DATA BREACHES

At the outset it is pertinent to note:

"Employees are the weakest Links" and "Employees are the linchpins for most of the data breaches".

Introduction:

Data Breaches are increasing in volume and scope in these days of high dependency on Internet and computer technology development. Hence if no stringent controls are in place all organisations are vulnerable for data theft either by internal persons or external hackers and cyber criminals working for a price to breach data and steal data for the benefit of one party and to the detriment of the organisation that is targeted.

Wikipedia definition of data breach:

…" A data breach is an intentional or unintentional release of secure or private /Confidential information to an untrusted environment……"

….." A data breach is a security incident in which, sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so…."

Broad Type of Data Breaches:

1.Internal 2. External

Other Category of Data Breach Types:

1.Unintentional 2. Hacking and Malware 3. Intentional breaches
4. Physical loss of documents or misplacing of documents
5. Stolen laptops, I pad, documents and devises.
6. Compromised records.
7.Business partners.

Statistical and other information on Data Breaches:

ITRC- Identity Theft Resource Centre-As per statistics of ITRC.in 2015, there 6000 data breaches were reported and more than 8.5 million records were compromised.

It becomes easy for Hackers to breach data if 128-bit data encryption is followed instead of 56 data encryptions.
External data breaches are rampant. Hacking or unauthorised intrusion of network in the case of Comcast-Nov 2015 reported, 590,000 customer addresses, emails and pass words were compromised.

Verizon in its annual data breaches Investigative Report reported that during 2004 to 2014,79,790 security breaches were reported, that led to 2,122 confirmed data breaches which resulted in about $400 Million in losses and 70,000 compromised records.

Verizon released 2018 Data Breach Investigative Report and it is revealed that Ransomware took the major share of about 39% reported this particular Vicious Malware related breaches. The report studied 53,000 security breach incidents including 2300 confirmed data breaches across 65 countries.

“Incident” Means, a security even that compromises the Integrity, confidentiality or availability of an information asset.

“Breach” an incident that results in the confirmed disclosure of data to an unauthorised party.

Oklahoma College of Medicine-department of Obstetrics and Gynaecology lost patients’ data of about 7,963 from a non-employee that is, external fraudsters.

Data breach may occur if the outsourcing company inadvertently sends data of one Client to another.

The above cases arise as a result of external thieves of data.

As per ACFE Survey of 4,662 cases, over a ten-year period, Internal causes 38%; External causes 47% and Untraceable 15%.

Another important factor identified from a survey is that Data Breaches occur due to “Improper protection or disposable of data “.21%; Current or former employees 9%; Hacking 2%; Loss of data 5%; External factors 7%; Non-Employees 4 %; Hacking by non-employees 25% and finally other unknown factors 27%.

2016 ACFE Report has observed that a typical organisation looses 5% of revenues in a given year as a result of frauds. Thus, the report mentioned 2.7$ as average cost per case with a median loss for all cases was $150,000/ with 23% cases causing $ 1 Million or more.

Verizon 2018 Data Breach Investigation Report Observations:

1.Ransomeware was identified as a big threat from online criminals in 2018. These types of attacks have far over taken all other threats of data theft of cybercrime. It is a rough weather for many corporates facing this form of malicious malware features hackers making money by holding critical business systems hostage. The report found that ransom ware attacks have doubled over the past year, accounting for 56 percent of malware -specific incidents in 2018.Businesses are still not investing in appropriate strategic strategies to combat ransomware. 56% of Malware related breaches are related to Ransomware. Cyber criminals are only the winners as the corporates are paying off ransom without taking steps to install control over such incidents.

2.The other data breach relates to phishing-that the fraudster sends an email message to the Victim who opens the e-mail and clicks on some malicious attachment or link which actually activates the Malware. The report states that though this type of data breach is of high incidence, the positive aspect is, that all most 78% of the users who receive such e-mails never click on such a Phishing e-mail the whole year.

Preventive steps from Data Breaches:

1.Protection of Data:

All-important data should be properly and securely protected and access should be restricted to only the concerned persons. Precautions must be taken not to reveal inadvertently any personal information too.

2.Data Storage:

All data of the organisation must be stored externally and at more than one storage location. Utmost precaution must be exercised while transfer of data is affected during g the storage process or there may be a possibility of loss of data or data falling in the wrong hands.

3.Disposal of storage or other devises and shredding of data:

Whenever there arises a situation where data is shredded or disposed utmost care should be taken in the execution of that process under direct supervision of responsible persons and in a way, no one can have any access to such shredded data or disposed data files.

4.Data movement:

Whenever any data is sent by courier or other third party the devises or files of data must be securely packed and make sure that the packet carrying such data is tamper proof. Data in transit and data at rest should be securely identified and tracked.

5.Encrypted Policy of devises:

The organisation should have a strict policy of all computer and other related equipment for encryption. unencrypted devises etc should eb banned. It applies as well to data encryption. Something locked with a 256-bit encryption would take a bank of super computers billions of years to decode using brute force alone. However, an organisation should choose a encryption that is most suitable and feasible for securing its data and devises. The encryption should happen by default on the devises not by invoking any option.

6.Password protection of data and devises:

The organisation must have a very strong passwords policy. The passwords should be unique and different users at different levels should have separate passwords for their respective restricted usage on need basis.

7.Tracking data in the organisation:

There should be a mechanism for tracking data within the organisational network passing in the organisation; This will help to know who logged in or logged out who accessed what data and such other logging information for tracing in case of any data breach.

8.Security training to employees:

The most important aspect of preventing data breaches, there should be security training to employees from time to time about the importance of data security and consequences if any employee is caught or traced for any breach of data.

9.Breach warning and response plans:

There should be a mechanism to give a warning signal to the IT department if there is any data breach or intrusion. Also, there should be a plan in place to deal with any data breach that might have occurred despite all precautions to trace the breach and take necessary action from any damage due to the leak.

10.Cloud Computing:

Use of the latest technology of cloud computing will help a lot in data security management. The data that is stored for access on cloud can be traced and only the persons with authorization can access, IT thus gets full visibility and control over data while the user gets the level of access they need to get their work done. It has the maximum safety of data.

Conclusion:

Data breach has become a universal problem and more rampant than another cause for misuse or loss of data that is detrimental to an organisation. There are several types of data breaches that are responsible for loss of valuable data of an organisation. However, an organisation should invest and take note of the importance for the prevention of such data breach by proper control mechanisms and secure passwords, data encryption and cloud computing methods. Also, the organisation should bring to light any data breaches to respective agencies and should not end up paying ransom to the fraudsters responsible for the breach.

References:

1.May-June-ACFE 2016 Magazine

2.Verizon -2018 Report

3.ACFE-2018 Report