resillion

Quality: Engineered. Tested. Assured.

Datasheet

Employee Data Theft

In our daily roles, many of us have access to a wide range of data, a large part classed as sensitive. This is any data that would pose a risk to the company if it was released to either a competitor, the general public, or got into the wrong hands from a data breach. This could be customer information, price lists, tender bid responses, IP, business information, classified information, or Human Resource personal and confidential data.

With the increased number of employees now working from home regularly, perhaps even using their own devices, it is imperative to ensure that your organisational data is secure. We all regularly access and work with sensitive information and although processes may be in place for security, employees are more isolated and there are fewer colleagues able to observe actions.

When an employee decides to leave

When an employee leaves an organisation, most will be cautious and aware that they should not take company information with them, however others may choose to deliberately (or naively) copy or take data that they feel will be of particular use to them.

What data they take will depend on their current role and the role they are heading to. Usually, the data in question is easy to access, and will save them time or make them look proficient in their new role. For example, an investigator working in a Digital Forensics position might take price lists, contacts, operating procedures, report templates, or even strategic business plans.

Employees occasionally believe that, as they have contributed to a project or policy, the information produced is theirs and not, in fact, owned by their employer. Alternatively, individuals will email their personal accounts from work accounts sending documents that will be useful to them.

What should companies do to prevent this?

When a staff member's resignation is accepted, get in touch with Resillion. We will conduct a digital investigation of the devices used by the respective employee to establish:

1. Emails that have been sent along with any attachments saved
2. Possible retrieval of deleted data
3. Report on external device usage
4. Analysis of file transfers
5. Cloud Forensics

Resillion Employee Assurance

Where it is known that an ex-employee has attempted to copy data, Resillion investigates the device(s), and confirms that the data has since been deleted or forensically removes it if not.

Previously we have assisted by creating a forensic image of the device, searching across for significant keywords, locating data of interest and then securely and forensically deleting said data. The device is then reimaged to confirm that the data has been entirely removed. This will provide independent confirmation that the data, once taken, has since been sufficiently deleted and removed from said device(s) so that it cannot be reinstated, allowing the employer and employee to come to a successful resolution.