19 ways data can be leaked

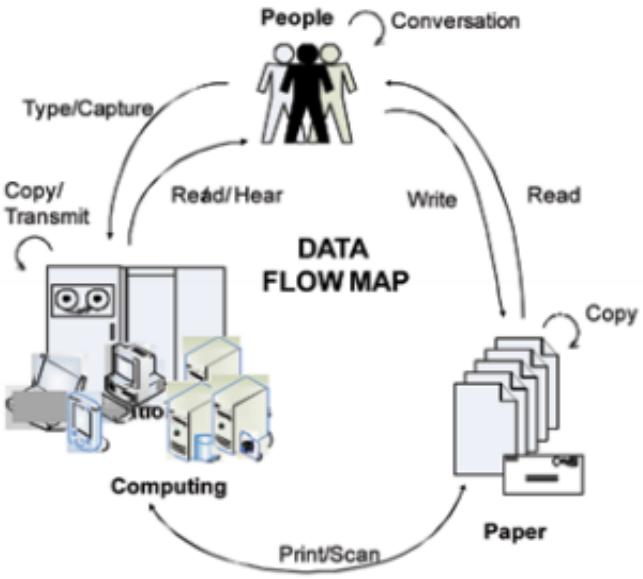
InterRisk Asia (Thailand) Co., Ltd.

What is data breach ?

Have you ever wonder how our confidential or personal information leaks from us? How they fall into the wrong hands?

A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner which can cost A small company or a large organization to suffer a great lost.

Stolen data may involve sensitive, proprietary, or confidential information, such as credit card numbers, customer data or trade secrets.



There are so many places data can easily leak out of an organization There are three buckets or containers where information "lives"— in digital form, in hard copy (paper) and in the conversation and heads of people.

Information is constantly flowing between these containers, usually resting in more than one of them at any given moment without some type of map or landscape that lays them all out.

Broadly, these data leak ways divided into 2 classes which are Internal data leakage and leakage from external threats

19 ways of leaking faucet

1# Instant messaging (peer-to-peer)

Many organizations allow employees to access Instant Messaging from their workstations or laptops which includes products such as Skype; AOL; Google Talk; and Peer-to-peer (P2P). It would be a simple process for an individual to send a confidential document (such as an Excel file containing sensitive pricing or financial data) to a third party. Equally a user could divulge confidential information in an Instant Messaging chat session to an external user.

2# Email

Traditional email clients, such as Microsoft Outlook, Lotus Notes, etc are ubiquitous within organizations. An internal user with the motivation could email a confidential document to an unauthorized individual as an attachment. They may also choose to compress and / or encrypt the file, or embed it within other files in order to disguise its presence. An employee could attach the wrong file inadvertently or even be tricked into sending a document through social engineering.Email also represents a vector for inadvertent disclosure due to employee oversight or poor business process.

3# Web Mail

Web Mail is well entrenched with users. Gmail, Yahoo, and Hotmail are popular examples. It represents another way for an individual to leak confidential data, either as an attachment or in the message body. Because Web Mail runs over HTTP/S a firewall may allow it through un-inspected as port 80 or 443 will in most organizations be allowed, and the connection is initiated from an internal IP address.

4# Web Logs / Wikis

Web Logs (Blogs) are web sites where people can write their thoughts, comments, opinions on a particular subject. The blog could include the input from thousands of individuals and could be used by someone to release confidential information, simply through entering the information in their blog. However, they would most likely be able to be tracked, so this is perhaps a less likely medium. A wiki site is“a collaborative website which can be directly edited by anyone with access to it and contains the possibility that confidential information may be added to a wikipage.

5# Hiding in SSL

In order to obfuscate data, a user may attempt to utilize a public proxy service via an SSL connection (often called Proxy Avoidance). They access the proxy service via a browser, type in the URL of the site they wish to visit, and their entire session is then encrypted. A Stateful Packet Inspection firewall will not be able to examine the data as it will be encrypted. Consequently sensitive information may be leaked through this medium without detection.

6# Malicious Web Pages

Web sites that are either compromised or are deliberately malicious, present the risk of a user’s computer being infected with malware, simply by visiting a web page containing malicious code with an OS/browser that contains a vulnerability. The malware could be in the form of a key logger, Trojan, etc. With a key logger the risk of data theft is introduced. Users would download a key logger/backdoor, “providing the attacker with full access to the compromised computer”

7# Data theft by intruders

An ever-popular topic in the media is the electronic break-in to an organization by intruders including the theft of sensitive information. There have been numerous stories in the press of the theft of credit card information by intruders. This particular event holds significant concern, because resumes contain a significant amount of information about an individual, including their full name, address, phone number(s), employment history, interests, and possibly contact details of third parties, such as referees. This allows for particularly targeted, and if crafted well, believable phishing attacks, or perhaps even more audacious social engineering attacks such as phone calls.

9# Malware

In recent years, if malware is classified as a zero day threat, and there is no signature yet available, there is a higher likelihood that the malware will evade inbound gateway protection measures and desktop anti-virus then initiate outbound communications, potentially sending out files which may contain sensitive data and when the traffic is from an internal source. Most firewalls will not restrict traffic that is initiated internally via an acceptable protocol.As discussed key loggers present a threat as they capture potentially sensitive information, such as login credentials, personal information, leading to the risk of identity theft.

11# Dumpster diving

Organizations that do not take appropriate care with the destruction of hard copy information run the risk of confidential information falling into unauthorized hands. Instead of having such information destroyed securely, businesses may simply throw their confidential information (perhaps unwittingly) into the rubbish. An attacker may decide to raid the company's dumpster and discover this information. This extends to information stored on media

8# SQL Injection

Web sites that use an SQL server as the back end database may be vulnerable to SQL Injection attacks, if they fail to correctly parse user input. This is usually a direct result of poor coding. SQL Injection attacks can result in content within the database being stolen. The initial action of the attack could be to enter a single quote within the input data in a POST element on a website Further trial and error by the attacker could eventually reveal table names, field names, and other information, that, once obtained, will allow them to construction SQL query within the POST element that yields sensitive data

10# Phishing and Pre-Phishing

Phishing is one form of social engineering which pose a threat to organizations, and not just individuals. Phishing spam may be received at peoples' work email address. Should they be fooled into visiting the phishing site, then they may lose personal information and or financial information.

Pre-phishing is emerging as a new method used by phisher. Instead of attempting to directly obtain credentials for a financial site, social networking and email sites are targeted. The attack seeks to obtain username and password combinations, on the (likely) assumption that in many cases, users will use the same or similar combinations on other web sites. The second part of the attack is to conduct a CSS History Hack, where the phishers can determine whether the user has visited specified sites. Banking sites visited by users may be obtained, and the phishers can then visit these and attempt to gain access using the compromised credential combinations.

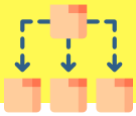
12# Physical Theft

Physical theft of computer systems, laptops, back up tapes, and other media also presents a data leakage risk to organizations. This may be due to poor physical security at an organization's premises or poor security practice by individuals. . Also possible is the mass theft of laptops from within an organizations premises after hours, should the business fail to secure the laptops overnight.

13# Removable Media / Storage

Theft or loss of a computer or data storage medium, such as a USB memory key, made up 54 percent of all identity theft-related data breaches. Due to their small size, USB keys are also easy to lose. Even if the copying of data onto the key is legitimate, the risk exists that the key could be lost by the user and found by a third party.

14# File Transfer Protocol (FTP)



FTP represents another method for an individual to release information. It is straightforward to install and configure a basic FTP server external to the organization. The individual then merely has to install a publicly available FTP client and upload the file or files to the server. This method could even utilize a "dead drop" public FTP site hosted off-shore, where the third party also has access. As FTP is a popular protocol there is the likelihood it will be allowed through the firewall.

15# Security Classification errors

Security models are intended to provide a framework for organizations to avoid classified and / or sensitive information being sent to individuals (internally and externally) without the appropriate security clearance level. It is conceivable that an individual with Top Secret clearance may either intentionally or inadvertently send a Top Secret document to another individual with only "Classified" clearance.

16# Hard copy

If an individual wishes to provide a competitor with sensitive material, and the victim organization has already implemented electronic countermeasures, it is still possible for the individual to print out the data and walk out of the office with it in their briefcase. Or, they simply place it in an envelope and mail it, postage happily paid by the victim organization.

17# Inadequate folder and file protection

If folders and files lack appropriate protection (via user/group privileges etc) then it becomes easy for a user to copy data from a network drive (for example) to their local system. The user could then copy that file to removable media, or send it out externally by methods discussed above.

18# Cameras

A determined individual may choose to take digital photos (or non-digital for that matter) of their screens. A camera is not even needed nowadays. Cellular telephones today are likely to have a camera built in, perhaps with up to 2 mega pixels or more. The photo could then be sent by email or Mobile Messaging directly from the telephone.

19# Inadequate database security

- Poor SQL programming can leave an organization exposed to SQL injection attacks, or allow inappropriate information to be retrieved in legitimate database queries. Additionally, organizations should not implement broad database privileges as this can lead to users accessing confidential information (either intentionally or inadvertently).

Further information :

https://www.sans.org/reading.../data-leakage-threats-mitigation-1931

https://www.sans.org/reading-room/whitepapers/analyst/data-leakage-landscape-data-leaks-generation-tools-apply-34695