POWERED BY Zerto

Disaster Recovery:

Is your business safe from the threat of data loss?

Data recovery and business continuity are now inextricably linked – and completely essential to the modern data-driven business. There are a number of factors that can result in data loss, and IT teams will need to develop disaster recovery plans capable of coping with them all.

Throughout the COVID-19 pandemic, the drive to maintain customer engagement and ensure services are always on to support enquiries has led to the spotlight shining on organisations' disaster recovery strategies. What's more, with the rise of the distributed workforce/hybrid working and omnichannel communication, it's important to consider whether the right tools in place to ensure business continuity, especially where compliance and data security are concerned.

Introduction

With hybrid working and omnichannel communication now part of many organisations' day-to-day operations, the workforce has evolved considerably throughout the previous few years. But as a result, the threat landscape and business continuity challenges faced by organisations have also evolved and must be carefully considered. With more employees connecting to corporate networks from home than ever before, there are an increasing number of opportunities for cyber criminals to create serious data breaches. This must be considered as part of the wider disaster recovery plan, to ensure that, should another move to remote working (or any other large-scale shift in the way we work) be required in the future, organisations can execute the shift with minimal disruption and zero data loss.

Businesses are apparently aware of the challenges involved here, with 69% saying that cyber security is a high priority. Yet almost unbelievably, 75% of small businesses claim they do not have a disaster recovery strategy in place, and 33% of those that do are not able to periodically test its effectiveness, due to a lack of internal knowledge or resources (highlighting the value of robust partnerships in creating an effective DR strategy).

As a result, 50% of businesses that experience a serious disaster event will not recover, while the cost of IT downtime for businesses averages around $5,600 per minute.

There also remains a disparity between understanding the need for business continuity and actually deploying effective measures. 89% of managers recognise business continuity as a key responsibility, but just 63% have suitable plans and provisions in place.

These kinds of discrepancies place businesses in serious danger of falling victim to a data loss event. Clearly it is time for businesses to begin applying themselves to increasing resilience and availability, or risk losing market share to better-prepared competitors. And where the CTO cannot de-risk completely, recovery plans need to restore operational functionality as quickly as possible.

Contents

A very real & present danger

British businesses and their IT systems are under constant threat from a range of sources. None of these risks are particularly mysterious, or even unknown, but most disaster recovery plans are geared towards coping with just one.

Cybercrime

Throughout 2020, ransomware attacks soared by 150%[1] as cyber criminals rushed to exploit the rapid move to remote working, with the average ransom standing at $170,000, but reaching as high as $2 million. At the start of 2021, such attacks caused an average of 16.2 days of downtime – a considerable financial loss when we consider the previously mentioned cost per minute of downtime[2], and a considerable blow to the victims' reputations and customer satisfaction, at a time when maintaining customer engagement and confidence is of vital importance. An effective DR strategy is the key to minimising the downtime caused by these attacks, while avoiding any potential data loss.

Employee activities

Although hackers grab the headlines, the largest threat to corporate data actually comes from inside the network. Whether deliberate or otherwise, employees present a significant risk to internal resources according to 78% of IT security professionals. These concerns appear to be valid too - human error accounts for 29% of all data loss.

Incidents of employee-related data destruction are common. One disgruntled employee deleted seven years' worth of drawings and blueprints worth $2.5 million from her architectural employer's systems for instance. The firm in question did not have an adequate data backup regime in place and was instead forced to recover the lost data using a third party service capable of retrieving information at the disk level.

Adopting a proactive approach to business continuity, to drive future success

With so many moving parts in the modern corporate network, data loss events are inevitable. 140,000 hard drives fail every week for instance, and 96% of business workstations are not regularly backed up (if at all).

- **95%** of organisations have had to rethink data protection due to the sudden emergence of work from home (WFH).
- New workloads, including containerised applications and SaaS, are driving data protection modernisation.
- Malware and ransomware attacks are so pervasive that organizations must provide protection from them and ensure recovery.
- **43%** of organisations suffered unrecoverable data within the past 12 months.
- **63%** of organisations have suffered a data-related business disruption within the past 12 months.

The State of Data Protection and Disaster Recovery Readiness: 2021 (sponsored by Zerto), Phil Goodwin

The actual cause may differ, but eventually every business faces a situation where data loss will occur if a robust disaster recovery programme is not in place.

Calculating the cost of data loss

The actual cost of data loss varies widely depending on several factors:

- The cause of the loss.
- The kind of data lost.
- How much data was lost.

Disaster recovery specialist Zerto reported the total cost of annual downtime as $700B[3] , and advocated greater visibility of the potential cost of downtime, particularly via their online downtime calculator. The goal here is to optimise both the Recovery Time Objective (RTO) - the length of time a business can be without a specific service without incurring cost or risk - and the Recovery Point Objective (RPO) - the most recent point from which data can be recovered, which can range from 15 minutes to 24 hours, depending on the solution utilised.

The specifics of the incident will have a knock-on effect on operations, adding compound costs associated with the loss. However, secondary costs such as fines of up to £500,000 from the Information Commissioner's Office, or damage to brand reputation will take the total higher still.

> "Depending upon the type of breach, the value of brand and reputation could decline as much as 17 percent to 31 percent of annual gross revenues."
>
> Ponemon Research.

As well as a drop in current revenue, future income will also be affected. 58% of consumers say they would actively avoid a provider that has recently experienced a data or security breach. The ability to recover data quickly and efficiently will go some way to restoring trust after a data loss incident.

In the event that your business is affected by a data loss incident, the ability to restore normal operations as quickly as possible will be essential to rebuilding customer trust - and reducing the associated long term costs.

Meeting the challenges of the future

Historically data protection regimes have been designed to protect against natural disasters or terrorist attacks that would affect core business operations at head office. The need to operate 24 / 7 x 365 however, requires more than a simple off-site duplicate of corporate data. Instead, organisations need to develop a business continuity plan that allows them to get up and running again as quickly as possible.

Malware and security attacks are becoming more sophisticated, and malicious employees remain a serious danger. Closing the entire network infrastructure for days at a time to deal with security issues is not only unacceptable,

but also prohibitively expensive.

How can Exponential-e protect your business & data?

With data loss increasingly becoming such a concern across all businesses and sectors, it is clear that companies need to look for a solution that will provide them with the security and privacy that they require to protect their data and infrastructure.

The solutions that Exponential-e offer are built on the foundation of security, privacy and reliability. This is imperative to ensure that your infrastructure, applications and services are all protected from the dangers previously discussed.

But just what solutions should a business look to implement to ensure that their data, application and infrastructure are managed and left in the very best hands?

Disaster Recovery & Business Continuity

Ensuring that if the worst happens you can repair and restore your data is vital. Therefore implementing a Disaster Recovery and Business Continuity solution should form the very basis of your IT plan.

Knowing that you have this in place to action should disaster strike will not only provide your business with the comfort blanket it needs, but also mean that employees aren't hindered and productivity isn't hugely impacted should you face an episode of data loss.

In partnership with industry leaders such as Zerto, Exponential-e is able to provide you with a Disaster Recovery solution that will enable your business to continue working, whether remotely or in a temporary location should you be required to.

Private Cloud

"Your Cloud is only as good as your Network" is our strapline and it is true; without the support of a reliable and secure Network your Cloud solution will underperform.

Our Private Cloud is designed with full operational resilience in mind, utilising DRaaS capabilities, and leveraging the support of our UK-based 24 / 7 x 365 customer service desk, so you can rest assured that your IT estate is in secure hands.

Ensuring security and privacy of your data and applications, our Cloud is built on the safe side of your firewall, providing complete visibility and access control. Should disaster strike you can rest assured that your data and applications are safely protected, and can be restored, where necessary, as quickly as possible to ensure that your business can get back up and running.

Enabling our Cloud solution within your business also means that your employees have the ability to work remotely, therefore if they are unable to access the office they will still be able to remain productive and access the tools that they require.

Secure Data Centre Facilities

With three UK-based Data Centres in Hayes, Enfield, and Farnborough, we are able to offer a range of services that can ensure the security and availability of your data should it be required in a disaster scenario.

From replication across multiple sites to moving from an in-house DC to a colocation solution, we can ensure that your data meets data sovereignty regulations and that is kept in the securest location.

Our Managed Data Centres offer best-in-class technology, allowing us to deliver the security, performance and flexibility that is expected. An essential requirement when sourcing options for your Disaster Recovery plan.

Delivering Peace of Mind as-a-Service

Exponential-e is a longstanding partner of Zerto – an industry leader in business continuity and disaster recovery solutions. The combination of our extensive cross-vertical experience and enterprise-class network with software-defined automation and replication ensures data is securely backed up and available for up to seven days, with extended journaling. With this in place, your critical data can always be restored with a single click, should you ever need to initiate a disaster recovery scenario. This way, your internal IT teams are free to focus on business growth activities, safe in the knowledge that any data loss will always be kept to the absolute minimum.

1. https://www.infosecurity-magazine.com/news/ransomware-attacks-soared-150-in/
2. https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate
3. https://www.zerto.com/page/the-real-cost-of-it-outages-and-disruptions/

exponential-e
APPLIED INNOVATION

www.**exponential-e**.com

Telephone
+44 (0) 845 470 4001

Visit the website
www.exponential-e.com

bsi. ISO 9001 Quality Management | ISO 27001 Information Security Management | ISO/IEC 20000-1 Information Technology Service Management | CSA STAR Cloud Security | ISO 22301 Business Continuity Management | ISO 50001 Energy Management | ISO 14001 Environmental Management | BS 10012 Data Protection | ISO 27017 Security Controls for Cloud Services

REF:2046