Picture credit: AdobeStock

BACK UP!

Iwona Zalewska *explains how adopting the 3-2-1 back-up rule can safeguard personal and corporate data*

People are on the move – to and from the office, working from home or logging on at remote sites – and this means their data, and that of their company, is at risk. Data loss or data inaccessibility comes in many forms and often at the most inopportune moments. It could be due to a cyber attack or a personal fraud attempt, it could be a power failure or an environmental threat such as water damage, or it could be human error. Either way the impact can be devastating for businesses and individuals. The costs of data breaches to companies are growing every year, but the risk of legal action and reputational damage are also immense.

Despite multiple awareness campaigns and data loss headlines in the media, it's surprising how many companies still leave themselves vulnerable to the risk of data loss. According to the 2021 Data Risk Report from Varonis, one-third of the folders used within a company were accessible by everyone and only 5 percent of folders were protected. Added to that, a study conducted by Censuswide for Beaming, found worrying backup practices among businesses. Up to a quarter of businesses do not back up their company data at all, while 12 percent maintain a single copy of data, stored either on individual computers or on a single server. The same proportion of businesses leaders admitted to being unaware of any backup strategies in place at their firms.

It's surprising how many companies still leave themselves vulnerable to the risk of data loss

Protecting data by backing up is a topical issue right now. World Backup Day, an annual event designed to raise awareness about the importance of regularly backing up digital data took place on 31 March. The event came about because of a post on Reddit from a user who had lost his hard drive and regretted that he'd not been reminded about the importance of backing up data. Among the stark facts on the World Backup Day website is that 21 percent of people have never made a backup, and 29 percent of data loss cases are caused by accident.

Indeed, while most of us are aware of the dangers of cyber attacks and take precautions to protect our data from phishing and other malware, the risks of losing data in other ways are equally worrying. According to the Verizon 2024 Data Breach Report, 68 percent of breaches involved a non-malicious human element, like a person falling victim to a social engineering attack or making an error

Despite the clear risks to data security, straightforward processes to implement backups are all too often missing from organisational practices. The result of this oversight leaves both companies and their employees unnecessarily exposed to potential data loss.

Let's consider some of the most common reasons businesses have given for experiencing data loss…

Human Error: When data backups rely on manual execution rather than automated processes, human error often comes into play. With employees juggling multiple tasks and dealing with vast amounts of data, backups can easily be overlooked.

Budget and Resource Constraints: Setting up reliable backup systems demands a dedicated budget, skilled personnel and sufficient storage capacity. Smaller businesses or those focused on other priorities may not allocate the necessary resources for proper data protection.

Over confidence: Some organisations mistakenly believe that catastrophic data loss won't happen to them. Despite high-profile incidents, they assume their primary storage systems are secure and fail to prepare for worst-case scenarios.

Outdated Technology: Businesses using legacy storage systems may struggle to integrate them with modern backup solutions. These older infrastructures can complicate backup procedures.

Lack of Planning and Protocols: In many cases, there is simply an absence of clear policies, assigned responsibilities and structured processes for conducting consistent and thorough data backups.

Insufficient Security: A Fastly report from November 2023 revealed that 29 percent of organisations identified data loss as the most common damage caused by a security breach. Safeguarding stored data is key.

Data backups should be seen as a critical aspect of data security, with automated systems in place to backup important files regularly. This process begins with maintaining a comprehensive, updated inventory of systems, folders and data files requiring backup. Companies should also determine backup frequency based on their operational needs.

There are various backup options available, from cloud storage and online services to physical devices like USB flash drives and optical media. Using a combination of methods adds layers of protection against data loss. However, it should be noted that cloud backups can be affected by cyber attacks, potentially making vital data temporarily inaccessible during a breach.

Using external encrypted SSDs as a backup provides access to terabytes of gated, air-gapped storage that is easily accessible to users, but keeps data offline and away from internet access where it could be targeted by hackers. If a cyber attack or system failure were to occur, these drives allow businesses to restore their files and folders from the latest backup date.

THE 3-2-1 METHOD PUTS GUARDRAILS AROUND PRECIOUS AND SENSITIVE CORPORATE DATA

For companies that have already suffered data loss whether through a ransomware breach, a power blackout or even the theft of an employee's laptop, it can be too late to get back critical files. However, for those with data intact, a solid backup plan can provide an essential layer of protection. A great example of this is what's known as the 3-2-1 backup method. This approach can mean the difference between catastrophic data loss and a swift return to normal operations.

The 3-2-1 backup strategy is a simple framework that delivers a proven and effective data protection method: **3 copies of the data –** the company's original data and two backups. **2 distinct methods of media storage –** including internal hard drives and external SSDs. **1 copy stored off-site –** preferably this is air-gapped from the internet and stored away from on-site backups.

By following this plan, organisations and individuals can mitigate against a wide range of failure situations, from natural disasters to cyber attacks, ensuring their critical data remains accessible and secure. Simultaneously, systematic testing of backups should be carried out to check that stored data has not been corrupted or tampered with and can be rapidly accessed when it is needed, providing confidence that any disruptions can be handled smoothly.

Not every file requires the same level of protection. Companies can begin by identifying the most vital data, the loss of which – if compromised – could impact the organisation's operations or security. These files should be kept separately and their protection should be prioritised so that the 3-2-1 strategy is targeted at the most important data for the company.

This might be:

Sensitive data that would be challenging to recover or recreate.

Essential operational data that is needed for daily business functions.

Compliance or Legal data that must be held to meet regulatory purposes.

Ransomware typically attacks by encrypting data – and not only primary data – but any network-connected backups. If all of the backups that are created by a company are linked to the central network, this makes them vulnerable to remote access and loss. Here's how each part of the 3-2-1 approach builds a barrier against total data loss:

A SOLID BACKUP PLAN CAN PROVIDE AN ESSENTIAL LAYER OF PROTECTION

Three copies of data

By maintaining three copies of the data – the original plus two backups – organisations are able to build in redundancy. If one copy is compromised, there are two others to fall back on, allowing all operations to continue business as usual with minimal disruption.

Two different types of storage media

Spreading backups across different storage media, such as a local server and an external encrypted SSD, gives companies an additional safeguard. Device failures, though rare, do happen, and creating backups on two media types drastically reduces the likelihood of simultaneous loss.

One off-site, air-gapped backup

Storing a backup off-site provides an additional, essential layer of security. This physically isolated copy should ideally be air-gapped, meaning it's not connected to the internet or network, stopping it from being compromised by remote cyber attacks. For example, an air-gapped backup could be kept on an encrypted SSD and withstand brute-force attacks.

Implementing a 3-2-1 backup method goes way beyond cyber security best practices – it can also save companies significant costs in the event of data loss, hence protecting the bottom line. Timed, but frequent backups – perhaps on a daily or weekly basis – limit the chances of data loss and ensure recovery efforts restore the most up-to-date information.

The financial ROI for a backup strategy like this is obvious – investing in backups now can prevent expensive ransom payments, unplanned downtime, the cost of fighting legal action or dealing with regulatory fines and emergency IT interventions at a later date. For small and medium-sized businesses with limited IT resources who lack the security teams and data protection of bigger organisations, the absence of a secure backup strategy poses an even greater risk. A single ransomware attack could cripple operations.

While the 3-2-1 method not only helps companies to ensure business continuity and protect their reputation, its key role is to put guardrails around their precious and often sensitive corporate and personal, data – the lifeblood of their organisation. There is too much to lose by leaving it to chance and not prioritising regular and comprehensive data backups. The Annual Backup Day is a useful reminder of what needs to be done, because if an organisation experiences a totally preventable data disaster, laziness, human error and lack of planning will be a poor excuse ●

Iwona Zalewska is Regional Director for UK & Ireland, DRAM Business Manager, EMEA Region, at Kingston Technology Europe.

21 percent of people have never made a backup and 29 percent of data loss cases are caused by accident

Picture credit: Tippa Patt/Shutterstock