Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 2, May : 2023

EXAMINE THE EFFECTS OF DATA BREACH AND ORGANIZATIONAL IMPACT: A REVIEW

Dr. Savya Sachi Assistant Professor, Department of Information Technology L. N. Mishra College of Business Management , Muzaffarpur, Bihar : savyasachilnmcbm@gmail.com
Dr. Indu Bhusan Lal Senior assistant Professor, Department of Information Technology, L. N. Mishra College of Business Management , Muzaffarpur, Bihar

Abstract-
This paper examines data breaches that resulted in the loss of more than five hundred million individual records. This demonstrates that data breaches are one of the most common issues for every firm that deals with the public. This demonstrates that data breaches are among the most frequent worries for any commercial organisation that interacts with the public. The type of data breaches has been fast changing as a result. Hacking is one of the main causes of data breaches, however in more recent years, the impact of hacking on data breaches has been lessened as a result of in-depth study on data security and hacker protection. Today, however, employees of the company are the ones responsible for data breaches. The conclusion of our investigation revealed one frightening finding: the application of security measures, which plays a significant role, is directly responsible for data breaches. One concerning finding from our final analysis is that data breaches are directly attributable to the execution of security measures, which plays a critical role. Finally, organisations must create strong security rules and give staff with the necessary and adequate training to enforce these policies.

Keywords— *Data Breaches, Security Measures, Frightening Finding, Investigation Revealed.*

INTRODUCTION

Enterprise operations, including those of businesses and governmental organisations, are seriously threatened by data leakage. A company's long-term stability may suffer as a result of the loss of sensitive information, in addition to suffering severe reputational and financial losses. Information on employees or customers, as well as intellectual property and medical records, is frequently leaked. The average total cost of a data breach has risen to $4 million, per IBM's 2016 Cost of Data Breach Study. Due to the growing digitization of consumer lives and business records, Juniper Research predicts that the yearly cost of data breaches will exceed $2.1 trillion globally by 2019. Numerous significant data loss incidents over the past few years have cost businesses millions of dollars. Target Corporation reported $248 million in losses as a result of a cyberattack in 2013 that resulted in the theft of 40 million payment card numbers and 70 million customers' personally identifiable information. In 2016, Yahoo revealed that a data breach that appeared to have been "state sponsored" in 2014 had resulted in the theft of at least 500 million accounts. The most significant issue for businesses is data breaches, which now cost an average of $4 million per incident (2019), a 12% rise from 2014 to 2019. Previous studies on data breaches have primarily concentrated on two points. They are (i) working to reduce the likelihood of a data breach by paying attention to every employee's behaviour, and (ii) taking into account the effects of data breaches on organisations. This essay examines data breaches that have led to the loss of more than 500 million individual records. This demonstrates that data breaches are among the most frequent worries for any commercial organisation that interacts with the public. As a result, the type of data breaches has been fast changing. Hacking is one of the main causes of data breaches, however in recent years, the impact of hacking on data breaches has been minimised as a result of substantial study on data security and resisting hackers. Today, however, employees of the company are the ones that compromise data.

Organisations must direct their business plans and collaborate with their stakeholders in the core domain of information systems (IS). The availability, integrity, and confidentiality of information systems must be maintained by organisations in order for them to function successfully and earn the trust of stakeholders. It had a significant influence on IS because there were more data breaches. The top concerns for business and IT managers are now those related to information security and confidentiality. Data breaches pose serious problems for all organisations. Any unauthorised access, unintentional disclosure, or leak of confidential information has a negative impact on the organization's reputation. As a result, the company may face fines for failing to comply with regulations and potentially legal action from customers, both of which increase the cost of enhancing security and may even result in a decline in customer confidence. According to a recent poll on data breaches, the average organisational cost of a data breach is $3.9 million (2019), and prices for data breaches are expected to rise. Researchers must therefore look into these concerns and start looking into the challenges associated with data breaches.

LITERATURE REVIEW

This data breach research is largely divided into two categories. The first category addresses problems that may lessen data breaches. Data breaches of this kind cannot be immediately addressed; instead, the causes of potential data breaches are addressed. The goal of this study is to fully understand how data breaches happen so that they can be easily avoided in the future. Employee non-compliance with the security policies set forth by the organisation is the primary cause of the majority of data breaches, according to this research portion. Campbell et al.discovered that organizations had been imposed heavily by fines when they found that private data loss is informed. Hovav & D'Arcy et.al found that the markets had acted differently to the breach warnings based on firm is either a pure e-tailer or not. Cavusoglu et al. report state that, on average, on an average 2.1% of the market share were been lost by the organization’s after they have reported a data breach. Only one exemption to the above studies is the work carried out by Culnan J.J et.al. In this paper, they found two hazardous data breaches at Choice Point and TJX. They opined that organizations while framing organizational privacy guidelines should consider ethical responsibilities. The current work presents findings on several data breaches that occurred between 2005-2019 from different organizations. This paper also deals with the earlier research on the data breaches in two crucial approaches. Firstly, we will consider all the data breaches that have been recorded since 2005, that extensively focus on the data breaches in a particular firm or industry. Secondly, we will discuss the impact of data breaches on publicly traded organizations. Accelerated progress in communication, networks and information technologies is shaping global business, and it is estimated to continue changing business structures for the foreseeable future. This development has many advantages and disadvantages for all organizations’ stakeholders. Information systems management is increasingly considering information security and privacy due to their potential critical issues for all company activities. The magnitude of the importance of breached data was described in the California Data Breach Report 2012-2015 (Harris, 2016) as follows: In the past four years, the Attorney General has received reports on 657 data breaches, affecting a total of over 49 million records of Californians. In 2012, there were 131 breaches, involving 2.6 million records of Californians; in 2015, 178 breaches put over 24 million records at risk. This means that nearly three in five Californians were victims of a data breach in 2015 alone. Multinational companies rely heavily on technology and always have some technical vulnerabilities, which means data breaches and losses are inevitable. Data is one of the company’s most important assets, and the threat of losing data control is becoming an issue that affects everyone. No matter whether companies establish guidelines and controls to mitigate the risk of data breaches, hacking and phishing threats still exist. Information security and privacy is a determining factor for companies’ continuity and sustainability. Companies are adopting several

protection techniques such as system authentication, data encryption, user access control and firewalls as well as practices that aim to minimize such risks such as employee training and user orientation to the company's information security policy and protocols. Despite these measures, perpetrators are becoming more organized and sophisticated, and the risk is growing. There are many recent examples of companies that have suffered from major data breaches Equifax, Anthem, eBay, JPMorgan Chase, Home Depot, Yahoo and Target, among others. Assessing the economic effects of data breaches is a challenge for both accounting and information security management (Schatz and Bashroush, 2016). Research concerning the implications of data breaches is considered an emerging area (Ghosh and Swaminatha, 2001; Spanos and Angelis, 2015, 2016). Event studies have mostly shown that data breaches have a negative effect on cumulative abnormal returns of publicly traded companies. However, these same studies have shown mixed results concerning the significance of the relationship between data breaches and company value/share. Event studies using daily share prices investigate the immediate effect of a breach. Over a longer timeframe, Kannan et al. (2007) found no significant negative effect of information security breaches on company value. In descriptive and comparative studies, Ko and Dorantes (2006) found that sales increased significantly for the breached firms in the fourth quarter after a security breach, contradicting the negative effects shown in most event studies performed using daily share prices. Stoel and Muhanna (2011) found that companies with information technology (IT) weaknesses performed worse than firms with no weaknesses. Data breaches indicate deficiencies in internal control particularly IT internal controls. Companies that are continually improving their IT controls to avoid cyber-incidents can reduce the risk of data breaches. However, hackers' ability to penetrate larger companies' records, such as those of Apple, Walmart and Equifax, indicates that hackers are becoming threats even to companies that invest heavily in IT. Brody et al. (2018) indicate that the potentially harmful effects of malware, which can be financial and nonfinancial, are often not well known.

To contribute to the existing literature, the goal of this article is to analyze the intermediate (quarterly) term effect of data breaches on companies' performance by including qualitative and quantitative factors. Qualitative factors are increasingly being used by researchers in accounting, finance and IT studies (Arnold et al., 2012; Vasarhelyi, 2012; No and Vasarhelyi, 2017). The article aims to verify the effect of data breach announcements on the overall performance of affected companies, as measured by changes in return on assets (ROA) and changes in return on equity (ROE). The study used nonfinancial variables such as the number of records breached and the type of breach. The nonfinancial information was obtained from online databases. The yearly fixed and industry-fixed effects were also incorporated. The financial variables used were ratios related to liquidity, solvency, leverage, book-to-market and capitalization. The Mergent Online database was used to obtain the companies' quarterly financial information.

Other Business organizations (BSO)	Other Business organizations (BSO)	Year
BSO	**603800**	**2005**
BSO	**133680**	**2006**
BSO	**1626947**	**2007**
BSO	**80126200**	**2008**
BSO	**91500**	**2009**

BSO	**200000**	**2010**
BSO	**1521129**	**2011**
BSO	**53267**	**2012**
BSO	**2176422**	**2013**
BSO	**2052330**	**2014**
BSO	**1568600**	**2015**
BSO	**2545563**	**2016**
BSO	**5013143**	**2017**
BSO	**2041500**	**2018**
BSO	**612**	**2019**

Table 1. Data breaches in BSO's

METHODOLOGY

Numerous empirical studies published after 2000 (Campbell et al., 2003; Ettredge and Richardson, 2003; Garg et al., 2003; Hovav and D'Arcy, 2003; Kannan et al., 2007; Gordon et al., 2010) examined how data breaches affect a company's value. Spanos and Angelis (2016) searched the database of empirical research and discovered 37 publications that were related to 45 investigations. The findings demonstrate that 75.6% of the time, data breaches have a major negative impact on the values of businesses. The prior research tended to focus on a small number of metrics, such as corporate and market return and the disclosure of data breaches. More research is required, according to Spanos and Angelis (2016), to understand the broad effects of data breaches on a company's performance, including the implications for sales, revenue, liquidity, solvency, profitability, and sustainability indices.

We have absorbed the idea of content analysis to thoroughly investigate the data breaches that were made public. For example, content analysis is frequently used in information system research to understand the strategic impact of information technology and the importance of e-commerce. To demonstrate the significance of information technology in upholding the organization's strategy, the Chief Executive Officers create and deliver annual reports that are encoded. All types of textual data can be subject to content analysis in order to draw an ideological conclusion about the data. We use this method to data breaches that have been made publically known. All of the data breaches from the Privacy rights clearinghouse are included in the data set. PRC is a nonprofit organisation that has been working since 1992 to bring about positive change and safeguard everyone's right to privacy. We have taken into account the data breaches that have happened in different businesses like BSO. PRC (Privacy Rights Clearing House) has been used to compile the data breaches from 2005 to 2019. Graphs have been created for the tabulated data, which has been organised chronologically by year and according to each entity. We have learned Python programming basics and used the Spyder application to analyse the data. Below is a summary of the findings from the analysis of data breaches. From 2005 to 2019, Table 1 lists the data breaches that occurred in the Other Business Organisations (BSO) category. The cumulative data breaches over the course of a year were taken into account while analysing the total number of data breaches in that industry for the entire year and were plotted accordingly.

(i) Data Collection- Pindado et al. (2008) claim that by including a wide variety of observations in a data collection, panel data enables the reduction of unobservable heterogeneity. Similar to Altman and Sabato (2007), panel data was employed in this study to arrange the data that had been gathered, along with secondary data. Data is gathered in relation to the announcements of data breaches that happened as a result of security flaws, assaults, lost data, thefts, or any other data privacy mismanagement in order to tie the data breaches to firm performance. The writers scan PrivacyRights.org and InformationIsBeautiful.net, two online databases, for announcements. The main data source is PrivacyRights.org, which maintains a database of more than 8,000 occurrences,

the majority of which pertain to governmental bodies, nonprofit organisations, and IJAIM private firms. Identifying significant breaches and validating the substance of data are done using InformationIsBeautiful.net. When there were differences between the announcements, Google Search was used to verify their substance. Companies in the study's sample must have financial reporting both before and after the disclosures of data breaches.

(ii) Data Explanation- According to Stoel and Muhanna (2009), external factors like industry traits affect how well and IT capacity affects a company's performance. The most frequent occurrence of data breaches is in the financial and insurance sectors. Due to the sensitivity of the data kept on file and the potential profit on the black market, this business is a target for hackers. Records of companies in the financial and insurance sectors are also a target. As financial indications for a particular occurrence, such a data breach, we employed financial ratios. The consequences of data breaches on firm performance are assessed using changes in each company's overall performance in Table 2. The indicator (R) is taken into consideration in the quarter of the data breach in order to assess the level of change in a particular ratio as a measure of such consequences.

Year	Frequency	Cumulative frequency	(%)	Cumulative (%)	Total number of breached records
2005	10	10	2.27	2.27	27,934,500
2006	36	46	8.16	10.43	238,602
2007	36	82	8.16	18.59	84,329
2008	19	101	4.31	22.90	24,300
2009	15	116	3.40	26.30	23,829
2010	53	169	12.02	38.32	786,264
2011	37	206	8.39	46.71	2,771,782
2012	41	247	9.30	56.01	50,116,187
2013	43	290	9.75	65.76	36,491,461
2014	65	355	14.74	80.50	155,186,775
2015	30	385	6.80	87.30	90,379,471
2016	27	412	6.12	93.42	32,312
2017	29	441	6.58	100.00	34,086,353
Total	441		100.00		

Table 2. Distribution of data breaches by year

Mean Time	Identify	Contain	Data Breach
2016	201	70	271
2017	191	66	257
2018	197	69	266
2019	206	73	279
2020	207	73	280
2021	212	75	287
2022	207	70	277

Table 3. The mean or average time to identify and contain a data breach

The mean or average time to identify and contain a data breach fell from 287 days in 2021 to 277 days in 2022, a decrease of 10 days or 3.5%. In 2022 it took an average of 207 days to identify the breach and 70 days to contain the breach. In 2021 it took an average of 212 days to identify the breach and 75 days to contain the breach. The 277-day average in 2022 means that if a breach occurred on January 1, it would take until October 4 of that year to identify and contain the breach.

The 277-day average is consistent with the average over the past seven years, with a maximum difference of 11% between the lowest total, 257 days in 2017, and the highest total, 287 days in 2021.

CONCLUSION

The trend analysis suggested that organisations whose security was penetrated underperformed during the quarter in question. This demonstrates that the financial statements and the notes that go with them, which are required information submitted in accordance with generally accepted accounting principles and SEC rules and regulations, are a crucial source of information for all parties involved. Companies' performance can be evaluated based on the information they willingly disclose about cybersecurity events and data breaches. As with many empirical studies, ratio and trend analyses are this study's main area of weakness. Such methods are frequently employed while examining accounting data. They rely on the companies' publicly available financial records, but they are merely proxies for the conditions and realities of the businesses. To report on their financial performance, businesses utilise a variety of accounting treatments, assumptions, and decisions. It is up to the reader to decide whether or not this information is consistent or reliable. Another drawback relates to the confounding events. Although the authors made an effort to pinpoint the significant conflating events that occurred around the periods of the data breaches, this was not sufficient to completely rule out the likelihood that other occurrences did not have an impact on these organisations' financial performance. The authors advise repeating the study when further announcements are made.

Since 2005, we have examined data breaches at various organisations and tracked their effects on the organisational entity. The techniques of machine learning can be used to do additional analysis of data breaches.

REFERENCES

[1] Ahmad, A., Maynard, S.B. and Shanks, G. (2015), “A case analysis of information systems and security
incident responses”, International Journal of Information Management, Vol. 35 No. 6, pp. 717-723.
[2] Altman, E.I. (1968), “Financial ratios, discriminant analysis and the prediction of corporate bankruptcy”, The Journal of Finance, Vol. 23 No. 4, pp. 589-609.
[3] Altman, E.I. and Sabato, G. (2007), “Modelling credit risk for SMEs: evidence from the US market”,
Abacus, Vol. 43 No. 3, pp. 332-357.
[4] Arnold, V., Bedard, J.C., Phillips, J.R. and Sutton, S.G. (2012), “The impact of tagging qualitative
financial information on investor decision making: implications for XBRL”, International Journal of Accounting Information Systems, Vol. 13 No. 1, pp. 2-20.
[5] Ashbaugh-Skaife, H., Collins, D.W. and Kinney, W.R. Jr, (2007), “The discovery and reporting of
internal control deficiencies prior to SOX-mandated audits”, Journal of Accounting and Economics, Vol. 44 Nos 1/2, pp. 166-192.
[6] Baird, D.G. and Morrison, E.R. (2005), “Serial entrepreneurs and small business bankruptcies”, Columbia Law Review, Vol. 105, p. 2310.
[7] Beaver, W.H. (1966), “Financial ratios as predictors of failure”, Journal of Accounting Research, Vol. 4,
pp. 71-111.

[8] Beaver, W.H. (1968), “Market prices, financial ratios, and the prediction of failure”, Journal of Accounting Research, Vol. 6 No. 2, pp. 179-192.
[9] P. R. Clearinghouse. Privacy Rights Clearinghouse’s Chronology of Data Breaches. Accessed: Nov. 2017.
[10] ITR Center. Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center, and CyberScout. Accessed: Nov. 2017.
[11] C. R. Center. Cybersecurity Incidents. Accessed: Nov. 2017.
[12] onernon Institute. "Is Your Company Ready for a Big Data Breach?". The Second Annual Study on Data Breach Preparedness. 2014.
[13] Amudhavel J, Reddy L.S.S. "Effects, challenges, opportunities and analysis on security-based cloud
resource virtualization - 2017." Journal of Advanced Research in Dynamical and Control Systems, Vol. 9,
Special issue 12.
[14] Nalajala S, (2020). Data Security in Cloud Computing Using Three-Factor Authentication. Lecture Notes in Electrical Engineering, Vol.637.
[15] abber B., (2019). A novel sampling approach for balancing the data and providing health care management system by government. International Journal of Advanced Trends in Computer Science and
Engineering, Vol.8, Issue 6.
[16] Beaver, W.H., Correia, M. and McNichols, M.F. (2012), “Do differences in financial reporting attributes impair the predictive ability of financial ratios for bankruptcy?”, Review of Accounting Studies,
Vol. 17 No. 4, pp. 969-1010.
[17] Beaver, W.H., McNichols, M.F. and Rhie, J.-W. (2005), “Have financial statements become less informative? Evidence from the ability of financial ratios to predict bankruptcy”, Review of Accounting Studies, Vol. 10 No. 1, pp. 93-122
[18] Black, K. (2009), Business Statistics: Contemporary Decision Making, John Wiley and Sons, Hoboken, NJ
[19] Bose, R. and Luo, X. (2014), “Investigating security investment impact on firm performance”, International Journal of Accounting and Information Management, Vol. 22 No. 3, pp. 194-208.
[20] Bradford, M. and Florin, J. (2003), “Examining the role of innovation diffusion factors on the implementation success of enterprise resource planning systems”, International Journal of Accounting Information Systems, Vol. 4 No. 3, pp. 205-225.
[21] Brody, R.G., Chang, H.U. and Schoenberg, E.S. (2018), “Malware at its worst: death and destruction”,
International Journal of Accounting and Information Management, Vol. 26 No. 4, pp. 527-540.