How to get the Right Backup Provision for your Organisation

Backup is a key part of an IT Disaster Recovery Plan. As remote working and the use of public cloud services, like Office365 and GSuite, is increasing rapidly, you need to think carefully to ensure you have the right backup processes. Here is a six-step process to help you make the right choice.

01 **List, locate and prioritise your applications**

Itemise all the applications your organisation uses, from email and file storage to your accounts package and graphic design tools. You need to be able to use them all going forward, but which are the most important to the successful functioning of your business? Restoring applications and data for the most important must take priority.
How is each delivered to your team? Cloud applications do not need to be backed up, as that is done by the provider. You just need to backup the data. Local applications do need a backup, along with the data.

02 **Determine your most critical data and where it is stored**

What data is essential to your organisation and how long can you survive without the data? Rank the data and set a recovery time objective:

- High Priority – your business cannot function without it. You need it back in seconds/minutes/hours.
- Medium Priority – you need it, but not right now. You need it back today.
- Low Priority – you want it, but you can easily re-create or even live without it. As long as you have it this week, that is okay.

Where is this data stored and how can you get to it, and how quickly, in a disaster recovery situation?

03 **How do you handle remote working?**

How does remotely created data get backed up and what are the implications of the process?
If they are running, for example, Office365, this data will need backup. If users automatically synchronise their remote data with network servers, these files should be scanned for malware during backup, as you now have an extended perimeter, and increased vulnerabilities to phishing and other cyber threats.

04 **Who is backing up what data?**

Contrary to popular belief, many of the popular public cloud providers, including Microsoft with Office365, Google with GSuite, Salesforce and Xero, do not backup your users' data. Many Private Cloud providers offer data backup, but typically keep the data in the same network as the application servers, creating a single point of failure. If they aren't doing a backup, with a Service Level Agreement (SLA), you need to. Look for those services that have independent certification, NIST FIPS is a good example.

05 **What threats are you protecting against?**

When thinking about backup, consider what threats are you planning for; a fire, a flood or power outage? These are all threats with natural origins and storing your data in two separate places will protect against these. If you are more concerned with data deletion, programming errors or ransomware these are threats of human origin, and each needs its own approach to minimise the threat

06 **Remember the 3,2,1 of backup good practice**

There should always be at least three copies of your data, two in backup. One of the backup copies must be offsite. Be aware, however, that this will NOT protect against the latest forms of evolved ransomware.

PDS POLICE DIGITAL SECURITY CENTRE

DATA2VAULT SECURE DATA SERVICES

DATA2VAULT
SECURE DATA SERVICES

It will happen! How to plan for the **"When, Not If"** of a Cyber Attack

Ransomware attacks are the largest single cause of recovery request to service providers. It can, and will happen to you; are you prepared? In the first month of the COVID-19 pandemic, phishing attacks went up over 600%. Many contained Ransomware payloads and this problem is not going away.

What is Ransomware?

Ransomware is malicious code (malware) inserted into your device, that spreads across your network, infects files with data encrypting code, before exporting the encryption key back to the original sender. A ransom note is presented on the users screens demanding a ransom is paid in Bitcoin. Paying the ransom does not guarantee you get the data decrypted, or that remnants of malicious code still remain on your network. 90% of infections are from users clicking a link in a phishing email.

I have a backup; can't I just restore my data?

Back in the early days of ransomware, this was exactly the way to get your systems back up and running. In 2017, ransomware, like SAMAS started to appear. The code was able to discover and delete popular backup files, before encrypting the data. Hackers had worked out if the recovery process can be disrupted, then it was more likely the ransom will be paid. Ransomware is evolving with SAMSAM, Zenis and Cryptowall continuing to identify and delete, or prevent backup files being recovered, creating Attack Loops of reinfection.

Why won't my restore work and what is an Attack Loop?

Since 2017, ransomware has evolved and now infects your network, but doesn't tell you by detonating (presenting you with the ransom demand). It sits quietly whilst your backup includes all the infected files. When you do try to restore from your backup, you are restoring infected files. All you can do is try older backup data, but with cyber breaches not being identified for an average of 191 days, all your backups may be infected. Restore, infect, restore, infect – that is an **Attack Loop**.

How do I protect my backups from evolved ransomware and Attack Loops?

Add **protection** for your essential files through backup, with integrated scanning of both backed up and recovered files, obscure the backup file names and provision multi-factor authentication for backup administration.

Finally...

Monitor & Test, test, test

Your daily backup will be successful, partially successful or a failure. You must know what happened and take any necessary action EVERY DAY if you want to be confident you have all the data you need.
The best way to ensure you are safe, is to test the recovery process. If you aren't regularly testing, you have no idea of whether it will work in a real disaster situation.

PDS
POLICE DIGITAL SECURITY CENTRE

For more information
website: www.data2vault.com
enquiries: 0333 344 2380
email: info@data2vault.com