ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 11, November 2017

A Detailed Survey on Big Data Application in Global Banking Data Management & Decision Making

[1] Dhanya G S, [2] Hemsai L, [3] Sachin Kumar, [4] Imthiyaz Ali, [5] Yuvaraj Patil
Electronics and Communication Engineering, Sri Sairam College Of Engineering Anekal, Bangalore

Abstract:- **This presentation mainly focuses on Information security. Information security deals with the privacy and security concerns of the data. Are all our data safe and secure with us? How can our data be secured from data phishing and hacking? How is the data misused? Everyday at least 10 millions of the records are getting swiped. Here we see how to protect the data.**

I. INTRODUCTION

Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may be either electronic or physical. Information systems security, more commonly referred to as INFOSEC, refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity. It also refers to: Access controls, which prevent unauthorized personnel from entering or accessing a system.

Current scenario

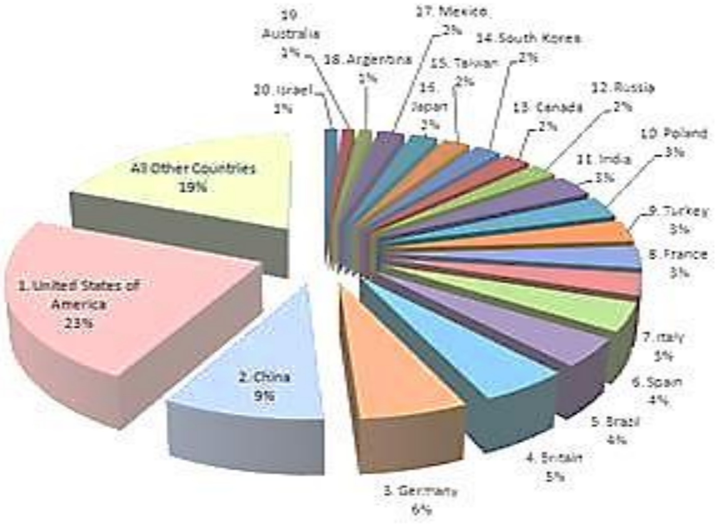
More data records were leaked or stolen by miscreants during the first half of 2017 (1.9 billion) than all of 2016 (1.37 billion). Digital security company Gemalto's Breach Level Index, published Wednesday, found that an average of 10.4 million records are exposed or swiped every day. During the first half of 2017 there were 918 reported data breaches worldwide, compared with 815 in the last six months of 2016, an increase of 13 per cent. A total 22 breaches in Q1 2017 included the compromise, theft or loss of more than a million records.

Present Trend

The commonly used are the hard disc drives found on most computers to store information. Information is stored using positive and negative magnetic charges to correspond with the 1s and 0s. Optical discs like CDs and DVDs store information as binary code that can be read by an optical sensor in a disc drive. Likewise, flash/SSD technology – commonly found in Smartphone's, USB drives and some laptops – stores that same information electronically. These Days most of the information is stored in cloud storage system. Cloud storage enables the user to access the data anywhere, anytime while the data is stored in the external hard drive by cloud service systems, where there is no guarantee of security for our information.

Why to protect information????

The Data Protection Act contains a set of principles that organisations, government and businesses have to adhere to in order to keep someone's data accurate, safe, secure and lawful. These principles ensure data is: Only used in specifically stated ways. Stored following people's data protection rights.



Cybercrime: Top 20 Countries

Information breaches

In recent years there has been rapid rise in cyber crime and data breaches, Developing country like India has 3% of cyber attacks in the world. It would result in economic and military breaches to the world. It's very important to protect our data. Here are some of the biggest data breaches of the year,

Yahoo

Yahoo announced that data associated with at least 500 million accounts had been stolen. Three months later, it disclosed a second breach affecting more than one billion accounts.

MySpace

Myspace confirmed a breach of user names and passwords for about 360 million accounts. The company attributed the breach to a Russian hacker who goes by the name Peace.

LinkedIn

Hacker, Peace, also took credit for hacking LinkedIn in 2012. The breach wasn't revealed, however, until 2016. LinkedIn said "more than 100 million" members were affected. The hacker reportedly tried to sell the account information online.

Precautions

With data breaches making headlines regularly, consumers are losing confidence in the privacy of their personal data. Here let's see early precautions to secure the data.

a. Monitor Access To Your Data

Make sure you monitor who has access to your data. Require multi-step authentication processes for employee access, verifying business reasons for each system access, logging and monitoring employee use to identify unusual system patterns or behaviours, installing secure internet access points, and using IP address profiling to prevent any unauthorized access. Be aware of any unusual network activity and data transmissions to unknown hosts.

b. Change Passwords Frequently

Something as simple as a password can be detrimental to the safety of your data. There are many preventative actions when it comes to passwords, including using longer passwords with a variety of numbers and symbols, different passwords for different systems, mandatory password changes every 90 days, or requiring employees to "sign out" a specific administrator password so passwords aren't floating around and easily obtainable by a hacker, both internal or external.

c. Take Physical Security Measures

Physical measures for safeguarding information can involve restricting access to facilities to prevent physical intrusions, monitoring computer equipment, locking up particular rooms or file cabinets housing sensitive information, and also shredding documents.

Myths

What people get wrong about their Information security?

- If I install security application I will be fine.
- I set a strong and complex password to my account, so I'll be ok.
- I don't need security software, I don't access unsafe locations.
- Internet security is expensive.
- My social networks are safe places. Friends will be friends.
- In case I get infected, I will see that for sure.

Preventions

Here are various steps to protect our data and keep it secure.

-Use two-factor authentication.

You can lock down your Facebook, Google, Dropbox, Apple ID, Microsoft, Twitter and other accounts with two-factor authentication. That means that when you log in, you'll also need to enter a special code that the site texts to your phone. Some services require it each time you log in, other just when you're using a new device or web browser. The Electronic Frontier Foundation has a great overview of what's available. Two-factor authentication works beautifully for keeping others from accessing your accounts, although some people feel it's too time consuming. But if you're serious about privacy, you'll put up with the friction.

-Pay for things with cash.

According to Business Insider, credit card companies are selling your purchase data to advertisers. Don't want companies knowing how much booze you're buying or other potentially embarrassing habits? Buy things the old fashioned way—with coins and bills.

-Keep your social network activity private.

Check your Face-book settings and make sure only friends can see what you're doing. Go to the settings cog in the upper right hand corner of your screen, then click on Privacy Settings >> Who can see my stuff.

-Use a password vault that generates and remembers strong and unique passwords.

Most people know better than to use the same password for more than one website or application. In reality, it can be impossible to remember a different one for the dozens of online services you use. The problem with using the same password in more than one place is if someone gets their hands on your password—say, through a phishing attack—

they can access all your accounts and cause all sorts of trouble.

-Lie when setting up password security questions.
"What is your mother's maiden name?" or "In what city were you born?" are common questions websites often ask you to answer so as to supposedly keep your account safe from intruders. In reality, there's nothing secure about such generic queries. That's because someone who wants access to your account could easily do some Internet research to dig up the answers.

II. CONCLUSION

Throughout the literature review it has been found that by and large many organizations are not following cyber security practices. It is concluded that irrespective of the industry segment, there is a need to conduct research to find out a comprehensive approach to protect sensitive data and take appropriate action. How important is privacy of our data to us and how our data is manipulated. We have also come across various method for protecting the data and keeping them secure.

REFERENCES

[1] Wikipedia

[2] http://www.zdnet.com/pictures/biggest-hacks-leaks-and-data-breaches-2017/3/

[3] International Journal of Engineering Research and General Science Volume 2, Issue 5

[4] Information Security Economics – and Beyond Ross Anderson and Tyler Moore

[5] http://techland.time.com/2013/07/24/11 -simple-ways-to-protect-your-privacy/

[6]http://money.cnn.com/2017/09/07/techn ology/business/biggest-breaches- ever/index.html

[7] http://www.wired.co.uk/article/hacks-data-breaches-2017

[8] https://iprsecure.com/7-preventative-measures-for-avoiding-a-data-breach

[9] https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

[10] Paul Marsh, ―Controlling Threats‖, IET Computing & Control Engineering.