International Journal of Data Informatics and Intelligent computing (IJDIIC)
Vol. 1, No. 2, December 2022, pp. 51~57
DOI: 10.59461/ijdiic.v1i2.31

Data Breach – Its Effects on Industry

Manju Bargavi[1], M.Senbagavalli[2], Tejashwini.K.R[3], Tejashvar.K.R[3]
[1]School of Computer Science & Information Technology, Jain Deemed-to-be University, Bengaluru, India
[2]Department of Information Technology, Alliance College of Engineering and Design ,Alliance University, Bengaluru, India
[3]B.Tech, Computer Science & Engineering, Christ Deemed-to-be University, Bengaluru, India

Article Info

Article history:

Received November 05, 2022
Revised December 16, 2022
Accepted December 20, 2022

Keywords:

Attack
Data Breach
Data Leakage
Security
Hacking

ABSTRACT

In this Digital world, Data has become one of the most crucial parts in every field. To protect this sensitive piece of information many methods and technologies are coming into existence. A data breach reveals sensitive, protected and confidential information to an unauthorized person. Increasingly opportunities exist for information to leak out as our computers and mobile devices become more associated. Data leaks pose a serious threat to companies and can cost them significantly either financially and reputationally. The long-term effects of a data breach can spread throughout a company, having an effect on all parties involved, including the user base, staff, and cybersecurity teams in charge of repair. By giving priority to the most frequently attacked industries, this article will advance understanding about data hacking incidents and aid in securing corporate data.

Corresponding Author:

Manju Bargavi
School of Computer Science & Information Technology
Jain Deemed-to-be University
Bengaluru
India
Email: cloudbargavi@gmail.com

1. INTRODUCTION

Data leakage is a significantissue when it comes to reputation and financial loss of an organization. The alternative name for data breach is data spill or Data leakage or Information leakage. The average consolidated cost of a data breach has reportedly surpassed 4 million dollars, according to the Cost of Data Breach Study of IBMs in the year 2016. According to a Juniper Research prediction2, the yearly cost of data breaches would exceed 2.1 trillion dollars globally by 2019 as a result of the quick digitization of client lives and business records. Over the past few years, there has been lot of data loss due to security issues which have costed the companies in million dollars. As many upcoming new technologies are being used without testing data breaches tend to continue. Some users take abrupt disadvantage of the sources and conveniences being provided. Without comprehensive security features, users are guaranteed to be at risk for many reasons. The data breach process is classified into four stages namely research, attack, social or network attack and Ex-filtration.

To do data breach research, one must identify system ambiguities. Here, the hacker looks for a system flaw or ambiguity that will allow it to target a specific group of data. The attack stage is crucial because the intruder wants to establish cordial contact with the victim so that they do not have any doubts regarding the likelihood of a data breach. The second stage could also be split up into social and network attacks. The first type of attack happens when a hacker tries to break into a system, network, or institution using organizational weaknesses, and the second type of attack involves deceiving people either by earning their trust up front or indirectly by granting them access to the network of the organization. Ex-filtration is the final step in this process of data leak. Here, a hacker can simply access secret and sensitive information and use it for their own purposes.

Some of the common ways to prevent data breach as given below:

- maintaining only pertinent data on the network
- Instruct users
- maintain the password protected
- safeguarding data
- use licensed and updated software
- use only private network by avoiding public network
- dispose unused data

2. RELATED WORK

Security architecture for data breaches is included here for better understanding in Figure 1 which will depict the security. A security architecture is a comprehensive security design that identifies the locations where security controls should be used and solves the requirements (such as authentication, authorisation, etc.) and dangers specific to a certain environment or situation. The design procedure ought to be repeatable. It is possible to apply security architecture at the enterprise, application, and product levels. Typically, product security architecture will focus on the security features of that specific product. Applications, infrastructure, and processes must all be taken into account in the enterprise security architecture, along with security management and operations. Application design addresses both the additional (compensating) controls needed outside of the application as well as the security offered within the application. Relationships & Dependencies are the main Security Architecture Properties. The main Properties of Security Architecture are Relationships & Dependencies.

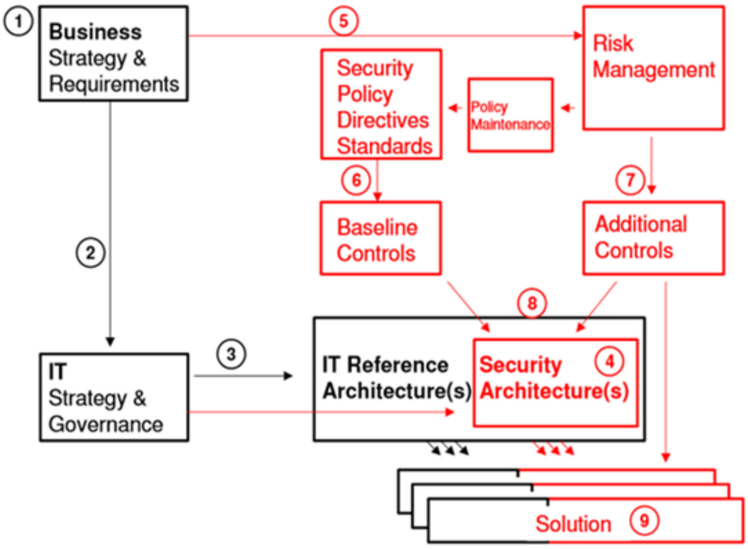

Fig.ure 1. Security Architecture

The following ideas are supposed to be illustrated by the diagram, starting in the top-left corner:

- Business strategy and requirements should be taken into consideration when designing security architecture.
- The IT strategy ought to be a reaction to the needs and requirements of the business.
- In response to the IT Strategy and governance, the IT Reference Architecture(s) should be developed. Usually, the reference architecture will cover several platforms.
- Even if it is published as a distinct document, the Reference Security Architecture(s)
- The Business strategy and requirements serve as the foundation for the IT Security Risk Management approach and criteria.

- Based on the security policy, directives, standards, etc., a set of baseline controls is created. We refer to baseline controls as the organization's mandatory minimum criteria. Benchmarking, documented security "good practise," the legal and regulatory framework, and other sources all contribute.
- The risk management approach leads to the development of additional controls.
- The foundational and supplementary security rules are embodied in the security architecture. It can also be defined to cover the risk management process as well as the rules, regulations, and standards.

The proposed system focuses on analyzing the effects of data breaches and overall performance of his company. Approach and methodology is important to steal any information from online database or from users. Variables linked to liquidity, profitability, solvency, firm size, and financial performance analysis were used to determine the type and extent of the data breach. Multiple regression analyses were performed on the data[1]. Cybercrime prosecutions are rare[2]. Cooperation between federal law enforcement agencies and their overseas colleagues on prosecution, investigation, and extradition of data breaches is challenging. Criminal hackers have benefited from using regulatory arbitrage to maximize their profits. For years, governments have tried to create information security management systems. Even though the increasing data breach vulnerabilities, user know slightly about how companies effectively detect and handle data breach incidents. Risk management theory has been used for a literature study to construct data breach risks and solutions. There are three categories of data breach risks that is cause, locus, and impact as well as three types of data breach resolutions like prevention, containment, and recovery [3][12]. When examining quarterly fluctuations in share prices, the study finds no evidence of a connection between data breaches and stock market response. The study's primary analytical flaw is its use of trend and ratio data. Such methods are frequently employed while examining accounting data[4][5]. Though they do not reveal any sensitive information regarding the company and their financial profits and losses. Another limitation concerns the confounding factors. Because of the nature of such events, this study requires specific information for case studies of the companies. Positive binomial and Poisson models showed promise and were able to accurately forecast data breach incidences [6][7]. This study highlights a fascinating but under-researched advantage of corporate diversity that has to do with information security. This study emphasizes the important bearing of organizations' operational structure on information security for working professionals [8]. The findings show that longer-maturity cyber insurance contracts are more economical. The main contributions of this research are a thorough examination, parameter calculation, and use of the MMNPP to model cyber hazards [9][13]. Data breach recovery has just recently become the subject of IS research. Prior studies have frequently concentrated on preventative privacy and security solutions to data breaches[11]. The framework may assist firms in preparing to include data privacy and security management features in their data breach notifications. Stakeholder management aims to suggest tactics for addressing the impacts of the stakeholders[14]. The stakeholder management stage, which comes after the stakeholder identification stage[15], is rooted in strategic management research and involves the creation of efficient plans of action.This could help businesses manage their ethical and legal obligations to account for their activities in maintaining the security and privacy of the personal data they hold [10].

3. WORKING METHODOLOGY

When a hacker accesses a service or business's data base, which contains the private information of users, a data breach happens. payment information, Usernames, passwords, social security numbers, addresses might all fall under this category. Following that, these lists are typically sold online to criminal organizations looking to benefit from this information. Firstly, the user needs to type the email address, the one in which he is logged in like Google, face book etc. Then the user can search for any breaches i.e. if personal data associated with any email address has been revealed in data breaches. Users will also receive a breach report with suggested steps. This report will be sent to your email address. Identity theft may result from account information being exposed in a data breach. The system makes sure not to store any private information or breach information of the user. No Credit card details required to perform any breach. Figure 2 explains the data breach process on the aspects of platform and network.

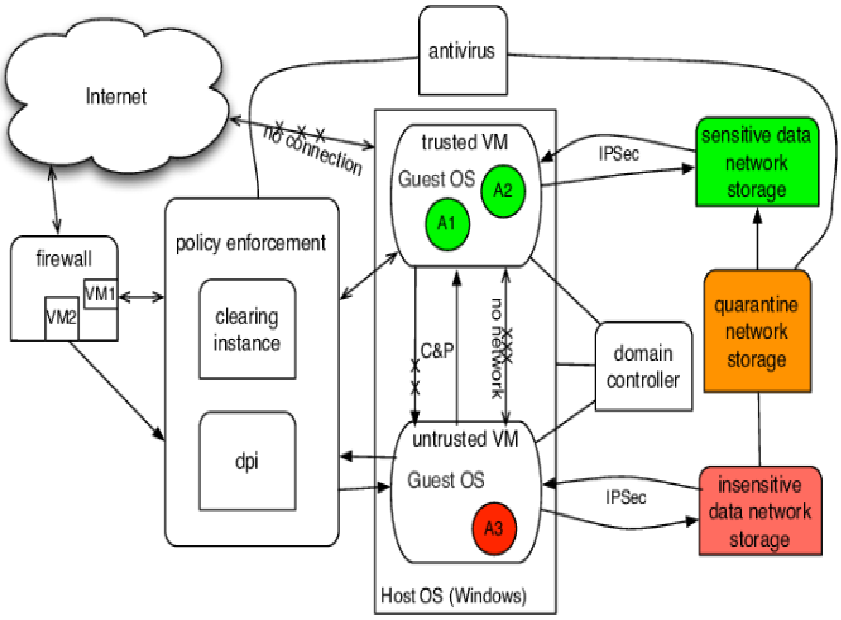

Fig.ure 2. Architecture view of data breach on the platform and networking aspects

4. ASPECTS OF DATA BREACHES

Data breaches can either occur by technology or user behavior shows in figure 3. Following can be the reasons for Data Breaches:

4.1. An Accidental Insider

Example - A worker viewing files on a coworker's PC without the required authorized permissions. Nothing is done on purpose, and nobody shares any knowledge with anyone else. The data is deemed to have been violated since it was viewed by an uninvited party.

4.2. A Malicious Insider

The malevolent insider may have access to the data and use it lawfully, but they intend to use it for bad purposes.

4.3. Lost or Stolen Devices

Any sensitive information from laptop or mobile device is used by an attacker for any illegal purposes.

4.4. Malicious Outside Criminals

Drudges that use different tools to collectsensitive information from computer system or computer network. Many Malicious attempts are also used by cybercriminals or hackers in order to perform data breach such as Phishing, Brute Force and Malware.

4.5. Phishing

It is a type of social engineering attack. Phishing attackers will send an email to deceive the victim and take out all the necessary information.

4.6. Brute force attacks

Hackers use various software tools to guess your sensitive passwords.

4.7. Malware

Malware is a kind of software that is planned to damage, destroy a computer system, server, client or computer network. Examples of malware include Trojans, viruses, worms etc. Spyware is a common malware used for stealing any kind of information.

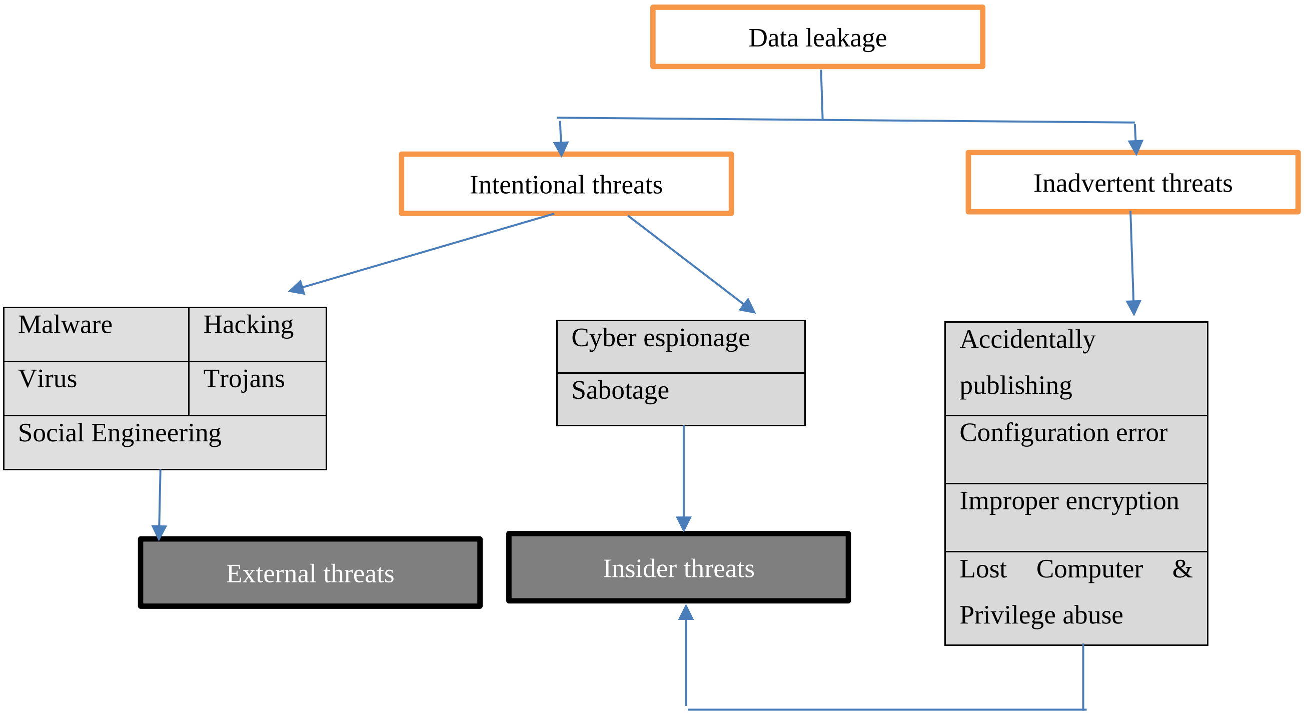

Figure 3. Classification of Data leakage

5. DAMAGE A DATA BREACH CAN DO

5.1. For business organizations

A data breach can have a destructive effect on an organization's status and economic bottom line. Large Organizations such as Target, Equifax and Yahoo, have been the victims of a data breach.

5.2. For government organizations

Polluted data may reveal exceptionally secret information to outside parties. A government and its citizens may be seriously threatened by political dealings, military activities, the disclosure of financial information to others, and information on vital national infrastructure.

5.3. For individuals

A serious risk for those affected by data breaches is identity theft. Data leaks can provide attackers access to any information, including bank account numbers. If the attacker comes into contact with your Aadhar card information, credit card information, or any other identification proof documents, they will misuse them and commit other thefts in your name.

6. PREVENTION

These days, data breaches are a growing threat, and everyone at all levels — from end users to IT staff, and everyone in between — needs to be involved in data breach prevention.Security of a system or the organization is considered to be the weakest link among all and hence attackers make sure to destroy that security and get access to the systems.Every user who engages with a system has the potential to be vulnerable.Few Practices are As soon as choices are available, updating and patching software, Advanced encryption for delicate data, Upgrading hardware when a manufacturer stops supporting a piece of software, Enforcing BYOD security regulations, such as mandating that all devices utilise antivirus and a VPN provider of the highest calibre. Enforcing multi-factor authentication and strong passwords to promote better user cyber security habits. Teaching staff members how to stay safe online and how to prevent social engineering attacks.

7. CONCLUSION

Data breaches can impact all kinds of businesses and people whose data is shared or stored online. In the modern world, data integrity is heavily relied upon by IT infrastructure companies. Data is protected by separate laws, is secret and confidential, and has value from a distinct standpoint. Even though there will likely always be a significant need for cyber security professionals, it is difficult to anticipate either the quantity of workers or the ideal combination of cyber security expertise. Therefore, critical information must constantly be protected, and passwords should be difficult for hackers to guess. Companies must always uphold customer trust and employ cutting-edge techniques to stop cybersecurity and data breach events.

REFERENCES

[1] Long Cheng, Fang Liu (2017) “Enterprise Data Breach”, Research Gate.

[2] Borders K, Prakash A. (2009) “Quantifying information leaksin outbound web traffic”. IEEE.

[3] Benjamin Edwards, Steven Hofmeyr, Stephanie Forrest. (2016) “Hype and heavy tails: A closer look at data breaches", Journal of Cybersecurity.

[4] HichamHammouchiʼ,OthmaneCherqi,GhitaMezzourʼMounirGhoghoʼMohammed ElKoutbi, (2019)“Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time”, Science Direct,

[5] Naga Vemprala, Glenn Dietrich, (2019) “A Social Network Analysis (SNA) Study on Data Breach Concerns Over Social Media”, Proceedings of the 52nd Hawaii International Conference on System Sciences,

[6] Joseph Buckman, Jesse C. Bockstedt, Matthew J. Hashim, TiemenWoutersen, (2019) “Do Organizations Learn from a Data Breach?”, University of Arizona.

[7] MehdiBarati and BenjaminYankson, (2022)“Predicting the Occurrence of a Data Breach“ in International Journal of Information Management Data Insights, Volume 2, Issue 2, November.

[8] QianWang and Eric W.T.Ngai, (2022)”Firm diversity and data breach risk: A longitudinal study”,in The Journal of Strategic Information Systems, Volume 31, Issue 4, December.

[9] YuyingLi and RogemarMamon, (2013)”Modelling health-data breaches with applicatcion to cyber insurance”,in Computers & Security, Volume 124, January.

[10] LouiseThomas,IqbalGondal,TaiwoOseni and Selena(Sally) Firmin,(2022)” A framework for data privacy and security accountability in data breach communications” in Computers & Security, Volume 116.

[11] D’Arcy, J., Hovav, A. and Galletta, D. (2009), “User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach”, Information Systems Research, Vol. 20 No. 1, pp. 79-98.

[12] Electronic Information Privacy Center (2021), “Equifax data breach”, available at: https://epic.org/ privacy/data-breach/equifax/.

[13] Rajesh, N., Selvakumar, A.A.L. Association rules and deep learning for cryptographic algorithm in privacy preserving data mining. Cluster Comput 22 (Suppl 1), 119–131 (2019). https://doi.org/10.1007/s10586-018-1827-6

[14] N. Thangarasu, R. Rajalakshmi, G. Manivasagam, & V. Vijayalakshmi. (2022). Performance of re-ranking techniques used for recommendation method to the user CF- Model. International Journal of Data Informatics and Intelligent Computing, 1(1), 30–38. https://doi.org/10.5281/zenodo.7108931

[15] Friedman, A.D. and Miles, S. (2002), “Developing stakeholder theory”, Journal of Management Studies, Vol. 39 No. 1, pp. 1-21.

BIOGRAPHIES OF AUTHORS

Dr. Manju bargavi S.K. is a Professor in the Department of Computer Science and IT in Jain (Deemed-to-be University), Bangalore, India. She has obtained PG and doctoral degrees from Anna University, Tamil nadu, India. She has 18+ years teaching experience in various engineering colleges located in India and Abroad. Her area of specialization is wireless ad hoc network, IoT, Security and image processing. She has published several Books, Patent and research papers in international journals related to computer science & engineering. She can be contacted at email: cloudbargavi@gmail.com

Dr. M. Senbagavalli received doctoral degree in Computer Science Engineering (Opinion Mining of Health Data for Cardiovascular Disease Diagnosis Using Unsupervised Feature Selection Algorithm) from Anna University. She also holds an M.E. degree in Computer Science and Engineering from Anna University and a B.E. degree in Information Technology from Periyar University. She has close to two decades of teaching experience in Computer Science and Engineering subjects. Her research area includes data mining, big data analytics, machine learning, deep learning, and IoT. She has presented and published papers in national and international conferences and reputed journals focusing on data mining, big data analytics, cloud computing, and opinion mining. She can be contacted at email: senba1983@gmail.com

Tejashwini K. R is studying in Christ (Deemed to be University), Bangalore pursuing B. Tech in Computer Science. She is a good oratory speaker and has won in many competitions. She is a South Indian Karate Player. She is good in drawing, and she is a pianist. She likes to interact with people and is keen to learn new things. She is interested in topics like data science, python, SQL and cyber security. She can be contacted at email: tejashwinikr2005@gmail.com

Tejashvar.K. R is studying in Christ (Deemed to be University), Bangalore pursuing B. Tech in Computer Science. Having a good interest in Computer's Data and Breach, led to collaboration with the professor. He is very keen to learn new things and upgrade to the societal needs. With soft skills, he has expertise in writing books, and he has published two books in Amazon kindle and Scribblitt. Areas such as Developing a game and a robot has been fascinations to him. He is a youtuber. His channel name is Learn with Tejashvar. He is a good animator and video editor. He is also skilled in playing Guitar. He is a district level chess player. He can be contacted at email: tejashvarkr@gmail.com