

On the seventh day of Techmas Waterstons gave to me...

Breadcrumb

- 1. [Home](#) /
- 2. [Print](#) /
- 3. [Pdf](#) /
- 4. [Node](#) /
- 5. [Entity Print](#)

Insight navigation

- [Latest insights](#)
- [Latest news](#)
- [Articles](#)
- [Case studies](#)

[Download PDF](#)

Dec 2022

On the seventh day of Techmas Waterstons gave to me...

Several back up top tips

Categories Technology Consulting, Data & Analytics, Data Protection and GDPR

Dec 2022

-
-
-
-



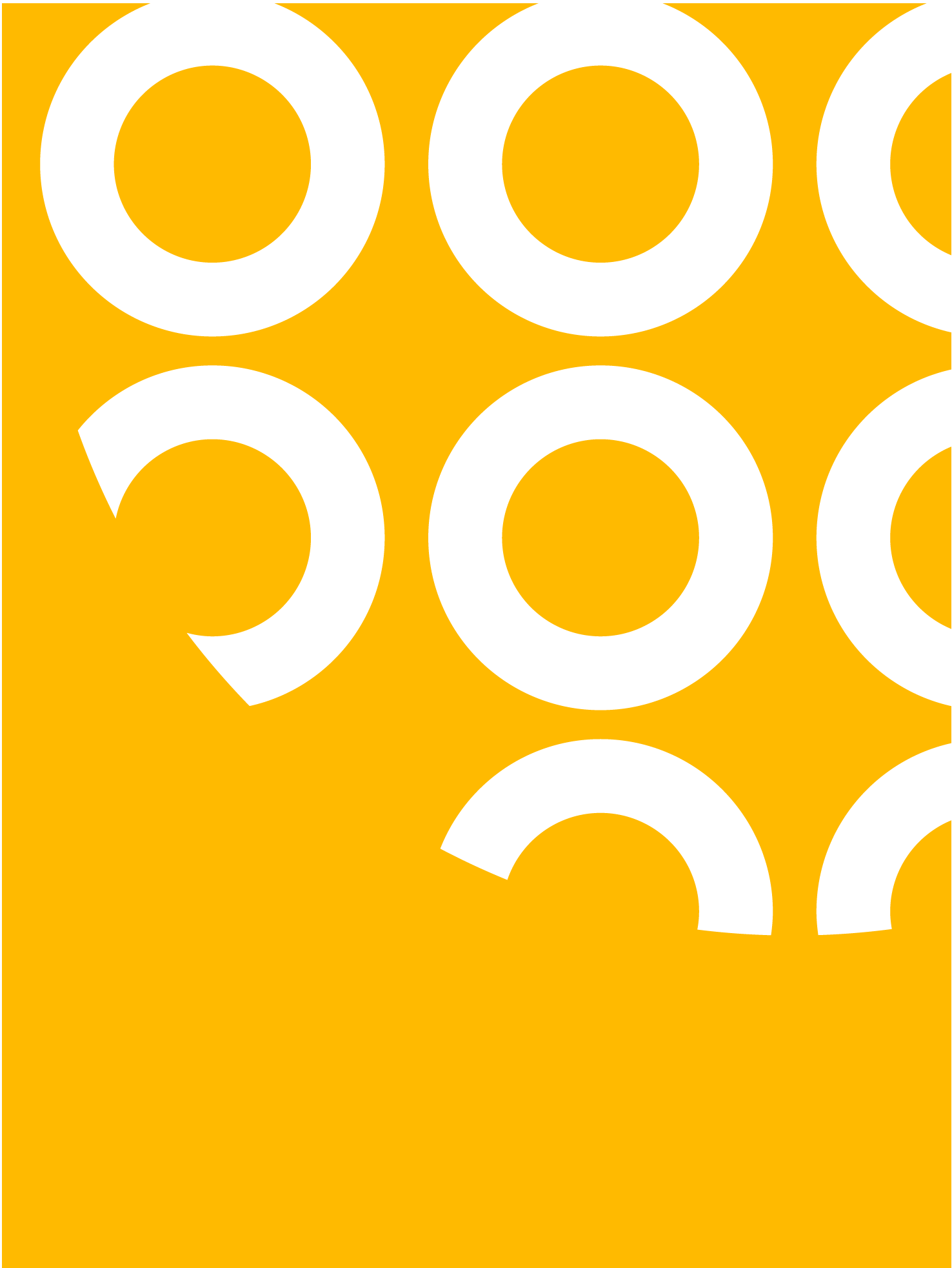
Andrew Quinn


Technical Strategy Lead

Email

andrew.quinn@waterstons.com







In a digital age, everything we create leaves an online footprint. Where in the past our important forms and documents were 'backed up' using carbon copy paper, we now must look for more technological options – and make sure they are used.

3-2-1

The venerable 3-2-1 rule for backups states that you should have:

- At least **three** copies of your data
- On **two** different media
- With **one** copy offsite.

This rule is good but needs updating for the modern context – for example, back in the day the offsite copy was probably on a tape, in a fireproof safe. It protected you not only from a localised disaster, but also from malicious action.

These days 'offsite' copies are often replicated across the network to another building or the cloud. The problem with networked copies is they're vulnerable to malicious (or careless) access. If a bad actor breaches your network and your backups are accessible on the network, they can be destroyed along with your live data.

Instead, consider that this one 'offsite' copy must now be 'offsite and immutable'. You don't need to put tapes in a safe (although that is still very effective), but you do need to make sure the data cannot be changed or deleted – even by one of your own administrators should their account be compromised (or they're having a bad day).

Testing testing

If you haven't tested your backups, you don't have any backups.

Just because a backup completes successfully, doesn't mean the data is recoverable.

Even if your backup runs a successful verification process, it could still be junk – it's checking its own homework at this point.

Just because it read and wrote identical data doesn't mean it was reading the correct data to begin with, or the data wasn't part-way through a modification when it was read.

The only backup that matters is the one you can recover from, and the only way to be sure that it's recoverable is to test it.

These days there are ways to automate many recovery tests, but a full disaster recovery rehearsal is the ultimate test of not just your data but also your processes.

To find out more about what Andrew discussed here about data backups, get in touch directly Andrew.quinn@waterstons.com

<https://waterstons.com/print/pdf/node/8470>