3 SIGNS YOUR DATA ACCESS COULD BE OUT OF CONTROL

1.
YOUR FILE PERMISSIONS AND CERTIFICATION CHECKS ARE CARRIED OUT BY A CENTRAL IT TEAM

Responsibility for cybersecurity has become more complex. It's not viable for a central IT department to know who should have access to what anymore. They have no chance of knowing who should have access to what information, why and when. Only the business user who created the document and/or their team are really the ones in the know.

All staff need to know how to handle information safely and securely, how to spot incidents and what to do in the event of a breach. Therefore it should fall to the business users to certify access to their own data.

While SharePoint and other collaboration tools such as Office 365 and Microsoft Teams are great for sharing files, folders and sites, access can quickly get out of control.

'Sprawl' is one of the major drawbacks of collaboration platforms, particularly as it affects crucial business practices such as data governance, cyber security and data management.

Access to data is shared on average, up to 44X more than it is revoked, presenting a situation where 'who has access to what' accumulates and sprawls at a rapid rate.

2.
YOU'RE USING A COLLABORATION PLATFORM SUCH AS SHAREPOINT, OFFICE 365 OR MS TEAMS

3.
YOUR DATA GOVERNANCE PROCESSES ARE CARRIED OUT MANUALLY

Businesses simply have too much data, too many people, and change, for data to be effectively managed by manual processes or tools.

There are processes you can put in place to limit the likelihood of a security breach such as creating a full catalogue of sites, restricting permissions and providing clear site descriptions. However, these processes are highly manual, the extent of which is far beyond the resources of most small businesses.

WHAT'S THE ANSWER?

The Torsion platform works with collaboration tools to automatically monitor and detect any inappropriate access, out of date folders and permissions, duplication or the movement of files. If anything doesn't look quite right it will promptly alert a business user associated with the file and shut down any potential breaches.

Other than that, it can run seamlessly in the background until and unless it is required. Owners or creators of files and folders can certify and revoke access themselves, taking the responsibility away from the IT function.