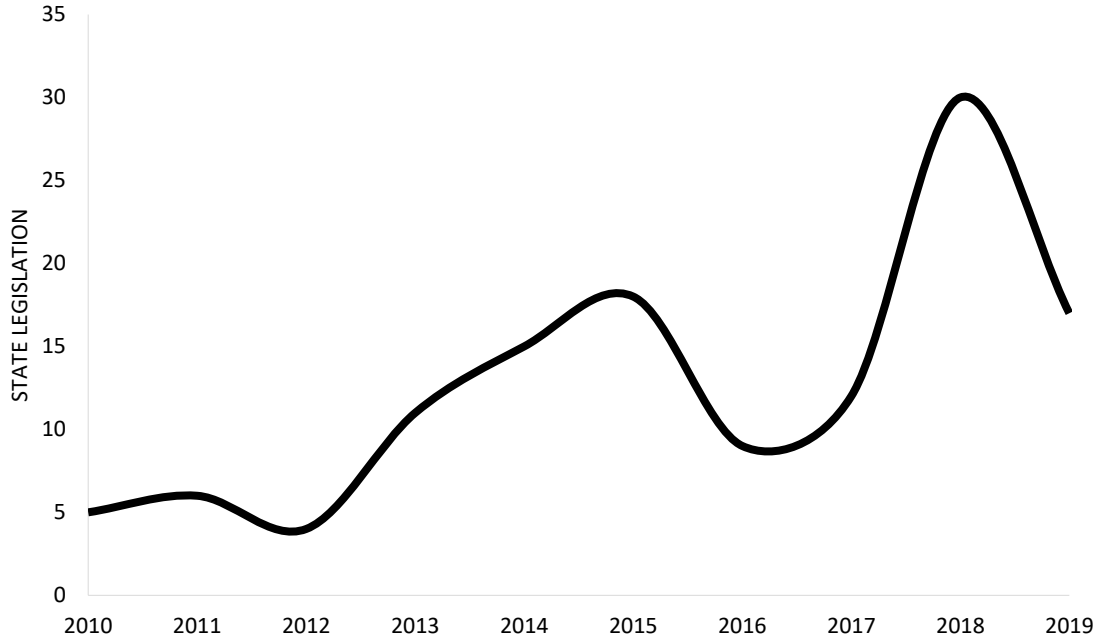
As the financial industry incident frequencies shown earlier in Figure 3, the estimated rate of data breaches in the education industry displayed in Figure 5 is not strongly correlated with time. The fluctuation perhaps indicates only simple variation but may also reflect the inadequacy of enactment or enforcement of data privacy laws. In particular, the spike in breaches in 2016 is a signal that additional protocols are needed to prevent future incidents.

Laws and Legislation

Due to the similarities between data breach incidents and data privacy legislation, it seems worthwhile to compare the two. State laws covering data privacy objectives are regularly enacted. Laws and legislation, both criminal and civil, written with the intention of regulating data privacy standards and breach notification procedures were the focus of this study. Records gathered by the National Conference of State Legislatures were consulted to obtain the data. As shown in Figure 6, the number of state laws enacted across the United States over time possesses a positive relationship—data security legislation enacted each year has increased over time.

Figure 6

Enacted State Legislation Related to Data Privacy and Security, 2010 – 2019

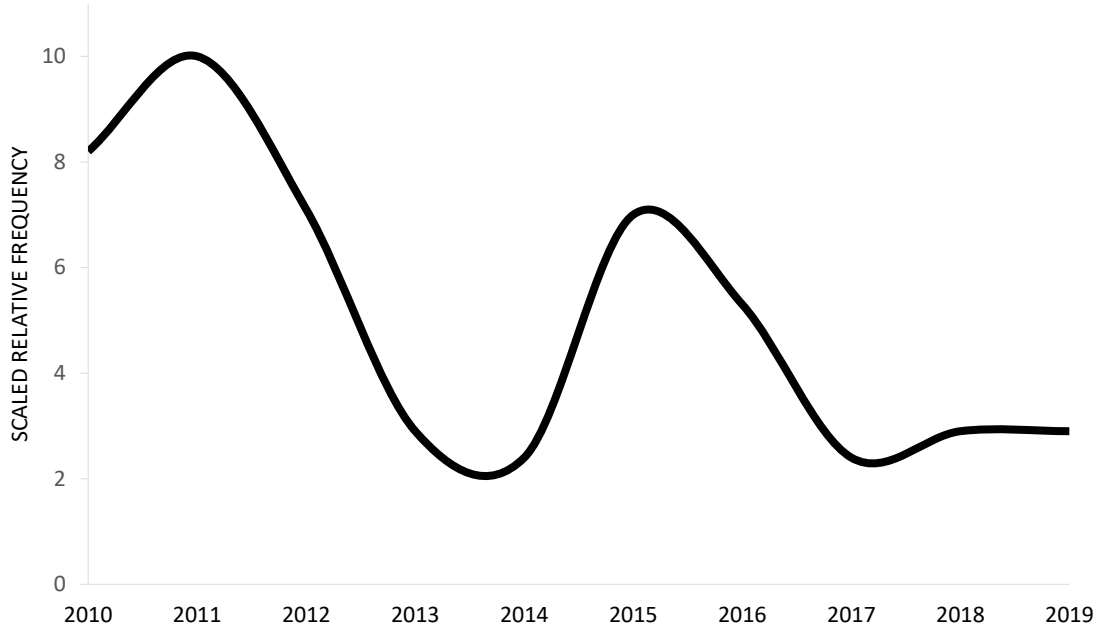


Note. The total number of state laws related to data privacy and security enacted over time across the United States in any of the fifty states is shown. The numbered legislation covers data privacy guidelines, data security standards, and data breach notification requirements. The data were retrieved from the National Conference of State Legislatures (www.ncsl.org).

The upward trend displayed in Figure 6 indicates a steady rise in the enactment of data privacy legislation overtime. There was a large spike in the passing of state legislation in 2018. Although it is difficult to identify a single reason for this dramatic increase, it is reasonable to assume that the publicity of electronic election interference in the 2016 federal election resulted in a sense of urgency to implement responsive measures in the years that follow. Conversely, as seen below in Figure 7, the estimated number of comprehensive data breach incidents affecting each of the four industries studied—healthcare, finance, government, and education—displays, with some fluctuation, an overall decrease in incidents over time.

Figure 7

Estimated Frequency of Comprehensive Data Breaches in the Studied Industries, 2010 – 2019



Note. The combined frequencies of data breach in the healthcare, financial, government, and education industries are shown. The number of incidents each year were scaled to better indicate change over time.

A rough comparison of Figure 6 and Figure 7, even without statistical analysis, make it evident that there is a general inverse relationship between the two data sets. For instance, 2011 is estimated to have had the greatest number of breaches, but only five data security state laws were enacted during that same year. This inverse trend is roughly followed throughout the observed timeframe up to 2019. A multitude of explanations could be offered to explain the suggested correlation. Interestingly, this inverse relationship may indicate that as more data security legislation is passed, fewer data breaches occur.

CONCLUSION and RECOMMENDATIONS

An analysis of findings of the data suggests that there is a moderate inverse relationship between the comprehensive number of electronic data breach incidents in the healthcare, finance, government, and education industries and the quantity of enacted electronic data laws per year over the last decade. The year 2011 was notable for its high rate of data breaches. In the years that followed, the number of incidents has declined, but the number of relevant laws has increased. It therefore seems likely that the enacted legislation at least partially succeeded in combating data exposure. Likewise, it is reasonable to assume that higher incident rates result in legislators feeling increased pressure to pass data privacy and security laws and regulations.

The various incident rates in the healthcare, finance, government, and education industries indicate that data breaches occurrences are not uniform across operational sectors. Instead, each industry possesses a unique set of qualities and characteristics that result in differences in incident levels. It may therefore be beneficial to conduct future data breach research on a single industry. Legislators may likewise consider passing data laws regulating specific industries in order to more efficiently respond to their distinctive needs.

As technology changes over time, so too will the methods used to gain unauthorized or prohibited access to sensitive personal data. It is necessary for legislative bodies across the United States to continue passing and enacting laws that seek to eliminate data breach events. Although it is unrealistic to expect data breaches to cease entirely, legislation provides a means through which incidents rates may be brought to a more acceptable level.

References

Angst, C. M., Block, E. S., D'arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. Mis Quarterly, 41(3), 893-916.

Bai, G., Jiang, J. X., & Flasher, R. (2017). Hospital risk of data breaches. *JAMA internal medicine*, *177*(6), 878-880.

Catalano, M. (2014). Data breaches of personally identifiable information at federal agencies : analyses and lessons. New York: Nova Science Publishers, Inc. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=776119&site=eds-live&scope=site.

Cheng, C., Flasher, R., & Higgins, J. P. (2019). Accounting firm data breaches: One state's records. *Journal of Accountancy*, *227*(6), 1–11. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=ent&AN=136855027&site=eds-live&scope=site.

Collier, R. (2014). US health information breaches up 137%.

Collins, J. D., Sainato, V. A., & Khey, D. N. (2011). Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors. *International Journal of Cyber Criminology*, *5*(1).

Froomkin, A. M. (2009). Government Data Breaches. *Berkeley Tech. LJ*, *24*, 1019.

Glenn, T., & Monteith, S. (2014). Privacy in the digital world: medical and health data outside of HIPAA protections. *Current psychiatry reports*, *16*(11), 494.

Gordon, K. (2014). *Big data: Opportunities and challenges*. Retrieved from https://ebookcentral.proquest.com.

Huq, N. (2005). Follow the data: Analyzing breaches by industry. *Trend micro analysis of privacy rights clearinghouse, 2015*.

Jones, M. E. (2007). Data breaches: Recent developments in the public and private sectors. *ISJLP*, *3*, 555.

Kazim, M., & Zhu, S. Y. (2015). A survey on top security threats in cloud computing.

Khan, S. I., & Latiful Hoque, A. S. M. (2016). Digital Health Data: A Comprehensive Review of Privacy and Security Risks and Some Recommendations. *Computer Science Journal of Moldova*, *24*(2).

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, *19*(6), 321-330.

Liu, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. *Jama*, *313*(14), 1471-1473.

NCSL. (2011, December 21). *Security breach legislation 2011*. NCSL.org. www.ncsl.org/research/telecommunications-and-information-technology/security-breach-legislation-2011.aspx.

Patil, H. K., & Seshadri, R. (2014, June). Big data security and privacy issues in healthcare. In *2014 IEEE international congress on big data* (pp. 762-765). IEEE.

Peretti, K. K. (2008). Data breaches: what the underground world of carding reveals. *Santa Clara Computer & High Tech. LJ*, *25*, 375.

Posey Garrison, C., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, *19*(4), 216-230.

Rhoda, Joseph C. (2017). Data breaches: public sector perspectives. *IT Professional, IT Prof,* (4), 57. https://doi-org.proxy006.nclive.org/10.1109/MITP.2017.265105441

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341.

Solove, D. J., & Citron, D. K. (2017). Risk and anxiety: A theory of data-breach harms. *Tex. L. Rev.*, *96*, 737.

Sraeel, H. (2006). Security: ID Theft Insight: In 2005, data breaches seemed rampant in financial services. But an analysis of public information on 70 data breaches shows the education sector took the biggest hit. Bank Technology News, (4). Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=edsbig&AN=edsbig.A144577994&site=eds-live&scope=site.

Tech & Learning (2018). Report finds increase in data breaches in education and offers tips to help prevent them (10). Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=edsbig&AN=edsbig.A547076292&site=eds-live&scope=site