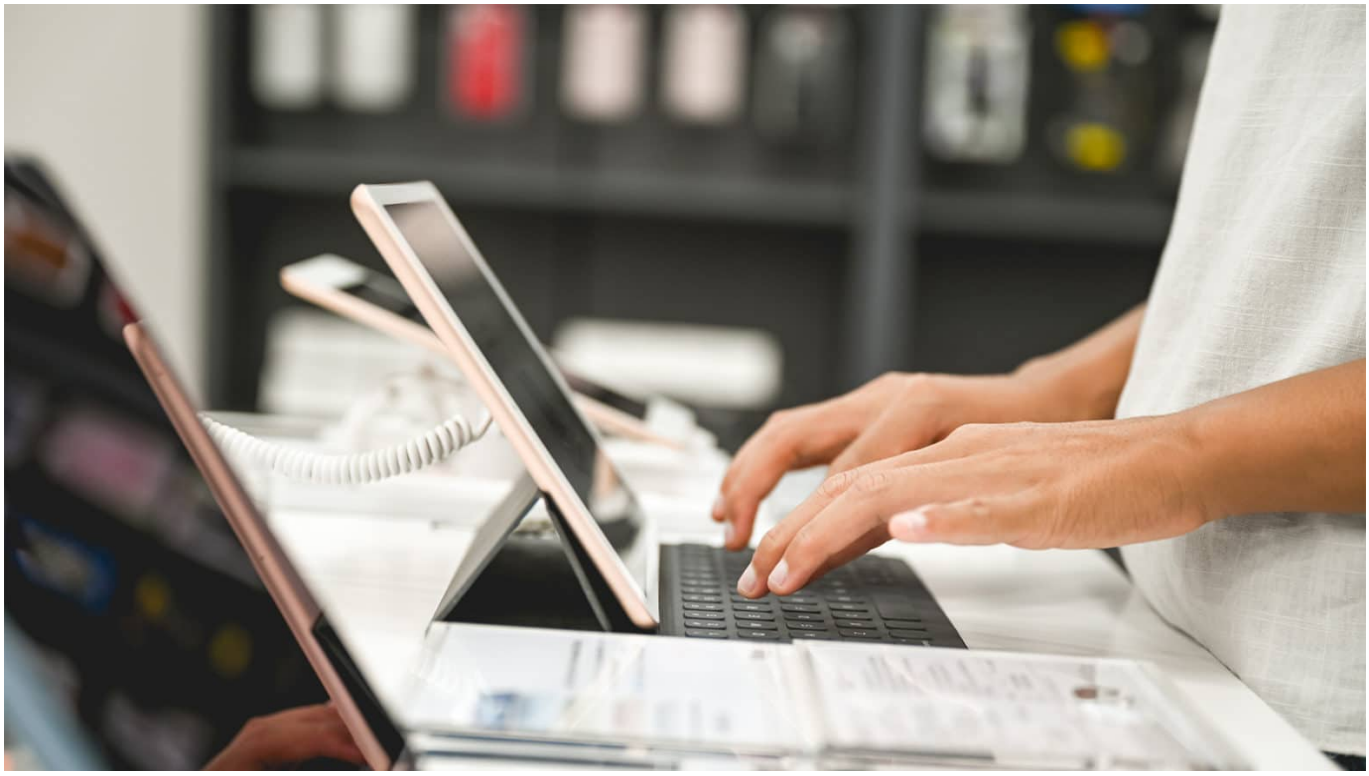
Help! An employee has stolen my data



Stop – don't panic. It is surprisingly common for an employee to (perhaps inadvertently) take material with them when they leave a company. Your first step is to identify what is missing and the risk to your business. We can then work with you to recover this information and help you put procedures in place to prevent this happening again.

What is missing?

Consider what the employee could have taken with them and the material they had access to prior to their departure. In particular, consider the following:

- Hardware – e.g. laptops, mobile phones, tablets.
- Emails – check the former employee's email account for suspicious emails. In particular, look out for emails to their personal email account or suspicious attachments.
- Client Databases – check whether they have accessed, downloaded, printed your CRM databases prior to their departure.
- Data Sticks – check what files have been exported from their work computer.

What are the risks?

Once you have identified what is missing, you can assess what the risk is to your business. In particular, you should consider whether the former employee may contact your customers, suppliers or poach other staff members. Further, the fact that data has been taken could amount to a breach of the Data Protection Act 1998.

What action can I take?

We have helped many different companies recover their confidential information and we can guide you through the process. If urgent action is required we can help you seek an injunction against the former employee (and their new employer) to prevent the use of this material or freeze their assets.

How can I stop this happening again?

Each business is different, but we can work with you to consider how best to prevent a future data breach. This can include taking practical steps, like ensuring you have appropriate IT systems / procedures, or checking your employment contracts / internal procedures are suitable.

Written by

Tom Bourne

Partner