BEYOND blue

INSIGHTS

In collaboration with redstor

BACKUP AND *RECOVERY*

Sounds simple, but is it?

WHY DOES IT MATTER?

Backup and recovery should be a critical part of every organisation's cyber resilience. The interest and focus on cyber within the C-Suite has shown a much-needed shift from the traditional view that cyber security should be a technical control dealt with by the IT department, to a realisation that a more holistic approach to resilience is needed.

Moreover, the intrinsic value of data has soared in recent years, as organisations are increasingly always-on, and technology makes its way deeper into all departments. The rise of remote-working and rush to the cloud (sparked in part by the COVID pandemic) has left IT teams facing mass proliferation of data, and users at greater risk of data loss, less able to access support and susceptible to the ever-prominent threat of ransomware.

Data integrity is a key concern with backups. They must be stored securely, uncorrupted and recoverable in the face of increasingly sophisticated efforts by attackers to corrupt those backups. Compliance, industry and legal regulation for data protection and retention must be respected, with policies that inform how data is managed.

BEST PRACTICES

The process of backing up data need not be a complex one. Whilst there is a raft of solutions available to suit teams and budgets of all sizes, in many instances modern backup solutions can be set up in a matter of hours.

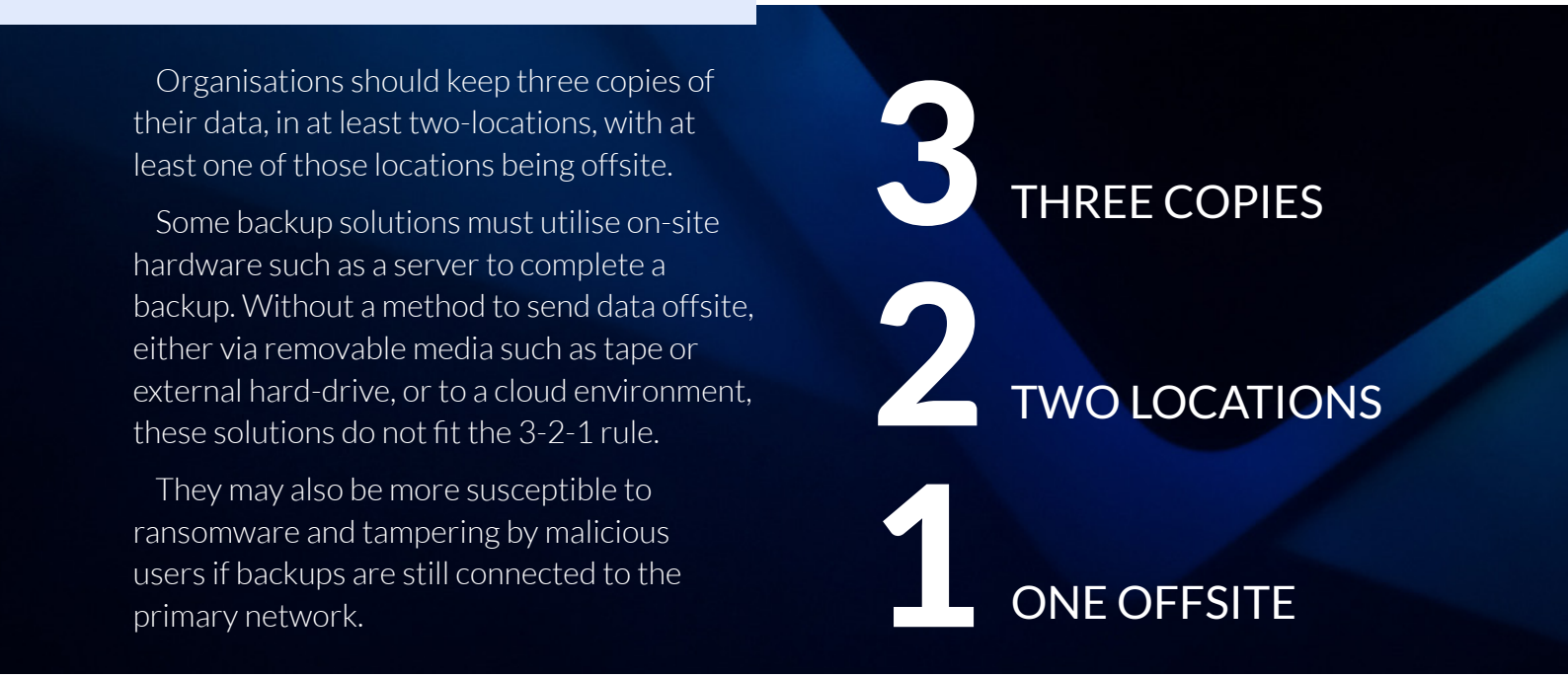
The UK's National Cyber Security Centre (NCSC) list backup as a key component of data security and have issued guidance on what organisations should consider. Not all backup solutions are created equal, so here are some of the key considerations, informed by the NCSC guidance.

THE 3-2-1 RULE

Organisations should keep three copies of their data, in at least two-locations, with at least one of those locations being offsite.

Some backup solutions must utilise on-site hardware such as a server to complete a backup. Without a method to send data offsite, either via removable media such as tape or external hard-drive, or to a cloud environment, these solutions do not fit the 3-2-1 rule.

They may also be more susceptible to ransomware and tampering by malicious users if backups are still connected to the primary network.



IMMUTABILITY AND OFFLINE BACKUPS

An organisation's backups should be both **immutable and offline**. This offers a resilient approach to help ensure data recovery in a ransomware event, which can only be a good thing with the continued threat of ransomware to organisations.

An offline backup is only connected to a live network when absolutely necessary, such as when a backup is in progress. The backed-up data is then stored separately from the live network.

An immutable backup is one which cannot be altered following its completion. This ensures the backed-up data cannot be infected by ransomware, and that the backed-up data cannot be deleted, maliciously or accidentally.

In addition, as organisations look to implement cyber insurance to mitigate the impact of a ransomware incident, insurance underwriters are increasingly asking organisations to follow similar guidance or risk higher premiums or be unable to purchase policies. Use the insurer's assessment process as part of a layered approach to security. It is a helpful opportunity to review and strengthen cyber security controls. Organisations should not rely on cyber insurance to pay a ransom demand but should expect that the insurer will cover the least expensive method of returning to BAU, which in some cases may go against the organisation's own ransom policy.

HARDWARE VS BANDWIDTH

Backup services and solutions can be split in to two categories:
1) those that take a hardware-based approach and
2) those that utilise the cloud to securely send data offsite.

There are positives and negatives to both approaches. These include billing models, implementation times and speed of recovery. The weighting of these concerns with vary depending on the needs of the business.

Typically, a hardware-based approach leverages a server on-site to offer faster recovery speeds. However, data will still need to be replicated off-site in some manner and set-up times are usually lengthened by the need to wait for hardware implementation.

When it comes to cloud-based solutions, the challenge that is most often cited is the lack of bandwidth availability and the possibility of slower restores. However, cloud-solutions could provide additional flexibility, can be billed on a 'pay-as-you-go' model and – most importantly – facilitate easy access and availability of data.

So, is there an approach that organisations can take that leverages the flexibility and rapid set-up offered by the cloud, without having to compromise on speed of recovery?

FOCUSING ON RECOVERY

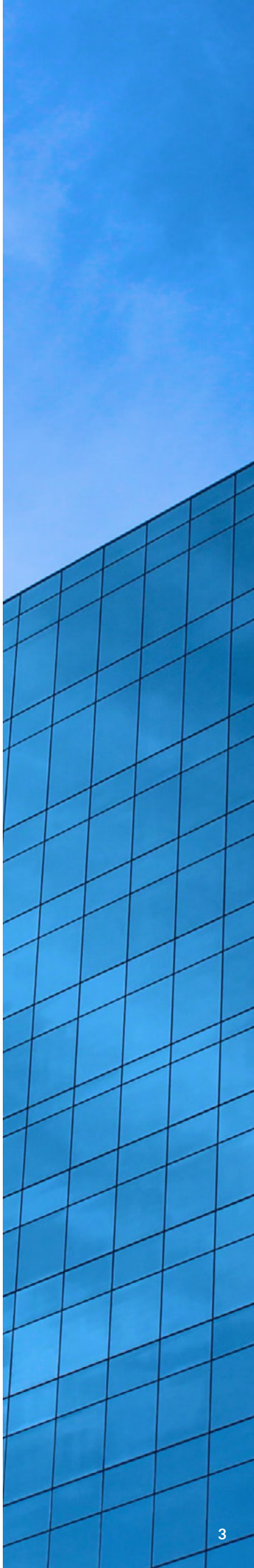
There are many methods of backing up data and comparisons can be made between different solutions while taking these into account. However, when organisations begin with the end in mind and focus on recovery, some solutions clearly stand out from the crowd.

In a disaster scenario, be it a fire or flood, or a user-side disaster such as the urgent need for access to a file that's gone missing, recovery is what will save the day.

In reviewing solutions, there are two critical metrics that should be understood: **recovery time objective** (RTO) and **recovery point objective** (RPO). Respectively, these help an organisation understand the acceptable speed with which recovery must be completed and the acceptable level of data that can be lost should the worst case scenario materialise.

Regardless of the priority between RTO and RPO, a further metric which can often be directly correlated to loss of sales or increased costs is the **amount of downtime** in the event of a disaster.

Downtime can be defined as the length of time between an incident taking place and the RTO being met. A 2014 Gartner study stated that the average cost of downtime for organisations was as much as $5,600 per minute, meaning that 24-hours of downtime could cost a business millions of dollars.



CRISIS MANAGEMENT

The media seems to be filled with news of high-profile ransomware attacks, many of which appear to be increasingly motivated by political factors. To avoid such an attack, it is essential to complement technical security controls with a dependable and effective backup strategy, to ensure that your data will be secure and rapidly available.

Recovery times for ransomware attacks often run to many months, as organisations face the challenge of rebuilding and securing their IT estate. They often find unsupported systems and corrupt or incomplete backups as they do so. We've noticed a common fallacy amongst many organisations: the assumption that having a backup plan in place will be sufficient. Unfortunately, this is often not the case. Regularly testing your backups is critical to ensuring you can regain access to your lost files, restore them and successfully recover from a ransomware incident.

Cyber exercising can also play a part in helping executives understand the impact of a cyber-attack, creating a safe environment which allows organisations to observe and practice their response capabilities. It also helps underline the importance of recovery plans and organisational resilience.

WHAT SOLUTION IS THERE TO ENDING DOWNTIME?

With more data sources than ever, the ideal solution needs to be able to protect multiple data sources without the headache of multiple windows, management consoles and platforms for teams to look after.

The solution needs to couple the recovery speed of hardware-based solutions along with the flexibility of cloud, allowing downtime to be minimised and RTOs and RPOs to be met.

With the growing threat of ransomware, users must also be confident that DR plans can be made around the solution so the ability to test a recovery from a disaster scenario must be as simple as testing the recovery of a single file. Testing your backups to validate data can be restored is vital to recovery and can help in identifying potential gaps before it's too late.

Additional features such as malware detection for backup data also gives organisations the ability to meet the National Cyber Security Centre's guidance and take a 'defence-in-depth' approach to keeping data secure.

Importantly, the solution must also be cost effective, simple to implement and simple to manage. Today's world is on demand and your data management should be too. Firms like Redstor are leading the industry in data management.

IN SHORT...

Managing data confidentiality, integrity and availability is by no means an easy process.

Cyber response plans should not be considered reliable or effective until they have been exercised. No matter how well designed a plan appears to be, realistic exercises should help identify issues and validate assumptions that require attention.

Take a holistic approach to defining your organisation's backup objectives, thinking about what data assets really matter and which systems must be recoverable, and make sure your solution is robust in a range of severe but plausible scenarios.

HOW DO BEYOND BLUE AND REDSTOR WORK TOGETHER?

As part of an alliance partnership, Beyond Blue and Redstor work together to deliver strategic cyber-security and resiliency which is underpinned by smart data backup and recovery.

With a wealth of knowledge held between the two organisations, businesses can benefit from the expertise delivered, tackle their most complex cyber challenges, and ensure data is at the heart of decision making.