

Implications of data Security Breaches on Individuals & Organisation

IMPACTS ON INDIVIDUALS

IMPACTS ON ORGANISATIONS

Impacts of Data Security Breaches

Data breaches have hit the headlines recently with some of the biggest breaches occurring in the past few years.

LinkedIn, Tumblr, Yahoo, Three Mobile, and Tesco Bank all hitting the headlines as victims of cybercrime.

The data that is stolen can lead to problems for the individuals whose data is now in someone else's hands.

What is a personal data security breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are the result of both accidental and deliberate causes.

It also means that a breach is more than just about losing personal data.

What is a personal data security breach?

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.



In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed.



Or if someone has accessed the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal Data Security Breaches

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Personal Data Security Breaches

In July 2015, a group calling itself "The Impact Team" stole the user data of Ashley Madison, a commercial website billed as enabling extramarital affairs.

The group copied personal information about the site's user base and threatened to release users' names and personally identifying information if Ashley Madison was not immediately shut down.

On the 18th and 20th August, the group leaked more than 25 gigabytes of company data, including user details.

Because of the site's policy of not deleting users' personal information – including real names, home addresses, search history and credit card transaction records – many users feared being publicly shamed.

Personal Data Security Breaches

Following the release of the data, some people on the internet went through the databases to try to find people who were members, and planned to publicly humiliate them.

It was later confirmed that at least two people who were members of the website had committed suicide.

While this is an extreme example of how a data breach can have a negative impact on people, other implications could be:

Personal Data Security Breaches

Financial loss

Financial reputation

Damaged personal reputation

Loss of employment

Marital breakdown

Stress/illness



Research Task

Research Task – Using the web, can you find any other data security breaches that impacted on Individuals?

Organisation Data Security Breaches

With the number of data breaches increasing every year, they are now a huge issue for organisations.

46% of all UK businesses identified at least one cyber breach in the past 12 months and it's been predicted that a quarter of the world's population will have been affected by a data breach by 2020.

It should be obvious that it's a priority for companies to learn how to keep data secure.

Organisation Data Security Breaches

A business suffers in many ways when it falls victim to a data breach, one of which is dealing with the financial repercussions.

There are a range of different costs associated with a data breach, such as paying back any money taken as a result of the breach, compensating affected customers, share value plummeting and having to pay for the right protection to ensure a breach doesn't happen again.

Organisation Data Security Breaches



In addition, breached companies can be fined by the Information Commissioner's Office (ICO), with penalties reaching a maximum of £500,000. This figure has drastically increased since the General Data Protection Regulation (GDPR) took effect in May 2018.



After paying off fines, the breached company also has to deal with reputational damage. Breaches have a massive negative impact on a company's customer base, particularly if the breach involved sensitive data. Customers lose confidence in the brand and don't feel that their data is secure. A breach also puts off many potential customers.

Organisation Data Security Breaches

The impact of a breach is tied to the type of data involved. If the organisation's confidential data has been exposed, it can have catastrophic effects.

If personal and financial details of staff and customers are breached, those people are left open to the risk of identity theft.

Impacts on organisations can include:

Reputational damage:

Theft:

Financial loss:

Fines:

Organisation Data Security Breaches Example



In 2015, TalkTalk suffered a data breach in which the details of more than 150,000 customers were stolen, including bank account details of about 15,000 of those customers.



The company lost 95,000 subscribers as a result of the attack, costing it £60 million. On top of that, TalkTalk was also fined £400,000 by the ICO. However, TalkTalk subsequently failed to adequately protect its data and, earlier this year, the details of more than 21,000 people were unlawfully taken.



On this occasion, the company was fined £100,000.

Research Task

Using the web, can you find any other examples of data security breaches on Organisations?