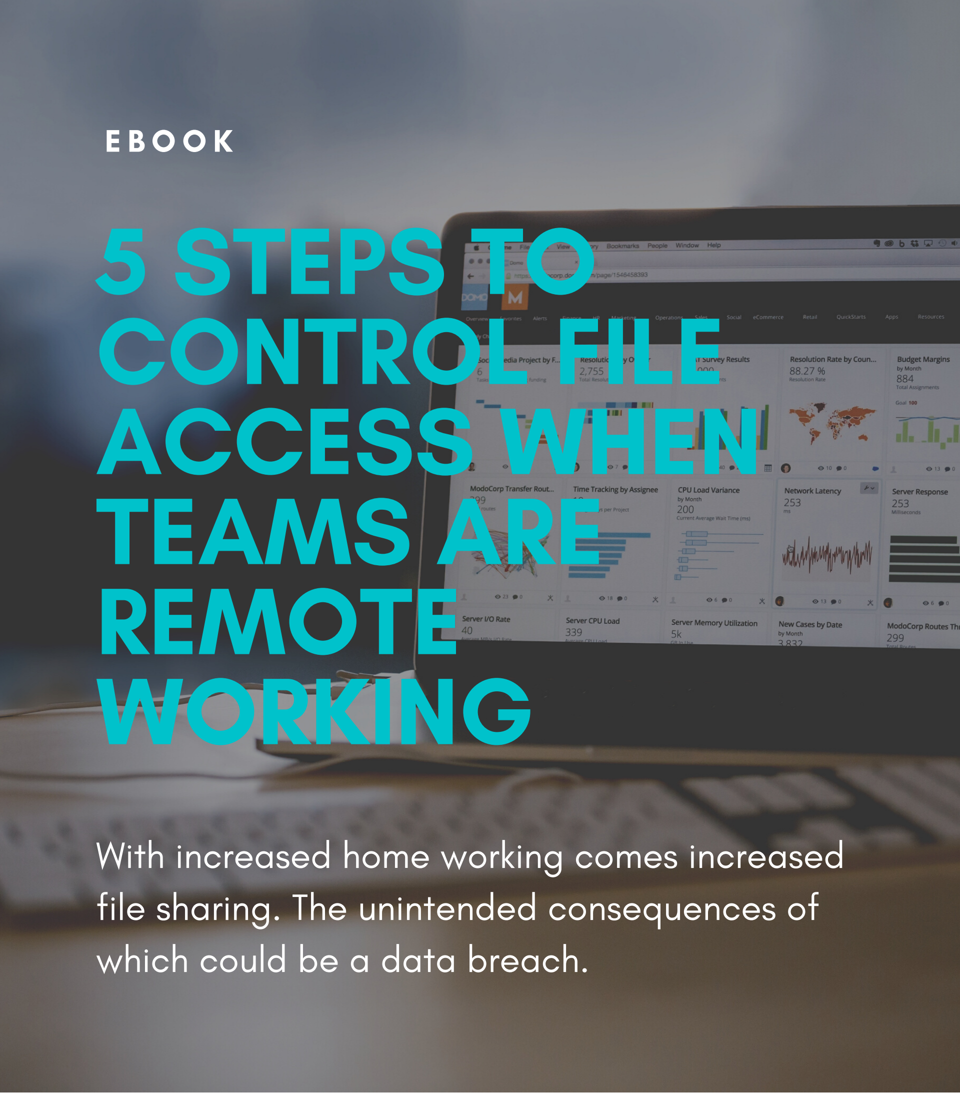
EBOOK



5 STEPS TO CONTROL FILE ACCESS WHEN TEAMS ARE REMOTE WORKING

With increased home working comes increased file sharing. The unintended consequences of which could be a data breach.

TORSION®
INFORMATION SECURITY

READ ON FOR OUR 5 TIPS FOR MORE SECURE HOME WORKING

Platforms like Microsoft Teams, Dropbox, Google Drive, Box, or Office 365 are great for sharing documents and can be really useful for team collaboration. But without the right measures in place it can be difficult to track where your data is being shared, by who, when and why.

Typically, files are shared 44 times more than their access is revoked. This leads to a spiral of out of control data even at the best of times. With the reported increase in usage reported by Microsoft, there will consequently be an unprecedented rise in the level of sharing too.

We can quickly see that at times such as this, it is even more paramount to establish and enforce clear data governance policies and remind business users of their responsibilities when it comes to avoiding data breaches.

1. AGREE YOUR POLICIES

When it comes to sharing files and compliance, you can't just implement collaboration platforms such as Teams or Office 365 without implementing data governance policies.

Agree how you are going to manage and share files throughout the entire organisation and then go ahead with it, no if's or but's. It has to be a totalitarian approach.

2. SHIFT RESPONSIBILITY AWAY FROM I.T.

Once you have communicated the policies and practices, how do you police them? You can’t stand behind your business users to make sure they are classifying the data correctly even when they are in the office. It is even less plausible to do it when your business users are working from home. And you can’t expect your IT team to do this within their role either.

3. MAKE BUSINESS USERS RESPONSIBLE FOR SHARING

Owners or creators of files and folders should certify and revoke access themselves. Only the business user who created the document and/or their team know how sensitive their files are and who should have access.

4. INTRODUCE AUTOMATION TO MAKE IT PRACTICAL

You have to rely on automation. The goal is to create a clear audit trail of who's got access to which data, why and when...without placing extra workload on your business users. Torsion works with collaboration tools to automatically monitor and detect any inappropriate access, out of date folders and permissions, or the movement of files.

Only with automation will you be able to stay in control of your data during increased remote collaboration.

5. STAY COMPLIANT

If we use the right automation tools to stay in control of who has access to what, why and when, we will consequently emerge compliant regardless of the volume of files being shared. Because data security is being automatically managed and controlled, when it comes to proving your compliance it's as simple as pressing a button to export a report.

TRY TORSION FREE

Get visibility of who has access to what, resolve security issues and put the power back in the hands of your business users.

Email 'FREE TRIAL' to info@torsionis.com or visit torsionis.com/get-torsion-free/

TORSION® INFORMATION SECURITY