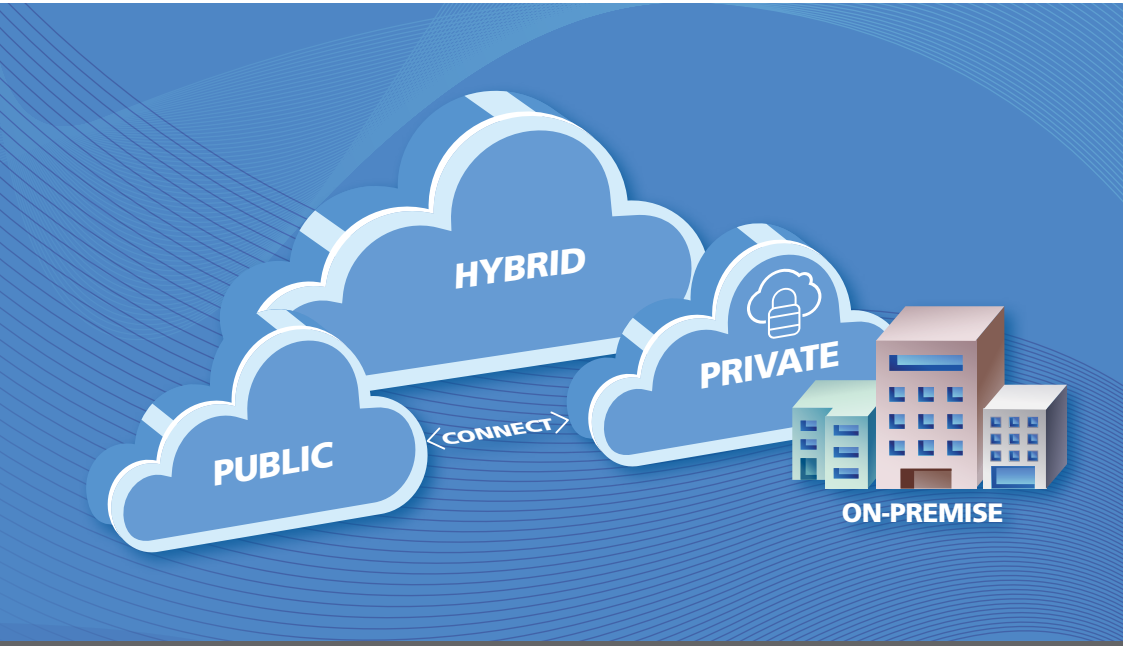
Breathe Easy –
Private Cloud



OFFLINE BACKUPS IN AN ONLINE WORLD

For Businesses

breathetechnology
support | cloud | security | infrastructure | comms

EMPOWERING BUSINESS THROUGH SECURE TECHNOLOGY

ISO 9001:2015 CERTIFIED COMPANY
ISO 27001:2013 CERTIFIED COMPANY
bcs Chartered IT Professional
Chartered Institute of Information Security
CISP
National Cyber Security Centre
CYBER ESSENTIALS
TOP CYBERSECURITY CONSULTING COMPANIES IN 2023

Craig Van Aswegen
MD & Snr IT Management Consultant
Breathe Technology LTD

"The NCSC has seen numerous incidents where ransomware has not only encrypted the original data on-disk, but also the connected USB and network storage drives holding data backups. Incidents involving ransomware have also compromised connected cloud storage locations containing backups.

In response to recent ransomware incidents, this document supplements our existing guidance to help you protect your backups stored in the public cloud. The four rules outlined below should be kept in mind when using the cloud to store any of your backups."

1. The offline rule

At any given time, are one or more backups offline?

The purpose of an 'offline backup' *(sometimes called a 'cold backup')* is to remain unaffected should any incident impact your live environment. You can do this by:

- only connecting the backup to live systems when absolutely necessary
- never having all backups connected (or 'hot') at the same time

With at least one backup offline at any given time, an incident cannot affect all of your backups simultaneously.

Using cloud storage to hold an offline backup is a good idea because it guarantees physical separation from your live environment. Crucially, when your offline backup isn't in use it also needs to be digitally disconnected.

Unlike conventional backup storage, you cannot take your cloud storage offline by simply unplugging it. However, there are a few steps that can be taken to apply the same level of protection.

Identity management

The first step to protect cloud storage is secure account identity. For cloud services this almost always appears as username and password credentials. All users able to access cloud backups should be properly protected in line with NCSC guidance. Without a trusted identity, ransomware should not be able to request access to your cloud storage and encrypt it.

Client management

A backup client is a device with credentials to access your cloud storage. Cloud backup clients should not have valid credentials while your cloud storage is not in use. The number of backup clients should also be kept to a minimum with standard user devices unable to modify cloud backups directly. Following this practice, a ransomware infection can only compromise your cloud backup if it occurs on an authorised client and while your cloud backup is being used.

Access control

Some cloud storage services offer more advanced access controls for identity and connectivity. If these controls are available, they should be configured to only allow authorised clients to create new backups (or append to existing ones), and deny connection requests while the storage is not in use ('cold'). If a ransomware infection occurs while your cloud backup is offline (denying connection requests), it will not be able to reach the cloud storage, giving you the same level of confidence as unplugging an on-premises storage drive. In the event of a ransomware incident occurring whilst your cloud backup is connected, ransomware acting with privilege to only create new data cannot overwrite your existing backups. This is comparable to traditional write-once storage (but is cheaper and more scalable).

2. The recovery rule

Is the data in cloud backups restorable and recoverable?

While all measures can be used to try and prevent a security incident from affecting your backups, it's best to have a backup plan for your backups. Some cloud storage services allow you to restore modified data back to an older version, and recover deleted data for a limited time after it was deleted. If ransomware does manage to affect your cloud backup, you can use these features to restore back to the last known-good state. When choosing a cloud storage provider, you should check that these features are included in the service.

3. The 3-2-1 rule

Is critical data saved in multiple backup locations?

It is vital to keep multiple backups and to logically separate them. Maintaining resilient backups means that if one is compromised, at least one other remains. The most common method for creating resilient data backups is to follow the '3-2-1' rule; at least 3 copies, on 2 devices, and 1 offsite. This strategy is popular because it scales effectively *(including the use of the cloud for an offsite backup)* and can give you confidence that your critical data is safe from a localised incident. However, it does not require any backup location to be offline – hence the need for our first offline rule.

4. The regular rule

Is critical data backed up regularly?

Finally, backups should be created on a regular basis. The more frequently backups are created, the less data is if you're forced to recover. Not only should your backups be created frequently, they should also be regularly tested to check they work as expected.

I think that the saying 'every cloud has a silver lining' is quite apt in this situation. The silver lining of recent incidents is that cloud backups are being created. By asking yourself these questions and following the guidelines, you can make your cloud backups more resistant to incidents like ransomware.

James L – Cloud Security Researcher

10 Reasons why we need a backup review

1. The current backup system was designed in 2017. **It is out of date.**
2. By the nature of it, there will be various issues that crept in over the years as things are used, maintained and updated.
3. There has been significant system changes and additions of new offices.
4. The NCSC has urged organisations to bolster up their security due to the high levels of attacks on businesses.
5. NCSC has release new minimum guidelines for backup. www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world
6. The Citrix Orchestra (Business Continuity) System doesn't work anymore.
7. The Backup Plan must be documented.
8. If we rely on 3rd Party's to provide Cloud Solutions as Core Systems, then we must review their backup & DR (This comes from ISO 27001 – Security)
9. Backup is not an I.T. decision. It's a management decision, but deployed and managed by I.T.
10. Downtime today has a bigger impact than in the past. We are completely reliant on the I.T. being available to fulfil the Teaching and Learning responsibility and almost all other supporting functions.

Cyber Attack Scenario?

BBC NEWS Debenham High School I.T. system by cyber attack

A high school has said it's I.T. system have been subjected to a cyber-attack.

Debenham High School, in Debenham, Suffolk said all its computer facilities were offline as a result of the hacking.

In a letter to parents, the head said police had been informed and there was no evidence that any data had been compromised.

The school said it was working to restore the systems before the new school term started.

Headteacher Simon Martin said: "Although it is difficult to provide recise timescales for a full restoration, the support team has assured us that due to the safeguards we have in place, the restoration process should happen more quickly." Work completed over the hlidays by students is currently not available to access.

"Staff are aware of this situation and please do not worry if any work had not been completed." The high school is a Church of England specialist academy.

sky news

Schools are 'powerhouses of data'

The National Cyber Security Centre, which is part of GCHQ has previously warned of an increase in ransomeware attacks affecting the education sector. This is when criminals gain access to a victim's network to plant malicious software designed to block access to a computer system until money is paid.

CAMBS TIMES

UK set to blame China for hack on elections watchdog

The UK will "stop at nothing" to protect against cyber attacks, a Government minister said, as China was set to be accused of targeting the elections watchdog.

The Government is expected to say Beijing-linked hackers were behind a cyber attack on the Electoral Commission, which exposed the personal data of 40 million voters, as well as 43 individuals including MPs and peers.

Efforts to step up pressure on China in response include looking at sanctions on individuals thought to be connected with the alleged activity, according to multiple reports.

Deputy Prime Minister Oliver Dowden is expected to update MPs on the situation later on Monday.

The Electoral Commission attack was identified in October 2022 but the hackers had first been able to access the commission's systems for more than a year, since August 2021.

The registers held at the time of the cyber attack include the name and address of anyone in the UK who was registered to vote between 2014 and 2022, as well as the names of those registered as overseas voters.

Nuclear minister Andrew Bowie said he could not comment on the speculation about China but told LBC Radio: "The fact is that this Government has invested a lot of time, money and effort in ensuring that our cyber security capabilities are at the place they need to be, we've increased the powers of our intelligence and security community to be able to deal with these threats.

"And we will stop at nothing to ensure that the British people, our democracy, our freedom of speech and our way of life is defended."

He insisted the Government took a pragmatic approach to dealing with Beijing, amid reports that China's EVE Energy is set to invest in a battery plant in the West Midlands.

"We have to have a grown-up, pragmatic relationship with China. And that means looking at each of these investments in the round, on a case-by-case basis, ensuring that our security and our individual liberties and freedoms are not undermined by any of the investments that are under way."

A small group of politicians who are hawkish on China are said to have been called to a briefing by Parliament's director of security, Alison Giles, in relation to the activity.

They include former Tory leader Sir Iain Duncan Smith, former minister Tim Loughton, crossbench peer Lord Alton and SNP MP Stewart McDonald, the Sunday Times reported.

The legislation includes measures to make it easier for agencies to examine and retain bulk datasets, such as publicly available online telephone records.

The four are members of the Inter-Parliamentary Alliance on China (IPAC) pressure group, which focuses on issues involving the increasingly assertive Asian power.

Meanwhile, reforms of UK spying laws are continue to make their way through Parliament, with the Investigatory Powers (Amendment) Bill also in the Commons on Monday.

BBC

Cambridge Water:
Customer details targeted in cyber attack

A water company customer has told how the theft of his details online had left him "feeling vulnerable".

Cambridge Water customers received letters this week after its parent firm, South Staffordshire PLC, was targeted by cyber-criminals in August.

Names, addresses and account details of direct debit customers were published on the dark web, the company said.

Richard Vaughan, from Foxton, Cambridgeshire, said he had "lost all trust" in his water supplier.

Cambridge Water apologised to customers and said "leading forensic experts" had discovered the data on the dark web, a part of the internet not accessible by conventional search engines.

The data breach was earlier revealed by Staffordshire Water.

South Staffordshire PLC, the parent company of South Staffs Water and Cambridge Water, said it had started informing customers involved after it was targeted on 16 August.

The company serves more than 1.7 million people, but it has not revealed how many of those are affected.

- BBC Technology: What is the Dark Web?
- Water customers' bank details may have been leaked

Mr Vaughan said: "I had no knowledge prior to that letter and it's left me feeling vulnerable.

"They've offered me a year's paid subscription to some analytical thing that tells me if my data has been sold on the dark web.

"Ultimately they're not doing anything to sort it out.

"I've lost all trust in Cambridge Water and if I had the opportunity, I'd switch supplier because they don't seem to care about their customers."

Sharon Bates, from St Ives, said her parents, aged 89 and 96, received the letter, which had caused "sleepless nights".

She said they had been advised by their bank to be vigilant to anyone calling them posing as the police or the bank in the light of the leak.

Richard Clayton, a security researcher at Cambridge University, who also received a letter from Cambridge Water, said the company could receive a substantial fine.

"People's data gets stolen all the time, but there's now a legal requirement on the company to tell customers when their data has been stolen," he said.

In a statement, Cambridge Water said: "Our investigation has now found that the incident resulted in unauthorised access to some of the personal data we hold for a subset of our customers.

"If customers do not receive a notification letter from us, then they do not need to take any action at this stage."

The National Crime Agency, the Information Commissioner's Office and water inspectorates had been notified, it added.

WANT TO KNOW MORE?

Times are changing, and so is the way we work too.
We are eager, to discuss how our 'Private Cloud' solution can support your organisation's goals.

Email lucy@breathetechnology or call us on 0122 320 9920 for a friendly informative conversation.

www.breathetechnology.com
(live chat available)

London	020 3519 0124
Cambridge	0122 320 9920
Sheffield	0114 349 8054
Suffolk	0144 059 2163

lucy@breathetechnology.com

breathetechnology

support | cloud | security | infrastructure | comms

EMPOWERING BUSINESS THROUGH SECURE TECHNOLOGY