ISSN 2347 - 3983
Volume 8. No. 10, October 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter588102020.pdf
https://doi.org/10.30534/ijeter/2020/588102020

Analysis of Data Breaches and Its impact on Organizations

K. Dileep[1], R Venkatesh[2], B Satish Kumar[3], K Umamaheswara Rao[4], D Phanindra Kshatra[5]
[1] KoneruLakshmaiahEducation Foundation, India, dileep.kotte@gmail.com
[2] KoneruLakshmaiah Education Foundation, India, rentalavenkatesh@gmail.com
[3]KoneruLakshmaiah Education Foundation, India, satish.gopi009@gmail.com
[4]KoneruLakshmaiah Education Foundation, India, mahesh550mo@gmail.com
[5]KoneruLakshmaiah Education Foundation, India, kshatra.pd@gmail.com

ABSTRACT

Data breaches are one biggest problem for the companies, costing an average of approximately four million dollars per breach (2019), which has shown an increased rate of 12% from 2014 to 2019. Past research on data breaches have mainly focused on two points. They are: (i) Striving to slash the chance of a data breach by addressing every employee by monitoring his / her behavior (ii) considering the impacts of data breaches on organizations. This paper deals with analyzing data breaches that have resulted in the loss of more than 500 million records of individuals. This proves that data breaches have been one of the most typical concerns for any business organization that deals with the public. From the result, the nature of the data breaches has been transforming rapidly. One of the main reasons for data breach is due to hacking, and in the recent times, the effect of hacking on data breaches has been reduced because of extensive research carried in the area of securing data in resisting to get protected from hacking. But nowadays, a data breach is being done by the persons working in the organization. One alarming result that had been obtained in our end analysis is, the data breaches are directly attributed to the implementation of security policies that accounts crucial role. In the end, the organizations must implement stringent security policies and must provide necessary and sufficient training to enforce these policies on the employees.

Information Systems (IS) is the core domain where organizations must lead their business strategies and mustwork together with their stakeholders. It is the main responsibility of the organizations to preserve the and availability, integrity, and confidentiality of the Information systems to work properly to have the faith of stakeholders towards the organization. It made a huge impact on IS due to the increased number of data breaches. Thus, the issues associated with information security and confidentiality have become the biggest worries for business and IT managers. For any organization, the data infringements are enormous challenges. Any unauthorized access or accidental revelation or leakage of sensitive information results in adverse outcomes to the reputation of the organization. Thus, the business entity can be also imposed fines due to regulatory compliance and may even have legal action from customers, which in turn increases the expenditure for improving security, and may even lead to loss of customer trust. The recent survey on data breaches states that breach of data costs to increase and the typical organizational cost of a data breach is $3.9 million (2019). Thus, researchers need to investigate these problems and start to examine the issues related to data breaches.

Key words : Data breaches, Multivariate Regression, Python, Organizations.

LITERATURE REVIEW OR BACKGROUND

This research allied to data breaches is mainly classified into two types. The first type deals with the issues which will reduce the data breaches. In this type, data breaches cannot be tackled directly; instead, the factors of possible data breaches are addressed. The theme of this research is to clearly understand how data breaches occur, such that data breaches can be easily prevented. In this research part, employees are the main reason for the cause of most of the data breaches and their non-compliance towards the guidelines of security governed by the organization is the main reason [6].

Campbell et al. [10] discovered that organizations had been imposed heavily by fines when they found that private data loss is informed. Hovav & D'Arcy et.al[22]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. [11] 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 [17]. In this study, 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.

METHODOLOGY

In this study, we have imbibed the concept of content analysis to study clearly about the data breaches that were reported publicly. Content analysis is extensively used in information system research, for an instance, to get to know the tactical effect of information technology and the value of e-commerce The reason to do this process is to encode the annual reports generated and delivered by Chief Executive Officers (to stake holders) to realize the importance of information technology in maintaining the organization's strategy [9],[13]. Content analysis is implacable to all kinds of textual data to get an ideological inference about the data. We perform this procedure on data breaches, which were reported publicly. The data chosen comprises all the data breaches from the Privacy rights clearinghouse [1], [5]. PRC is a non-profit organization that protects the privacy of all the individuals and striving for a positive change since 1992.

We have considered the data breaches that occurred in various organizations like BSF, BSO, BSR, EDU, GOV, MED, NGO [12]. The data breaches from 2005-2019 have been taken from PRC (Privacy Rights Clearing House). That data has been tabulated according to each entity, year-wise in chronological order, and graphs have been plotted for the tabulated data [7]. We have Imbibed the programming concepts of python and analyzed the data using the Spyder application [8].

The results after performing the analysis of data breaches have been tabulated below.

Table 1.0 indicates the data breaches in the Other Business organizations (BSO) category from 2005 to 2019. The cumulative data breaches in a year were been considered for analyzing the total data breaches in that sector in the whole year and were plotted respectively.

Table 1. Data breaches in BSO's

Other Business organizations	Total Data Breaches	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

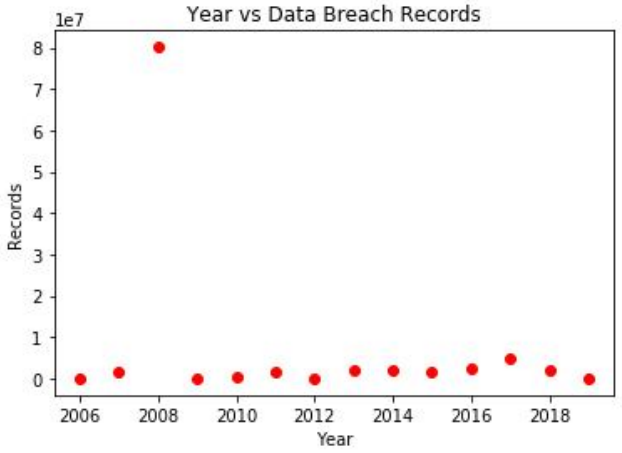

Figure 1. Data breaches inOther Business organizations (BSO) from 2005 to 2019

Table 2.0 depicts the data breaches in the Business Retail/Merchant entities (BSR) category from 2005 to 2019. The cumulative data breaches in a year were been considered for analyzing the total data breaches in that sector in the whole year and were plotted respectively.

Table 2. Data breaches in BSR's

Business Retail/Merchant entities	Total Data Breaches	Year
BSR	1400	2005
BSR	539903	2006
BSR	12037	2007
BSR	69436	2008
BSR	1140	2009
BSR	71049	2010
BSR	502842	2011
BSR	1452726	2012
BSR	42602228	2013
BSR	2361900	2014
BSR	3100	2015
BSR	2540855	2017
BSR	18202589	2018

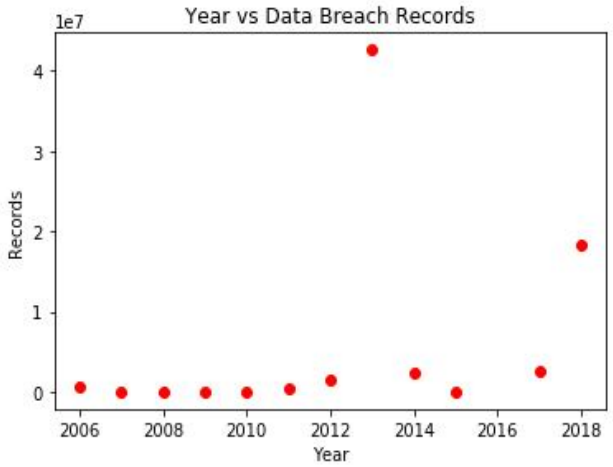

Figure 2. Data breaches in Business Retail/Merchant entities from 2005 to 2019

Table 3.0 depicts the data breaches in the Business Financial and Insurance Services (BSF) category from 2005 to 2019. The cumulative data breaches in a year were been considered for analyzing the total data breaches in that sector in the whole year and were plotted respectively

Table 3. Data breaches in BSF

Business Financial and Insurance Services (BSF)	Total Data Breaches	Year
BSF	48898573	2005
BSF	24923909	2006
BSF	33763562	2007
BSF	36457891	2008
BSF	13500008	2009
BSF	5852742	2010
BSF	593208	2011
BSF	8667164	2012
BSF	1830281	2013
BSF	76698887	2014
BSF	12200008	2015
BSF	1009897	2016
BSF	1470008	2017
BSF	1765210	2018

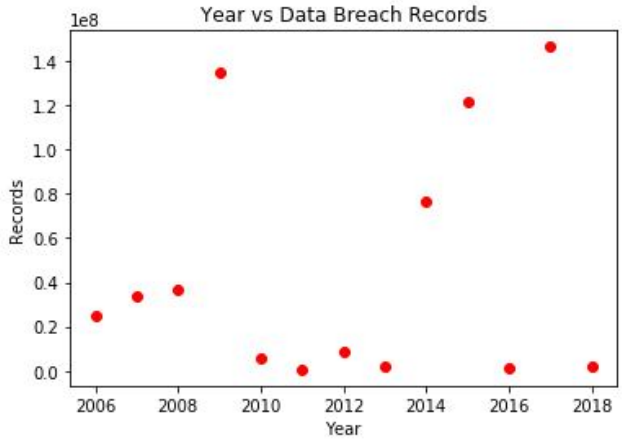

Figure 3.Data breaches in Business Financial and Insurance Services (BSF) from 2005 to 2019

Table 4.0 depicts the data breaches in the Educational Organizations (EDU) category from 2005 to 2019. The cumulative data breaches in a year were been considered for analyzing the total data breaches in that sector in the whole year and were plotted respectively.

Table 4. Data breaches in EDU's

Educational Organizations	Total Data Breaches	Year
EDU	555200	2005
EDU	187709	2006
EDU	187462	2007
EDU	119779	2008
EDU	176627	2009
EDU	115753	2010
EDU	189190	2011
EDU	735618	2012
EDU	134220	2013
EDU	1257200	2014
EDU	23000	2015
EDU	6100	2016
EDU	42980	2017
EDU	40053180	2018

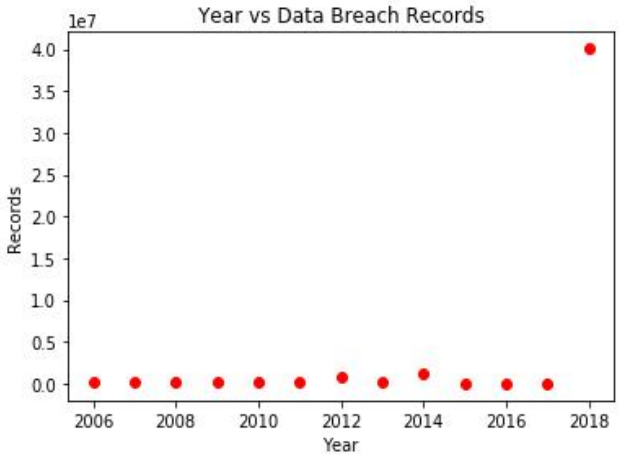

Figure 4. Data breaches in Educational Organizations (EDU) from 2005 to 2019

Table.5: This table depicts the data breaches in the Government Organizations (Gov) category from 2005 to 2019. The cumulative data breaches in a year were been considered for analyzing the total data breaches in that sector in the whole year and were plotted respectively.

Table 5. Data breaches in GOV's

Government Organizations (Gov)	Total Data Breaches	Year
GOV	522900	2005
GOV	3058530	2006
GOV	1857000	2007
GOV	374364	2008
GOV	77095475	2009
GOV	514840	2010
GOV	68311	2011
GOV	344671	2012
GOV	1225875	2013
GOV	2075730	2014
GOV	50018	2015
GOV	6919143	2016
GOV	139357	2017
GOV	500	2018

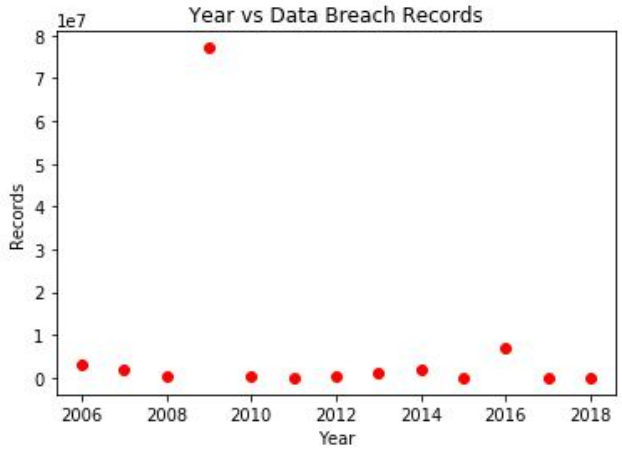

Figure 5. Data breaches in Government Organizations since 2005 to 2019

Table 6.0depicts the data breaches in the Medical Organizations (MED) category from 2005 to 2019. The cumulative data breaches in a year were been considered for analyzing the total data breaches in that sector in the whole year and were plotted respectively.

Table 6. Data breaches in MED's

Medical Organizations (MED)	Total Data Breaches	Year
MED	37740	2005
MED	102099	2006
MED	801988	2007
MED	490284	2008
MED	1713850	2009
MED	510095	2010
MED	4216154	2011
MED	641689	2012
MED	928328	2013
MED	2243739	2014
MED	26452480	2015
MED	875199	2016
MED	1046296	2017
MED	181500	2018
MED	364995	2019

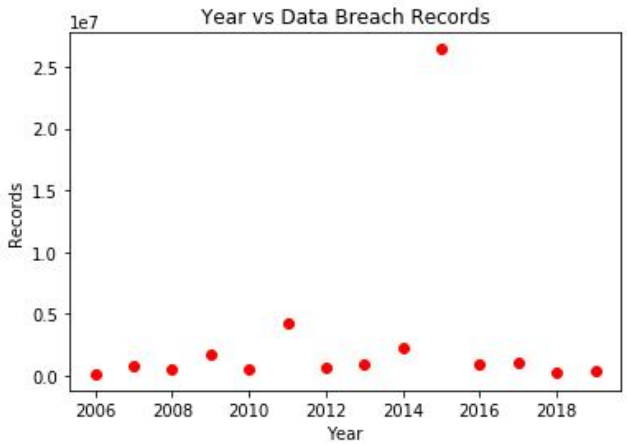

Figure 6. Data breaches in Medical Organizations from 2005 to 2019

Table 7.0 depicts the data breaches in the Non-Profit Organizations (NGO) category from 2005 to 2019. The cumulative data breaches in a year were been considered for analyzing the total data breaches in that sector in the whole year and were plotted respectively

Table 7. Data breaches in NGO's

Non-Profit Organizations (NGO)	Total Data Breaches	Year
NGO	15000	2005
NGO	1036176	2006
NGO	86845	2007
NGO	207170	2008
NGO	20360	2009
NGO	12250	2010
NGO	17352	2011
NGO	16355	2012
NGO	4000	2013
NGO	1	2017

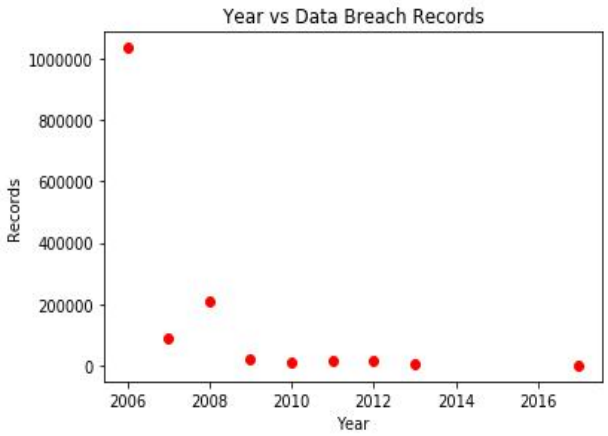

Figure 7. Data breaches in Non-Profit Organizations from 2005 to 2019

CONCLUSION

We have analyzed data breaches on several organizations and have observed the impact of data breaches on the organization entity since 2005 to till date. Further analysis of data breaches can be carried out using machine learning concepts. We can analyze the data breaches with the help of the Support Vector Machine (SVM) algorithm and can classify the rate of data breaches impacts on organizations.

REFERENCES

1. P. R. Clearinghouse. Privacy Rights Clearinghouse's Chronology of Data Breaches. Accessed: Nov. 2017. [Online]. Retrieved from https://www.privacyrights.org/data-breaches
2. ITR Center. Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center, and CyberScout. Accessed: Nov. 2017. [Online]. Retrieved fromhttp://www.idtheftcenter.org/2016databreaches.html
3. C. R. Center. Cybersecurity Incidents. Accessed: Nov. 2017. [Online]. Retrieved fromhttps://www.opm.gov/cybersecurity/cybersecurity-incidents
4. Ponernon Institute. "Is Your Company Ready for a Big Data Breach?". The Second Annual Study on Data Breach Preparedness. 2014. [Online]. Retrieved from http://www.experian. com/assets/ data - breachlbrochures!20 I4-ponemon2nd-annual-preparedness.pdf
5. 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.
6. Nalajala S, (2020). Data Security in Cloud Computing Using Three-Factor Authentication. Lecture Notes in Electrical Engineering, Vol.637.
7. Jabber 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.
8. Vijaya Chandra J (2019). Authentication and authorization mechanism for cloud security, International Journal of Engineering and Advanced Technology, vol.8, Issue 6.
9. Gurajada L.B.,Security attacks in wireless sensor networks (2018). International Journal of Engineering and Technology Vol.7, Speciall Issue 32.
10. Campbell, K., Gordon, L. A, Loeb, M.P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer Security, 11, 431--448.

11. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(I) 69-104.
12. Reddy V.J (2020) Mining regular patterns in cloud databases. Test Engineering and Management, Vol.83.
13. Chintala R.R(2019). FPGA implementation of Katan block cipher for security in wireless sensor networks, International Journal of Emerging Trends in Engineering Research 7(11).
14. Crabtree, B. F., & Miller, W. F. (1992). Doing qualitative research. Newbury Park, CA: Sage Publications,
15. Creswell, J. W. (2007). Qualitative inquiry and research design: Choosing among five approaches. Thousand Oaks, CA: Sage Publications.
16. Creswell, J. W. (2005). Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Upper Saddle River, NJ: Pearson Education.
17. Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. MIS Quarterly, 33(4), 673-687.
18. Doyle, K. (2009). Information security in health care - four critical errors. Retrieved from http://www.itworld.comlsecurity/68838/information-security-health-care-fourcritical-errors
19. Experian (2012). Healthcare breaches and fraud are here to stay. Retrieved from http://www.experian.comlblogs/data-breach/2012/05/15/healthcare-breaches-fraudare-here-to-stayl
20. Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. Risk Management and Insurance Review, 13(1), 61-83.
21. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. European Journal of Information Systems, 18(2), 106-125.
22. Hovav, A. & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms, Risk Management and Insurance Review, 6(2),97-121.
23. Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization, European Journal of Information Systems, 18(2), 140-150.
24. ISACA. (2008). Top business/technology issues survey results. Retrieved from http://www.isaca.orglKnowledge-Center/Pages/Top-Business-Technology-IssuesSurvey-Results.aspx
25. ISMG. (2011). Healthcare information security today. Retrieved from http://www.healthcareinfosecurity.comlp-his-survey-2011.