What action we've taken in Q4, what you've reported to us and what you can do to stay secure Data security incidents, which are breaches of the seventh data protection principle or personal data breaches reported under the Privacy and Electronic Communications Regulations, are a major concern for those affected and a key area

of action for the ICO. We have published this information to help organisations understand what we're seeing and help

What action we've taken in Q4

One fine

them to take appropriate action.



We fined The Carphone Warehouse Ltd £400,000 after serious failures put customer and employee data at risk. The company's failure to secure a computer system allowed unauthorised access to the personal data of over three million customers and 1,000 employees.

There were 957 reported data security incidents in Q4

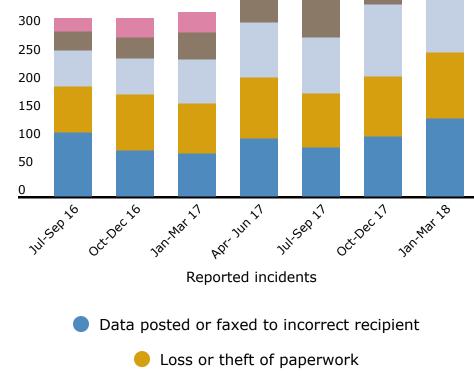
What you've reported to us



350

This was a 17% increase on Q3 (815 reports).

450 400



We believe recent increases are possibly due to increased awareness of the GDPR and the launch of our new Personal Data Breach helpline.

Data sent by email to incorrect recipient Failure to redact data

Failure to use bcc when sending email Total cyber security incidents per quarter

Jul-Sept 2016

Oct-Dec 2017 Jan-Mar 2018 40 50 60 70 80 90 100 110 120

most reported incidents

Data security incidents by sector, Q4 2017-18

Cyber incidents

Data posted or faxed to incorrect recipient

Other principle 7 failure

Loss/theft of unencrypted

Verbal disclosure

Insecure disposal of

paperwork

This does not include health sector data.

Reported incidents

Reported cyber security incidents increased by

This was the first month-on-month increase since Q4 of

31% in Q4 of 2017-18

2016-17.

General business, education and local government were again the sectors with the

Education

paperwork rose from 6 to 16.

Justice Data left in insecure location

Oct-Dec 2016

Jan-Mar 2017

Apr-Jun 2017

Jul-Sep 2017

Data sent by email to incorrect recipient Failure to redact data Failure to use bcc when sending email Charitable and giving

Loss/theft of only copy of encrypted data Loss/theft of paperwork

10 35 15 20 25 30 Education Cyber incidents 13 Data left in insecure location Data posted or faxed to incorrect recipient Data sent by email to 20 incorrect recipient Failure to redact data Failure to use bcc when sending email 31 Other principle 7 failure Insecure disposal of Loss/theft of only copy of encrypted data Loss/theft of paperwork Loss/theft of unencrypted

5

10

20

25

30

35

35

Reported incidents in this sector rose by 69% from Q3, from 35 to 59. Incidents involving data sent to an incorrect email recipient rose from 4 to 20.

Reported incidents in this sector rose by 32% from Q3,

from 96 to 127. Incidents involving loss or theft of

Verbal disclosure

Finance, insurance & credit

Cyber incidents

Data left in insecure location

Data posted or faxed to incorrect recipient Data sent by email to incorrect recipient

Failure to redact data Failure to use bcc when

Other principle 7 failure

Insecure disposal of

incorrect recipient

sending email

Loss/theft of only copy of encrypted data Loss/theft of paperwork Loss/theft of unencrypted Verbal disclosure General business 27 Cyber incidents Data left in insecure location Data posted or faxed to incorrect recipient Data sent by email to 14

Failure to redact data Reported incidents Failure to use bcc when sending email Other principle 7 failure Insecure disposal of paperwork Loss/theft of only copy of encrypted data Loss/theft of paperwork Loss/theft of unencrypted Verbal disclosure 0 10 15 20 25 30 35 **Local Government** Cyber incidents Data left in insecure location Data posted or faxed to 13 incorrect recipient Data sent by email to 9 incorrect recipient Failure to redact data 15 Failure to use bcc when 2 sending email 20 Other principle 7 failure

Insecure disposal of paperwork Loss/theft of only copy of encrypted data Loss/theft of paperwork Loss/theft of unencrypted Verbal disclosure 10 15 20 25 30 35 Legal

Cyber incidents

8

5

6

This follows a 22% rise from Q2 to Q3.

Data left in insecure location

Data posted or faxed to

incorrect recipient Data sent by email to

incorrect recipient

sending email

Failure to redact data Failure to use bcc when

Other principle 7 failure

Loss/theft of only copy of

Loss/theft of paperwork Loss/theft of unencrypted

Health sector in Q4

Insecure disposal of

encrypted data

Verbal disclosure

device

number of reports.

Health sector incidents by type, Q4 2017-18

Loss or theft of paperwork

Data left in insecure location

Loss or theft of unencrypted device

Failure to use bcc when sending email

400

380

360

340

Failure to redact data

Verbal disclosure

Principle 1 breach

Data posted or faxed to incorrect recipient

Data sent by email to incorrect recipent

50

year

most common.

bottom of this page.

120

Breach reporting is mandatory in the health sector. This contributes to the health sector having the highest

0 Various other principle 7 failures also accounted for a total of 121 further incidents.

20

10

There was a 21% increase in reported health incidents in Q4

320 300

2017-18 financial year round-up

Data security reports by month, 2017-18 financial year

280 260 240 220 200 180 Health sector in 2017-18 Health sector incidents by type, 2017-18 financial year Data posted or faxed to incorrect recipient Loss or theft of paperwork Data sent by email to incorrect recipient

160

180

200

220

240

Aside from health, general business was the

sector with the most reports in the financial

There were 362 reports in this sector - incidents of emails being sent to the incorrect recipient (50) were

Click here to download the csv or see the link at the

Full statistics on the financial year

Loss or theft of unencrypted device Principle 1 breach Insecure disposal of paperwork

Verbal disclosure

Data left in insecure location

Failure to use bcc when sending email

Failure to redact data

What you can do to stay secure

1. Consider metadata when redacting information.

Various other principle 7 failures also accounted for a total of 346 further incidents.

20

2. Check all data has been redacted and is not reversible before releasing. 3. Get someone to double check redactions.

We published the above information on 14 May 2018. We plan to update it each quarter.

Before releasing a redacted document, always follow these three tips: