CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

Defeating Business Disruption in a Post-COVID-19 Era

Will Urban

Will Urban
Senior Technical
Marketing Manager
iland

Biography

Will Urban is the Senior Marketing Technologist at iland Cloud (https://www.iland.com).

land is a global cloud service provider of secure and compliant hosting for infrastructure (IaaS), disaster recovery (DRaaS), and backup as a service (BaaS). It is recognized by industry analysts as a leader in disaster recovery. The award-winning iland Secure Cloud Console natively combines deep layered security, predictive analytics, and compliance to deliver unmatched visibility and ease of management for all of iland's cloud services. Headquartered in Houston, Texas and London, UK, iland delivers cloud services from its data centres throughout North America, Europe, Australia, and Asia. Learn more at www.iland.com

Keywords Cloud, COVID-19, Disaster Recovery as a Service (DRaaS), Data backup, Business continuity, Cloud migration
Paper type Opinion

Abstract

Nearly every organization is dependent on some form of technology and connectivity, and in a time of crisis, the term 'IT resilience' is directly intertwined with the resilience of the business. Risks to business continuity impacts on productivity, prosperity, financial stability and reputation. In this article, the author discusses the strength of an organization's cloud or on-premises infrastructure as being the backbone of the organization – and if it fails or suffers an outage, many businesses will suffer significant business disruption.

Introduction

The prospect of an IT outage is one of the key issues that keeps IT professionals awake at night. From natural disasters to malicious cyber-attacks, organizations face an abundance of risks to business continuity that impact productivity, prosperity, financial stability and reputation. These worries have only been exacerbated in recent months as the COVID-19 pandemic continues to have an unprecedented impact on worldwide economies, trade and the survival of individual businesses.

Therefore, it has never been more important for these organizations to take the necessary steps to protect their business from any of the above scenarios, which have become increasingly prevalent. Despite these constant threats, customers want assurances that their day-to-day operations will not be impacted, should a partner business suffer a loss of data or significant business disruption.

IT resilience powering business continuity

With nearly every organization on earth dependent on some form of technology and connectivity, the term 'IT resilience' is directly intertwined with the resilience of the business, in a time of crisis. The strength of an organization's cloud or on-premises infrastructure is the backbone of the organization; therefore, if it fails or suffers an outage, many subsequent businesses could suffer significant business disruption.

Organizations develop business resilience plans so they can rapidly adapt when disruptions occur, helping them to maintain business operations, in addition to keeping data, staff and the company's reputation safe. This should be teamed with IT resilience, to continue business system operation no matter the disruption.

Many organizations will instantly think of maintaining backups when they hear of business continuity – and to some degree they are correct. However, that is only part of the problem; Disaster Recovery (DR) and Disaster Recovery-as-a-Service (DRaaS) has been increasingly adopted to protect businesses against outages, through an infrastructure and strategy that deals with worst-case scenarios.

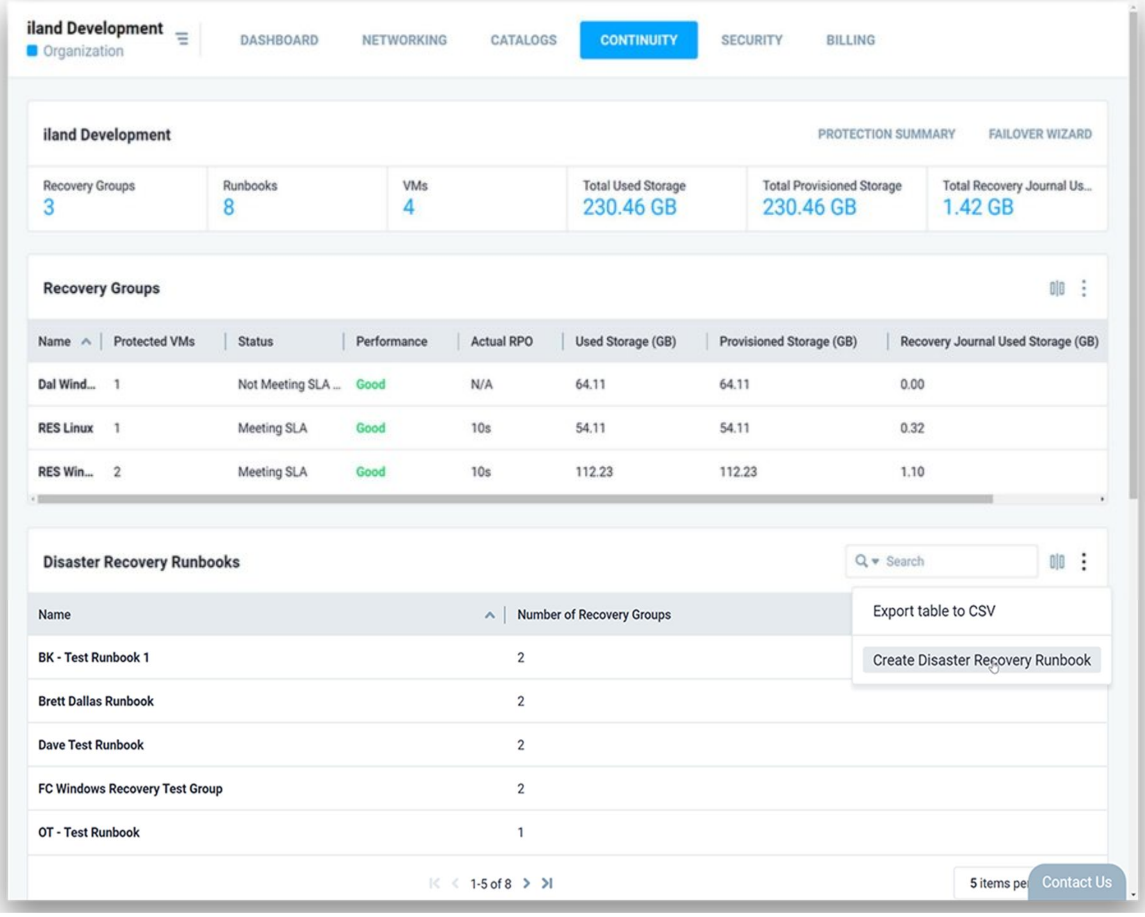
Whilst many organizations align the term 'Disaster Recovery' with a natural disaster or potential meteorite strike that threatens human life, a software fault, malicious external hack, subsequent data breach, or a careless accident initiated by an insider can be equally disastrous from a business disruption perspective.

CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

Moving from backups to Disaster Recovery

Business resiliency is all about the ability to bring your organization online to another location as quickly as possible to continue to run your business and support your customers internally and externally. Whilst backups are key to protecting data, maintaining archives and compliance, they must be layered with a DR capability to reduce the chances of a business being disrupted.



iland Development

Recovery Groups	Runbooks	VMs	Total Used Storage	Total Provisioned Storage	Total Recovery Journal Us...
3	8	4	230.46 GB	230.46 GB	1.42 GB

Recovery Groups

Name	Protected VMs	Status	Performance	Actual RPO	Used Storage (GB)	Provisioned Storage (GB)	Recovery Journal Used Storage (GB)
Dal Wind...	1	Not Meeting SLA ...	Good	N/A	64.11	64.11	0.00
RES Linux	1	Meeting SLA	Good	10s	54.11	54.11	0.32
RES Win...	2	Meeting SLA	Good	10s	112.23	112.23	1.10

Disaster Recovery Runbooks

Name	Number of Recovery Groups
BK - Test Runbook 1	2
Brett Dallas Runbook	2
Dave Test Runbook	2
FC Windows Recovery Test Group	2
OT - Test Runbook	1

The disadvantage of backups, especially when organizations try to recover quickly, is that they are prone to unacceptable Recovery Point Objectives (RPO). If a business is only backing up every night and something happens an hour before the backup, an entire day of workloads will be lost. In addition, backups can have painful Recovery Time Objectives (RTO). If it takes 17 hours to recover an organization's entire data centre from tapes, in addition to how long it has been down for – that is a considerable amount of time.

Furthermore, local backups can be targeted by malicious software, which target backup applications and database backup files, proactively searching for them and fully encrypting the data. Backups also need something to restore to; if the power fails in the building where the business' data is housed, backups are not going to help.

This is where a cloud based DRaaS solution fills the gaps. It is a flexible, cost-effective way to deliver essential DR capability without all the CAPEX costs and pains of managing a physical DR site. At the press of the button, a business can instantly switch to its DRaaS environment, with an isolated, production-ready copy of its entire infrastructure available in the event of unplanned downtime or data loss. Furthermore, with regulations such as GDPR and CCPA increasing in popularity and becoming more stringent, DRaaS helps organizations to illustrate that they have taken all necessary steps to protect their customers' data, giving them confidence that should the worst-case-scenario happen, their data – and business – will be protected.

With DRaaS, teams can run recovery tests in replica environments in a short time, providing full visibility into a business' response during a 'disaster'. This is much more effective than annual testing of on-premises systems, helping businesses develop a full disaster recovery plan with absolute confidence it will work when needed, minimizing potential downtime. Quickly enacting these DR plans will only increase this confidence. In the midst of an outage, a quick and coordinated response will actually increase customer faith in the organization that it can instantly switch to a cloud-based data centre if any of the primary equipment fails.

Downtime will be increasingly disruptive

In the world we currently occupy, many businesses are facing an unprecedented financial crisis due to the COVID-19 pandemic that is driving them out of business. For example, in retail, many have shifted to, or quickly started to offer improved eCommerce channels, allowing them to deliver their services or goods to customers. Regardless, this has led to shrinking revenues and severe tightening of budgets.

Therefore, the last thing a business needs is any unscheduled periods of downtime due to IT systems going offline. This goes hand-in-hand with the online attack surface widening in many industries, as cyber criminals take advantage of the current global climate, ramping up their efforts to cause further disruption and distress.

In conclusion

DR is increasingly critical. Customer experience rests upon IT systems; interruptions of service, inability to transact, and data loss can be frustrating, debilitating, or even life-threatening in certain industries. Organizations should also think about the costs of downtime and the perception of customers should a vital application be down, especially during a time when a global pandemic is having a knock-on effect throughout the supply chain.

Acceptable amounts of downtime and data loss are at an all-time low, and recovery features that were once considered ‘nice to have’ are now mandatory. With the emphasis of IT resilience on maintaining business processes and making a complete recovery as soon as possible, it is no wonder that DR is becoming increasingly mission-critical to day-to-day operations. Taking the necessary steps to overcome business disruption when faced with a potential ‘disaster’ will easily outweigh the initial financial outlay of implementing an effective DRaaS solution.