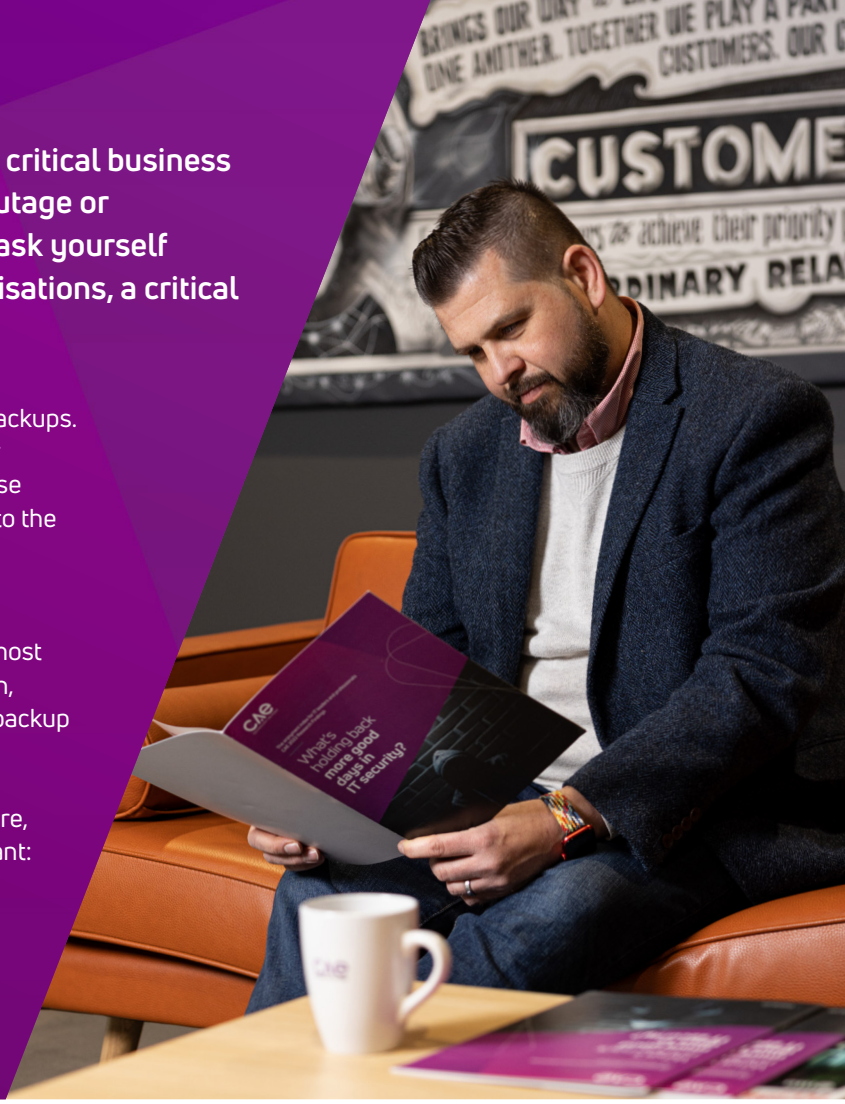
Beware the gap in your backups that many organisations fail to address

Are your backups sufficient to restore your critical business operations in the event of an unexpected outage or cyber-attack? It's a question you no doubt ask yourself regularly. So why is it that, for many organisations, a critical part of the answer is too often overlooked?



You probably hear a lot about the importance of data backups. In fact, the latest update to the UK Government's Cyber Essentials scheme included a reorientation to emphasise the importance of a good backup strategy in response to the growing threat of ransomware.

National Cyber Security Centre (NCSC) guidance recommends that you "make regular backups of your most important files, it will be different for every organisation, check that you know how to restore the files from the backup and regularly test that it is working as expected."

Yet, when considering what their most important files are, many organisations overlook some of the most important: their cloud networking operational data.

Why is it essential to backup cloud networking operational data?

You might have the best backups and incident response processes in place but, if you aren't backing up your cloud networking operational data, you could have big problems in the event of an outage or cyber-attack.

Imagine: a cyber-attack has brought your systems down. Your IT team has worked tirelessly to restore your applications and user data and get systems back online. But no one can access any of it – not until you restore your network.

Sounds far-fetched? It can happen to even the largest organisations in some of the most highly regulated industries. In April 2018, the TSB bank updated its IT systems and migrated its corporate and customer services onto a new IT platform. While the data migrated successfully, the platform immediately experienced technical failures. More than five million customers were affected. As well as the reputational and regulatory damage, TSB paid £32.7 million in redress to customers. It took until December 2018 for the bank to return to business as usual.

Without the ability to quickly restore the platform, the bank's recovery point objectives (RPO) and recovery time objectives (RTO) were sunk.

Why cyber security matters to every retailer

Cyber security matters to every retailer because of both the significant damage to your reputation and the high cost to your profit margins. According to Symantec, large retailers suffering data breaches can expect to find themselves facing charges in the double – and triple-digit millions. The average cost of cybercrime attacks per organisation in the United States is estimated at $12.69M. These expenses include detection, escalation, notification, and after-the-fact responses such as legal, consulting, card replacement and credit monitoring fees. Slow reaction and delays in notification, however, can drive expenses even higher. Add to that the loss of future revenue as customers turn away from brands they can't trust with their data, and you'll see why cyber security is a critical investment. An expert cyber security partner can help you to identify your potential risk levels and build a case for creating a comprehensive strategy. Then they can help you execute that strategy.

Why do you need cloud networking backups?

There are many different reasons why you might need to rapidly restore an earlier configuration of your cloud networking platform or some of its devices, such as Firewalls, Switches or even CCTV.

These include:

- Accidental data deletion through the platform UI or API
- Accidental error by the cloud networking service provider
- Cyber-attack by unauthorised access
- Poor leavers policy with multiple providers having platform access
- Deliberate data deletion

In all of these situations, it's important that you have a backup of your cloud networking devices because their configuration can be difficult and time-consuming to manually rebuild due to a lack of expertise or up-to-date documentation.

To demonstrate this need, try answering the following questions:

- How long would it take the business to recover today from a platform-wide deletion of all networks?
- What would be the impact and cost of a service outage to the business?
- What is your business risk of doing nothing?

Imagine trying to answer these questions (and more) for every network device across your estate. Then doing the hard work of configuring each of them appropriately, in a high-pressure situation. When your ability to serve your customers has been compromised, every minute that you delay is costing the business money.

It's clear that a backup solution is required.

What is best practice when it comes to cloud networking backups?

When it comes to cloud networking backups, you need to have a reliable backup of your most recent correctly working configuration to restore from. By default, there is no backup capability or first-line defence natively available on the cloud networking platform, to provide this protection or restore point.

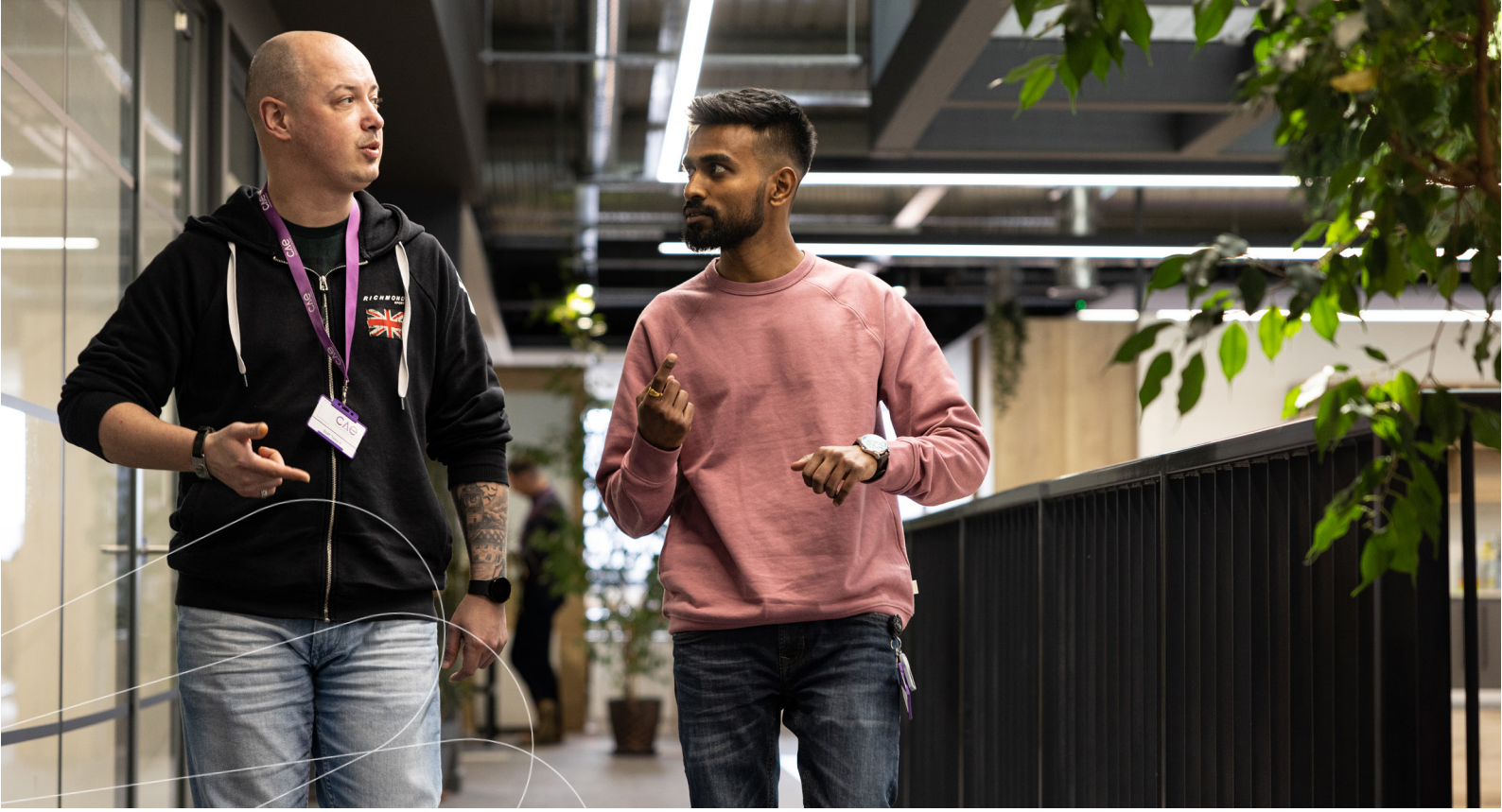
Based on common standards, it is often the responsibility of the business consuming the cloud service to take regular data backups. Ensuring there is an up-to-date restore point available for a business to use. This way, the latest, most stable configuration will be available if for any reason you need to restore parts or the whole cloud networking environment.

Backup and restore for Cisco Networking Cloud (CNC)

Your Cisco Meraki cloud networking solution is no different to any other backups you maintain for your other cloud services. The best news? We have the right solution that enables you to manage these backups: Assure powered by CAE Labs.

Our Assure solution is a managed service which delivers backup and restore capabilities for your Cisco Meraki cloud networking platform. We manage all the disaster recovery and business continuity activities on your behalf, so you have complete peace of mind. This way, your business is protected in the event of a major failure – or a malicious attack.

Instead of taking weeks to configure each device and network from scratch, we can get you back up and running in no time, and restore your latest configuration from your backup, reducing your recovery time from days, weeks or even months to a matter of minutes.



Assure delivers

- Increased uptime and reduced business restoration downtime - from days and weeks to hours and minutes
- Eliminating operational disruption, financial losses, and reputational damages
- The secure capture of all operational changes - backup when they happen, in real time
- Bi-annual business resilience sandbox testing, so you can establish a restoration process with your IT team
- The mitigation of future outages; prevent them from ever occurring through ongoing service intelligence and additional risk removal
- 24/7 access to UK-based expert support as and when needed

With Assure from CAE Labs, you are assured of the best possible recovery time in any data loss scenario. For example, a leading UK retailer rebuild would have taken around 90 minutes to restore per location. With them now on Assure, this can be achieved in under one minute per location, resulting in the best recovery time for their business and significantly reducing disruption.

By minimising service restoration downtime, if the worst happens you can minimise potential losses to your business – whether in customer retention, revenue, share value, compliance, or reputation.

ASSURE

What now?

Protect your business continuity and give yourself complete peace of mind. Find out more about Assure from CAE Labs by booking a demo with our team today.

thisiscae.com

TECHNOLOGY ON POINT