

Fear of failure

Roman Marszalek explains why it's worth keeping technology on your side

In a working environment that is becoming increasingly high tech, competitive and credit crunched, the room for error is non-existent. What does this mean for lawyers relying on technology to do their jobs? How does this affect the processes put in place to protect vital information?

Franklin D Roosevelt's inaugural address during the depths of the depression is being re-quoted almost daily. "The only thing we have to fear is fear itself," he said. Motivating during our current economic misery, but I can't help thinking "that's a man without a machine to worry about."

Technology runs through every aspect of daily life and when time is taken to manage it well it can make the impossible schedule, the enormous workload, the requisite research manageable. But when the pressure is on, it's often the last thing on anyone's mind. Promises to back up are forgotten, policies to avoid the use of flashdrives ignored, best practice to ban saving onto inaccessible laptops seems irrelevant. Some people never realise how valuable their data is until they lose it.

Lawyers today use a plethora of technical wizardry to keep them connected. As the number of ways of storing, sharing and searching for information increases, the risks go up. There are so many horror stories: a laptop left in the back of a cab, a system crash minutes before deadline, a missing file that could have got into the wrong hands. The way to reduce the risk is to ensure that the systems are in place to back up vital files, store securely and retrieve when needed at a moment's notice.

Automatic backup

Automatic backup is a must. At your busiest, when you have no time to re-do the work, you probably also don't have time to backup your computer. Backup should be set to work behind the scenes, online if possible, and continuously. Backed-up media should be stored

offsite, either within the organisation or with a third party. Systems that are critical to operations must be frequently fault-tested to ensure downtime is avoided. And vulnerability to power failure can be reduced with the adoption of an uninterruptible power supply.

If this seems like something that should be the responsibility of your IT department, it should. But the credit crunch has hit hard on the UK's tech teams. As technology specialists, we see that the weak economy will undoubtedly push IT positively to deliver more for less. But it will also bring out the worst traits of IT departments and the consultants they hire: agreeing to impossible targets

“ Lawyers today use a plethora of technical wizardry to keep them connected ”

without question, making mistakes on a large scale because of a short-sighted focus on saving money and sensible caution turning into nervous inertia when it comes to investing.

You wouldn't drive a car without insurance, or run a business without a strategy. Blindly trusting to luck that every employee will store their vital files with care doesn't make commercial sense. This is a time when mistakes really cost—in terms of reputation as well as the bottom line.

So what should you be doing? Until computers never crash, people never make mistakes and gremlins don't thrive in offices, you need to know that vital information is stored effectively, backed up automatically and can be retrieved in good time.

- Check your business practices and guidelines for storing, copying and sharing files. Does everyone in your team know the policy for file storage?
- Are your business processes split over more than one site? If so, find out if there are duplications of files, issues

with version control or the risk of losing a file between multiple servers.

- Insist your office provides a UPS (Uninterruptible Power Supply) to reduce vulnerability to power failure.
- Store your backup media offsite for business continuity, preferably to multiple destinations.
- Fault test high-availability or critical applications to ensure minimal downtime.
- Find out if your IT team is taking advantage of RAID (Redundant Array of Independent Disks) and disk mirroring for LAN (Local Area Network) servers to guard against data loss and to ensure continued availability of data.
- Investigate whether your IT supplier or department has spare equipment that can be used in the event of equipment or component failure.
- Run your backups minute to minute,

from office-based computers and remote devices.

- Protect your data during backup transfer. Confidentiality is a business imperative and all backups should be strongly encrypted (448-bit encryption key).
- If using a third party for online backup, choose a UK provider as physical restores will be faster and there may also be legal implications of storing your and your clients' data abroad.

The news is full of IT horror stories and fear of IT failure is all too real. Closing statements, witness testimony, contracts, contact numbers might all be stored on your laptop and vulnerable. If the thought of losing them doesn't make you nervous, it should. Fear should motivate everyone to take the steps needed to avoid data loss.

NLJ

Roman Marszalek, managing director and founder of London-based IT specialist Dr Logic. E-mail: genius@drlogicbackup.com. Website: www.drlogicbackup.com