DPD21 ADVENT IM

TRAINING | POLICY| PROCESS

This is why you need it ...

Source: ICO; Q2 2021 vs Q2 2020

NEARLY 15% DROP IN ALL DATA BREACH

DRIVEN BY A SIGNIFICANT DROP IN NON-CYBER BREACHES

2021 Q2 saw a drop of almost 15% in total data breaches. This was driven by significant drop in non-cyber breaches compared to Q2 in 2020. As non-cyber is the vast majority or overall data breach incidents (72% in Q2 2021) it has a big impact. The drop is great news, however, there are some types of non-cyber breaches that are seeing significant growth...

THE BIG 3 ALL ON THE RISE

IS YOUR COMPANY CULTURE CAUSING A BREACH?

- Data emailed to the wrong recipient **(+17%)**
- Failure to redact **(+40%)**
- Incorrect disposal of hardware **(+100)**

All 3 breach types on the rise. Incorrect disposal of hardware does look like a scary figure due to its growth from very small base figures, but it is still a warning about behaviour. All three of these breaches are AVOIDABLE. The right training can change the behaviour of employees and can help create a culture where data protection is the norm.

16.5% INCREASE IN EMAILS TO WRONG RECIPIENT

HEALTH, EDUCATION AND LOCAL GOVERNMENT SUFFER THE MOST

Data emailed to the wrong recipient has grown by 16.5% overall in 2021 Q2. The highest offenders were; Health **(+78%)**, Education **(+121%)** and Local Government **(+11.5%).** These three sectors are the biggest contributors to overall breach, so any changes and training are sure to have a significant impact on the total outcome.

GROWTH FOR RETAIL & MANUFACTURING

Retail and Manufacturing saw an increase in both cyber and non-cyber breach in 2021 Q2 vs the same period in the previous year, up **146%** for cyber and **170%** for non-cyber breach. Despite non-cyber being in decline **(-15%)** overall across ALL sectors in 2021 Q2, retail & manufacturing is in triple figure growth! This is a trend that is sure to cause concern. **Training, policy** and **procedure** could correct these behaviour type issues.

THE TOP 3 FOR CYBER AND NON-CYBER

The breach **type** with the largest share across ALL **Cyber** breach are;

- Ransomware **(21%)**
- Unauthorised access **(26%)**
- Phishing **(35%)**

Th breach **type** with the largest share across ALL **non-cyber** are;

- Data emailed to wrong recipient **(22%)**
- Data posted or faxed to wrong recipient **(14%)**
- Loss / Theft of data or data left in insecure location **(8%)**

WHERE DOES TRAINING COME INTO THIS?

Having a strong security culture will protect your organisation against cyber and non-cyber threats and possible data breaches. Keep in mind the average cost of a data breach, as well as a financial loss, this could also result in a loss of business projects, vulnerability to future attacks and a damaged reputation. The benefits of investing in good training, far outweigh the consequences of not having any at all.

Consultancy
A common sense approach to information and physical security.

Training
Training services to support a variety of organisational education needs.

Testing
Our testing, in line with our security, is holistic.