Potential Effects on organisations

DATA SECURITY

Potential Effects on Organisations

Each organisation is unique in terms of how a data breach affects them. On most occasions, it depends on the time of the breach, how long it lasted before it was discovered, and the sector in which the organisation operates.

The most common impacts that should be considered are:

- Reputational damage
- Theft
- Financial Loss
- Fines

Let’s look at these in a little more detail …

Reputational Damage

Loss of customer confidence can be one of the most harmful and damaging impacts of a data breach.

Most people would not want to do business with a company that had been breached, especially if its customer data was not protected properly.

This loss of confidence can lead to loss of business, and money, as well as devaluing the brand of the company, which sometimes has taken years to build up.

Damage to reputation may also affect the company’s ability to hire staff and attract investors.

Theft

Banks are an obvious target for hackers to target.

The financial rewards can be huge, but smaller businesses also make a good target, as they have less sophisticated defences.

Stolen data from soft targets can be worth a lot of money, especially when sold to the highest bidder on the Dark Web.

The theft of intellectual property may also be very damaging.

If a company has invested a lot of money and several years into Research and Development for a new product, and then those trade secrets become part of a data breach that can give their competitors a big advantage.

Financial Loss

Data breaches and cybercrime in general, cost smaller businesses a disproportionately higher amount in terms of their turnover, than big businesses.

For a big business, such as Amazon, Tesco or Bank of Scotland, a financial impact could run into millions of pounds, loss of share value, for example, could contribute to this.

However, by their scale, that can be a very small amount.

Smaller businesses could be wiped out.

The estimated cost for a small business to recover from a cyber-related incident is between £75-311k in 2015. That cost will only increase as the data breaches and the cyber more common and sophisticated.

Fines

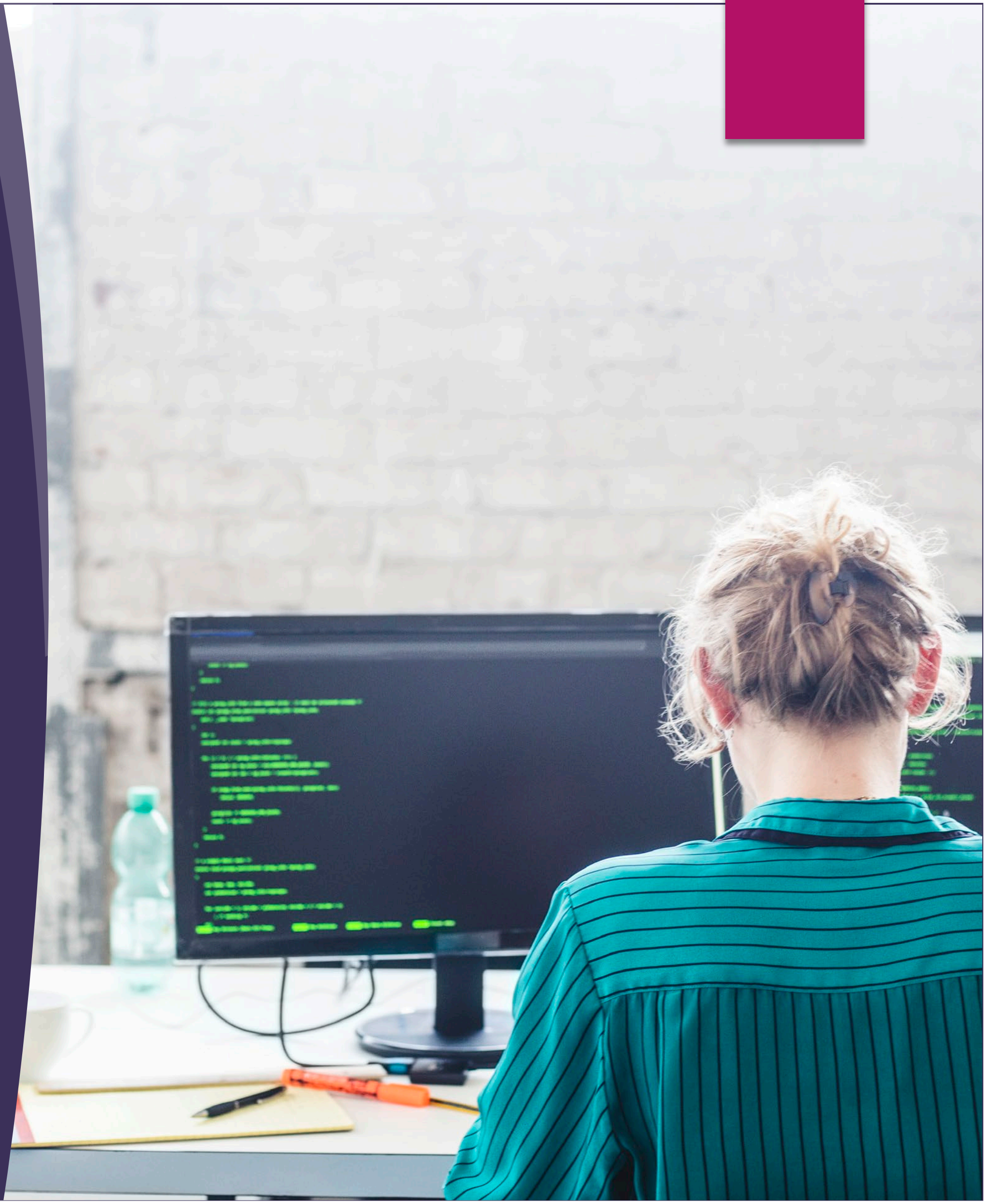
A financial loss is bad enough, but when the organisation of business has to contend with a fine as well, that can be disastrous.

Some organisations have been fined for failing to comply with data protection legislation.

One of the more severe measures proposed by the European Parliament for a privacy breach, applicable from 25 May 2018, is a fine of 20 million euros, or 4% global annual revenues, whichever is higher– a sum that would threaten many growing businesses with insolvency.

ICO guidance – Breach Management Plan

- Containment and Recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response



TASK

Now do Task 16