Protect your Data
Protect your Business
Backup & DR meets Cyber Recovery

DATA2VAULT
SECURE DATA SERVICES

On the **Risk and Threat Index** prediction for the next 12 months the NUMBER ONE THREAT is **Cyber-attack & data breach***

How certain are you that when **cyber disaster strikes,** your business can be recovered and start working quickly again?

The key factor in any successful IT business interruption response is recovery of data and fast return to work.

This is more complex than ever now that Cyber threats are sweeping the globe. If your data isn't recovered or recoverable, your ability to work will be severely disrupted and the business could fail. Recovery from Cyberattack, specifically Ransomware, should be included in all IT DR and Business Continuity planning. Using air gaps and storing recovery data offsite is no longer fit for purpose as disaster recovery processes that rely solely on air gaps have become obsolete due to evolved Ransomware.

By understanding what evolved Ransomware is and how to combat it, you can plan for a successful IT recovery from a Cyberattack.

What is evolved Ransomware?

Since 2017 Ransomware has been evolving by disrupting recovery processes, which results in more Ransomware attacks getting paid out. Malware is rapidly developing to locate, identify and delete backup files on a network before encrypting the user data. Vendors responded by recommending air gaps.

During 2019 and beyond Ransomware continued to evolve. Malware is now being embedded as hidden code in Windows files, and more recently Microsoft365 files, traversing networks and infecting more user data. The hidden code may sit dormant for up to six months, during which time backups are being infected, both those stored locally and those offsite that are air gapped. When the Ransomware eventually detonates, user data is encrypted. Restoring infected backups recovers encrypted data and puts it back onto the network, creating Attack Loops. This is evolved Ransomware.

If you have had a breach and are concerned evolved Ransomware is in your network or MS365 files, Call Us, we can backup and scan your data, to quarantine files with hidden malware before it detonates

"How could you let this happen to us?"

This is not a question that any IT Manager or Director of an IT MSP ever wants to face, but you will if the DR services you run today can't recover successfully from a Ransomware attack.

You test your fire alarm.
Have you ever tested that your backup not only works but you can recover quickly from Ransomware?

* https://www.beazley.com/documents/2020/Beazley-Breach-Briefing-2020.html

How long could your business survive without its data?

Data2Vault will audit your business and provide you with a report detailing your Business Impact Analysis. **What does the report give you?**

1. **It evaluates your current** state in terms of preparedness for a disaster, highlighting vulnerabilities and what you need to do next.
2. **It increases your resilience** and prioritises spend in an ever-complex world, which now includes the added security vulnerabilities of more staff working from home.
3. **It provides insight** - what are your risks? - and what you need to do now and in the future.
4. **It will identify any additional layers of protection that are acutely needed.**

As organisations migrate to cloud platforms, your DR services must adapt to support the business. Flexible DR plans protect the investment made in those services, because the data continues to be protected, even if it now runs in public cloud services. Too often, organisations get locked in with hardware based DR solutions that stifle agility.

Does your DR service need to protect on-premises workloads, as well as cloud workloads and data in public cloud services like Microsoft365? Bear in mind that public cloud services do not backup your data. Your DR plan must be adapted to address the timely recovery of data from many sources, free from infection and Ransomware.

Data2Vault's DR services are integrated and flexible, and work together to provide a wide range of Recovery Time and Recovery Point Objectives. They also contain the ultimate last line of defence, protection and recovery from evolved Ransomware.

Ransomware attacks are increasing, with IT service providers or vendors being targeted and compromised by hackers.

Recovery from Ransomware must be included in your DR plan and not overlooked.

Each one of our DR services has a different price point dependent upon budget and operational need.

Let's look at each of them individually as DR scenarios cannot always be resolved by using just one DR option.

Your DR Options Data2Vault Disaster Recovery & Advanced Backup services

DR service	
Cloud Replication	Offering RTOs and RPOs in minutes to hours, across VMWare workloads to offsite infrastructure.
Instant Recovery Appliance (local)	Offering RTOs and RPOs in minutes to hours, for rapid local recovery across physical and virtual VMWare, Windows, SQL, SharePoint, Exchange and Container environments. Supports fast mount shares and also sends data to the offsite cloud infrastructure.
Cloud rVDR	Protects VMWare workloads, uses VADP snapshots to automatically create VMDK files daily
Advanced Backup Service	
Continuous Data Protection (CDP)	Uses backup to provide more Recovery Points for VM-Ware, Linux, SSH, NFS v3, Windows files, Windows VSS, MS SQL, SharePoint and Exchange.
Cloud Backup with Attack Loop Ransomware Protection	Protects Windows network stored file data from evolved Ransomware. Ideal for supporting clean data during DR for Office365 public cloud services. Often provides the only clean copy of user data post-Cyberattack.

All Data2Vault DR services are delivered from UK data centres that are ISO 9001, ISO27001 and ISO14001 accredited.

All DR services include the following:

- ✔ An IT Disaster Recovery Plan aligned to your Business Impact Analysis
- ✔ Annual testing
- ✔ Change control to the services
- ✔ Remote access as required

POWERED BY Asigra.

MALWARE-IN-YOUR-BACKUP Attack-Loop™ Prevention.

Why do we offer a range DR options?

Adopting a one-size-fits-all DR service always means more money is being spent than is necessary. Grading applications and data into Essential / Important / Non-Essential categories against their criticality to business operations, and then matching them to the appropriate DR service, will result in less money being spent but the right support in place.

Changing Threat Patterns

Throughout 2020, the Business Continuity Institute has consistently seen Cyberattacks identified as the highest impact to business and the highest frequency threat to Organisational Resilience. The 2019-20 Beazley breach insights report[1] from leading Cyber Insurance underwriter, Beazley Group, has seen»»

Service Providers that adopt Remote, Monitoring & Management (RMM) applications are being targeted by hacking groups like APT10[2]. Any vulnerabilities within the RMM setup are exploited and attacks are then launched against all the Service Providers' customers. Providers that adopt backup services that are integrated with their RMM are at greater risk as their client's backup data is also being compromised during an attack.

Separate your backup services and files from all RMM solutions before it is too late.

131%

Ransomware claims increase

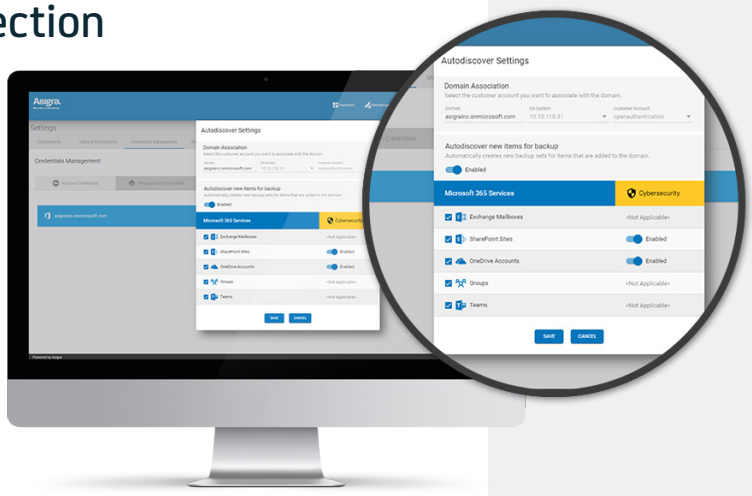
24%

of the claims were tracked back to the compromise of a Service Provider or vendor that is connected to the customers network.[1]

Additional Layer of Protection

Many businesses have already invested in DR solutions, often in the form of replication or Instant Recovery appliances. As Cyber threats have adapted over recent years, so must the contingency planning and services to combat these threats.

Our agentless service architecture minimises the amount of software that needs to be installed to perform backup, recovery and DR operations by up to 90% when compared to using backup agents. Less software to go wrong and less software to attack.



This allows our Attack Loop data protection for evolved Ransomware to be added to any network alongside an existing agent-based solution, without any disruption.

DR Orchestration

Reducing human involvement in the DR process will help improve recovery outcomes, as automation creates consistency. It is often unavoidable to eliminate human intervention completely, but with our DR services it is kept to a minimum.

Three Service Delivery Support Options are available; self-service, assisted and fully managed across the DR and Advanced Backup Services.

Talk to Data2Vault about your DR Project, **Call us on**

0333 344 2380

[1] https://www.beazley.com/documents/2020/Beazley-Breach-Briefing-2020.html
[2] https://www.ncsc.gov.uk/report/incident-trends-report. Supply chain and relationships

Recovery from a disaster that impacts business operations starts with good planning.

In simple terms, work from these five points and you can start tomorrow.

1

Understand where all your applications and data are running to complete a Business Impact Analysis. Better still, let us do it for you and gain a sanity check. Determine the IT services and data that are essential, and the disaster scenarios you are planning to recover from. Don't forget recovery from Ransomware attack.

2

Define the realistic Recovery Time and Recovery Point Objective for each application and its data.

3

Review the market for appropriate DR services. Flexibility to support business agility is key in these uncertain times.

4

Adopt proven, referenced services from reputable service providers and technology vendors delivered with an intgrated IT DR plan.

5

Test, test, test and review.

The formidable team at Data2Vault have been supporting businesses with Disaster Recovery Services since 2007. During this period, the platforms and systems in use and the threats posed have changed dramatically, with the adoption of public cloud services, DevOps, hosted IT, and the emergence of highly disruptive Cyberattacks. One thing remains as a constant: the need to deliver the highest possible recoverability of systems and data, because without the data there is no business.

Talk to Data2Vault about your DR Project,
Call us on 0333 344 2380

Protect the Data
Protect the Business.....and sleep tight

DATA2VAULT
SECURE DATA SERVICES

info@data2vault.com | www.data2vault.com