An Investigation Study On Data Breeching

Akriti Gupta [1], Megha Gupta [1], Dr. Deepak Chahal[2]

[1]MCA Student, [2]Professor,
[1,2] Department of IT, Jagan Institute of Management Studies, Sector-05, Rohini, New Delhi, India

ABSTRACT

In order to prevent Data Breaches and subsequent public exposure, security audits standards are becoming more important to protecting critical assets. Data breaches are inevitable incidents that can disrupt business operations and carry severe reputational and financial effect making them one of the largest risk facing organizations today.

There can be many reasons for Data Breach. For example Weak and vulnerable credentials like most commonly used password, Poor network system, Malware, and many more. Although there are many laws for prevention of Data Breach, still there are cases of Data Breach in Organizations.

Security breaches have been arising issues that cast a large amount of financial losses and social problems to society and people. This paper will explore the several disconnects between established and accepted security audit framework and the variable of hidden infections.

Keywords : *Security, Data, Access,Information.*

Introduction

Data breach is an incident where sensitive and protected information is disclosed to an unauthorized person. The field or data is viewed and shared without the user's permission. Includes personal information, such as credit card numbers, Social Security numbers and health care history, and business details, such as customer lists, production processes and source code. Anyone who is not specifically authorized to view that data is responsible for protecting the information that the company encounters with data breaches. If breach of information includes theft of identity document and / or violation of state or federal law, the perpetrator faces a fine or other penalty.

How Data Breeches Occur?

Data breaches can occur in a variety of ways. This can be done physically by accessing a computer or network to steal local files or bypass a secure network remotely.

Data breaches occur when a cybercriminal successfully releases personal and sensitive personal data, organization or loss of digital media such as computer tapes, hard drives, or laptop computers containing those sources of sensitive data.
Data breaches occur when there is an unauthorized access to business information that allows cyber shoppers access to customer data such as passwords, credit card numbers, social security numbers, bank details, driver's license numbers, medical records, and other sensitive information. Data breach can result in the loss of millions, or billions, of confidential records and sensitive data, affecting not only the broken organization, but also everyone whose personal information may have been stolen. Integrity of data refers to protecting information from falsely being modified by an unauthorized party. Information is valuable only if it is correct, tampered information could prove costly to both the sender and the receiver party[1]. Another reason for a data breach is from a trusted employee to access sensitive information if the employee retains access to data after the termination of the trust relationship

Causes Of Data Breaches

Not even a day has gone when there is no news about cybercrime innewspaper and put business at risk. So its important to know the cause of these crimes so that we find the solutions to mitigate the threats.
Some of the most common causes of data breeches are:

1. Weak and vulnerable credentials like most commonly used password: Hacking attacks can be a very common cause of data breach, but it is often a weak or lost password that is being exploited by

opportunistic hackers. Statistics show that 5 violations classified as "hack" were due to weak or lost (stolen) passwords. The simplest solution: use complicated passwords which is difficult to be hacked and never share passwords.

2. Poor network system: Developers create a software which is very poorly written or are poorly designed and implemented network system. This gives the hackers a great opportunity to exploit the software and easily get the entire data.
   Simple solution: Keep all software and hardware solutions completely up-to-date.
3. Malware: The use of both direct and indirect malware is growing. Malware is, by definition, malicious software: utility-loading software that opens access to hackers to exploit a system and potentially connected systems.
   The simplest solution: Beware of accessing websites they don't see, or opening emails that you suspect have their origins, both of which are popular ways to spread malware.

4. Exfiltration: When a cybercriminal enters a single computer, it can attack the network and integrate its own private data path. When a computer is released of data, the attack is considered successful.

Laws Of Data Breeches

Since personal information is individuals manifestation so various Indian courts including Supreme courts have recognized that the right to privacy is individuals right to life and personal liberty.

Various laws are made to protect the right to privacy of every person

1. Information Technology Act

IT law is made which protects against certain breaches of data from Computer Systems. The Act contains provisions for prevention unauthorized use of computers, computer systems and data stored therein. This section creates personal liability for the improper or unauthorized use of computers, ADPS and thus the info stored therein. However, this section is silent on this responsibility of Internet Service Providers or Network Service Providers, additionally as entities managing data. As a result, the companies in charge for the safe delivery and data processing like vendors and our outsourcing service providers is out the scope of this section.

2. Indian Penal Law

The Indian codification doesn't directly address the confidentiality of information. In accordance with the Indian codification, the liability for such violations must be assessed against related offenses. as an example, section 403 of the Indian codification applies to judges who face criminal misconduct or alteration of 'movable property' 2 for personal use.

3. Holding Law

It is important to note here that Indian courts have recognized copyright.

Database. it absolutely was organized to compile a listing of developed customers / customers. By taking some time, money, labour and skill money for somebody's "literary work" the author is copyrighted under the Copyright Act. If anything there is a breach regarding the data base, our outsourcing could even be the parent unit promise under copyright law.

4. Credit Information Companies Regulation Act, 2005(“CICRA”)

Credit information regarding persons in India, per CICRA must be collected in accordance with the privacy standards per the CICRA Regulation. Institutions. in charge for collecting and managing data the utmost amount as possible this will be a knowledge leak or change. The fair relies on the Credit Reporting Act and Graham Leach The Blake Act, CICRA has drafted a strict framework for information Loans and Finance of individuals and Institutions in India. Terms under CICRA has recently been notified of providing for strict data privacy principles by the bank of India.

Data Breech Prevention

1. Know the law

There are many laws governing consumer data protection and privacy. Depending on the type of industry and the

type of data you collect, you may have to deal with several data protection laws. The best way is to create a data protection policy that protects data from risks both inside and outside the company.

2. Growth rate security policy

The best way to avoid infringement is to prioritize security by using best practices, procedures and procedures and adding it to policy. The best ways that policies are discussed are:
Fer Keep data transfer to a minimum. Transfer data from one device to another only if necessary. Extractive media is easily lost, putting all information at risk.
Tasks store the data you need to complete your tasks. This is an important part of the new Data Protection Regulation.
Password Change passwords often, all unexpected and difficult to crack. Symbols and numbers are flexible.
Policies clearly define computer policies and acceptable use. Ask employees to sign a policy affecting trusted websites (Google, Wikipedia, YouTube) and unreliable websites.
Use when the cloud makes sense. Cloud servers are encrypted and monitored by professionals who are looking for different behaviours. These servers also make it easy to move and unplug AC

3. Reduce Human Errors

Human error is the cause of a large number of data breaches, but you can reduce the number of accidental violations by automating many of your processes and processes.
You can use automated security measures, such as a system that regularly checks passwords and / or reminds you to change them periodically. You can also use Technology Assessment Server and Firewall Configurations, which will alert you to any holes or leaks. Instead of asking employees not to download anonymous content, take it one step further and use filters in email and Internet browsers. This way, there is an extra security guard to prevent employees from accidentally clicking on wrong websites or emails.

4. Train and educate STAFF

Training and training of employees is essential to keep the organization safe and sound.
In this case, the training not only gives employees the tools to look out for others' risky behaviour and careless behaviour within themselves, but also helps to make the company's culture more secure, protect privacy first and keep it safe. A focus is made on machines as machines cannot be understood by verbal communication it forms abstractions and concepts [2].

5. Use encryption

When dealing with private data regularly, encryption is important. You can only set documents or emails labelled with related documents.
This can help you protect sensitive data, anywhere, even if the document has been sent to the wrong email, the work laptop has been stolen, and the data has gone into the wrong hands. If the recipient does not know the correct encryption key, he or she will not be able to access the information.

6. User Authorization and Access

It makes more sense to properly control data access from scratch and try to rename it negligently. Not everyone has access to everything, so give employees access to the files they need to complete their tasks.
Use multi-level authentication to protect hackers from accessing non-personal accounts. Emphasize complex passwords that require a lower case letter, higher case letter, number and symbol.

7. Use track data and monitor

System monitoring can be a great added security for your company. Internal Behaviour Monitoring allows anyone to reuse computers in the HR or IT team. This way, they can track which file they are entering. They can keep or follow the scenes of an item and where they are posted.

The speed of data monitoring will give you a clear idea of when and where to fly and who is responsible.

8. Regular Audit and Evaluation

Check for weaknesses once a month or week. Always check the security controls and content of each application on the network (internal and external) to detect and prepare for attacks.

9. Backup data

This step not only prevents data breaches, but also makes the loss much easier. Not all hackers want to steal, sell, trade or use your files to do illegal activities. Some cyber criminals want to annoy the pot by deleting your data.

If a virus deletes some of the content of your program, the basic backup plan will help you restore the data to the

original location.

10. Developing a data breach response plan

While many companies have not yet implemented a strong wind response system, such framework is essential for cyber security events, as well as for reducing risk and restoring public confidence with employees. The main purpose is to determine the roles and responsibilities of those who work in crime; It is also important to capture the investigation process, including draft information.

Security is looked in terms of how data is stored, coded, transmitted, encrypted and deleted. Various statistics has shown that companies take security of the data of an individual with very high priority [3].

The importance of the response system is emphasized by the rules. Subject to GDPR requirements, for example, companies must respond to data breaches within 72 hours; This includes collecting all relevant information, reporting violations to the appropriate administrator and notifying the person affected.

As technology continues to drive businesses, it puts them at risk of cybercrime. To minimize the risk of enriching a growing range of cyber victims, cyber security should be a priority for every organization.

Conclusion

From the last few years we have noticed many cyber security attacks in all over the world and in almost all sectors like telecom, banking, e-commerce etc with make cyber security as biggest challenges for world [4].Preventing and detecting data leaks require constant effort and investment from organizations. In this paper, we have presented a review of data leak threats. We described the variety of ways through which data breeches occur. In this review article, we highlighted the causes of data breeches. We also pointed out several laws that are made to protect the right to privacy of every person. At the end, we presented various ways how the users can prevent themselves from data breeches.

Reference

1. Varyani Y. et al. A Survey on Cryptography, Encryption and Compression Techniques, International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 11 | Nov 2019.

2. Kharb.L et al (2019) “Brain Emulation Machine Model for Communication” in International Journal of Scientific & Technology Research (IJSTR). pp 1410-1418.

3. Bhutani S. et al, Data privacy and security issues in India: An empirical study, International Journal of Research in Engineering, Volume 1; Issue 4; October 2019; Page No. 15-17.

4. Shubham. et al. Security for Digital Payments, Int. J. Sci. Res. in Network Security and Communication, Volume-6, Issue-5, October 2018.