mytoolkit

Webinar: Backing up your business data

How and how often should your business back up its data?

Kit Barker
Chief Technology Officer

myhrtoolkit

Why should I backup my data?

- Lost devices
- Breakages and failures
- User error
- Malicious actors

- You have a duty to keep certain types of data safe
  - GDPR
  - Regulated environments or accreditation
- Worst case scenario: your business may fail if you don’t

myhrtoolkit

What should I back up?

- It’s impossible to back up everything

- Perform a simple audit of business data
  - Where is the data kept?
  - How critical is this to my business?
  - What would happen if we lost this?
  - How likely is this to happen?

- Consider centralising data storage to a single location

myhrtoolkit

All my data is in the cloud. I'm good, right?

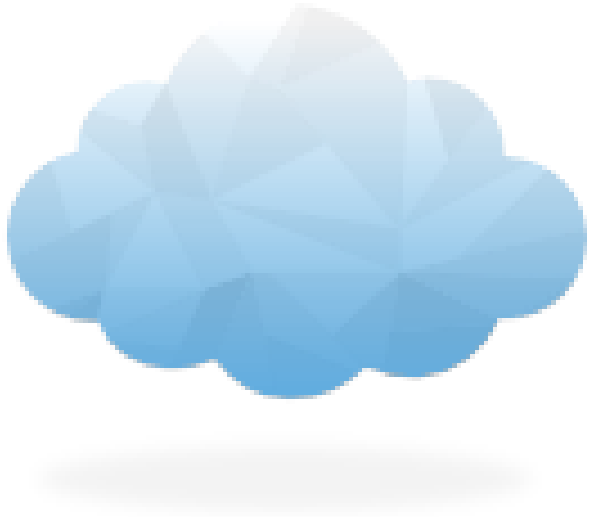
- Backups provide protection from:
  - Mistakes and deletions
  - Ransomware attacks
  - Corruption and breakage
  - Loss of access to your data

- Cloud storage is highly available and extremely durable
  - Availability – can I access my data when I need to?
  - Durability – can my data be retrieved accurately?
  - Google Cloud Storage has a typical availability of 99.99% and durability of 99.999999999%

myhrtoolkit

Cloud storage does not cover all bases

- No protect against changes to large amounts of data:
  - Ransomware attacks
  - Malicious actors
- Problems with your cloud storage provider
  - Aggressively handling unpaid invoices
  - Loss of access due to phishing attack



- Stored in the cloud does is not the same as “backed up”

mynrtoolkit

What is a good backup strategy?

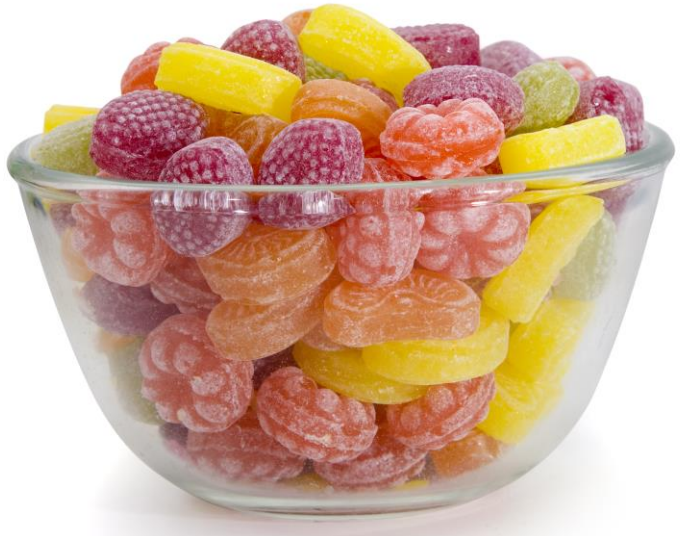
- Not all strategies are “good”
- Should be part of a Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP)
- A good strategy is:

✓ **Frequent**
✓ **Tested**
✓ **Secure**
✓ **Time limited**

myhrtoolkit

A good backup is… Frequent

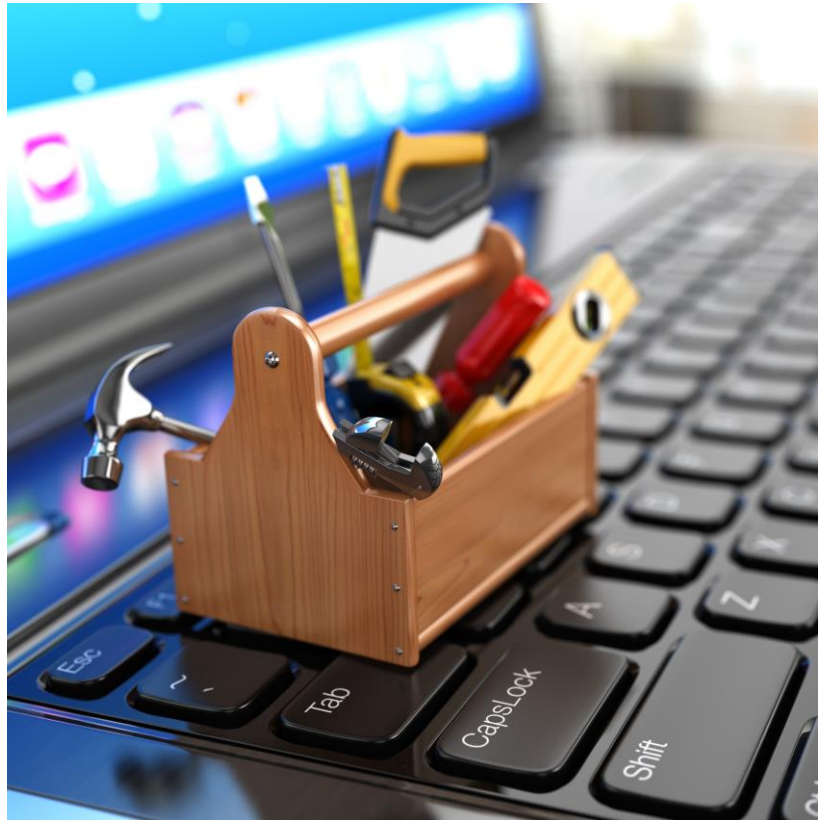
- Consider your desired Recovery Point Objective
  - RPO – the maximum amount of data, expressed in time, that you could lose in the event of a failure.
- RPO of 1 day is preferable
  - 1 week is better than nothing!
- Automation allows increased frequency



mynrtoolkit

A good backup is… Tested

- Do not assume that it works!
- Changes to processes and systems can cause breakages
- Have a regular test schedule
  - Set simple tasks such as recovering a file or mailbox
  - Fix any issues as a priority

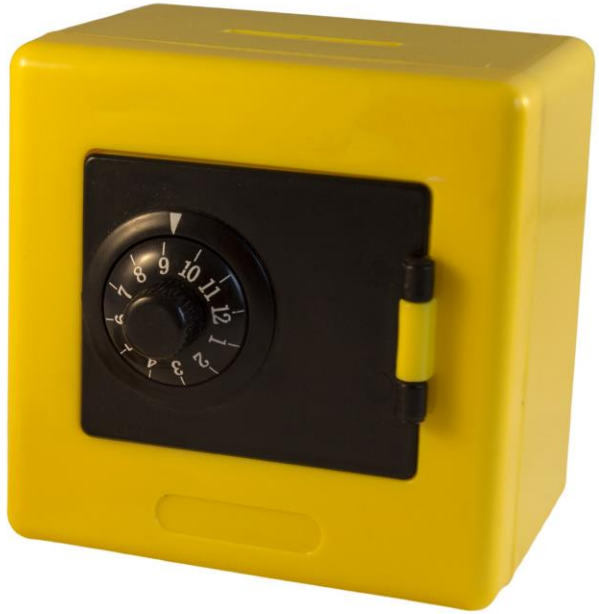


myhrtoolkit

A good backup is… Secure

- Backups need backups!

- Consider the 3-2-1 approach
  - 3 copies of your data
  - 2 different devices or media
  - 1 off-site location



- Encrypt your backups and restrict access to them

mynrtoolkit

A good backup is… Time Limited

- Don’t keep your backups forever
- Consider any legal duties
  - GDPR storage limitation
  - Regulatory requirements
- Automate if possible

myhrtoolkit

In summary

- Cloud storage providers are excellent but they’re not sufficient
- Consider disaster scenarios
- Audit your data
- Integrate backup in a disaster recovery plan
- Ensure your strategy is frequent, tested, secure and time limited

myhrtoolkit

Any questions?

mytoolkit

myHRtoolkit

Next webinar: Is your SME prepared for Brexit and changes to immigration law?