IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

It’s Not Always Malware

Johnny Carpenter

Johnny Carpenter
General Manager EMEA
11:11 Systems

Biography

Johnny Carpenter, General Manager of EMEA at 11:11 Systems (https://www.1111systems.com) has worked in IT, addressing network and cloud challenges, for nearly three decades. With a history of consistently delivering sound commercial judgement, Johnny has a reputation for acute market insight.

Joining iland (now 11:11 Systems) over a decade ago, Johnny’s close relationships with other technical experts and customers across a wide range of industries have shaped his deep understanding of the trends, nuances and concerns around digital transformation strategies.

Johnny blogs at https://1111systems.com/blog/

Keywords Cloud, Disaster Recovery, Malware, Disaster Recovery strategy, Public Cloud, Private Cloud, Risk assessment, Cloud data centres
Paper type Research

Abstract

The threats to data are increasing, yet it is not always about malware attacks. Sometimes it can be down to disruption with physical assets, as was the case when earlier this year, one of the hyperscalers suffered a major data centre incident in which a water leak triggered a fire in a co-location data centre knocking more than 90 services offline in France. As the author of this article explains, the hyperscaler’s experience is a timely reminder that disaster recovery plans need to cover physical assets as well.

Introduction

Every day, cyber incidents and their subsequent downtimes seem to fill the news. These downtimes, both costly and damaging to consumer trust, have rightfully been something that CISOs and CIOs work to prevent with increasingly sophisticated security measures. But sometimes the most damaging “disasters” are the simplest.

Earlier this year, one of the hyperscalers suffered a major data centre incident in which a water leak triggered a fire in a co-location data centre, knocking more than 90 services offline in France. This serves as a reminder to us all that, despite rising cybercrime stealing the headlines, preparing for physical disasters remains a vital part of any disaster recovery (DR) plan. It is crucial that businesses consider the impact that these incidents may create on their own day-to-day operations and invest in their own disaster recovery.

Heatwaves[1], flooding and hurricanes are facts of life for many people today, and their intensity and frequency seem to rise each year. IDC research[2] found that 79% of IT and business leaders had activated a disaster recovery plan in 2021, and yet some enterprises still don't have a robust strategy in place. Like security defences, disaster recovery strategies need to be multi-layered, and while other regions have factored extreme weather into the equation for decades, climate change is making these disasters impossible to ignore in UK recovery plans.

Preparing for the worst

Over the summer we witnessed climate-based extreme weather events across continental Europe and as we look to 2024 and beyond, preparing for such events should be on every CISO's agenda. Last year's record heatwaves in the UK were the second highest in Europe[3] and even triggered wildfires. Weather events will continue to have a significant impact in the years to come and these events should be considered a meaningful threat to business continuity.

Nine out of ten organizations associate a single hour of downtime with more than £300,000 in damages[4] – an estimation that only continues to rise, and which spells out not just revenue loss but potential business closure for the vast majority. Even a loss of data for ten days has driven many otherwise robust businesses to bankruptcy in recent years. Whether it's a blackout or risk to IT infrastructure, the damage of these downtimes to a business, its customers and employees alike can't be undervalued.

Downtime can be costly, and investing upfront in the ability to failover your systems in the event of a physical disaster could be the difference between business success and serious financial losses. Disaster Recovery (DRaaS) allows organizations to replicate all IT workloads and applications from public or private clouds, for both virtual and physical environments at a highly successful price point.

It only takes one incident to harm an organization. So, a tested business continuity plan is a fundamental step to ensure lasting profitability for your business.

Future proofing your operations

In today's threat landscape, disaster recovery is an essential part of any security strategy. Focused on quickly recovering and maintaining data and crucial functions in the wake of an unplanned incident, the first step of any DR strategy lies in assessing exactly which applications, servers, and types of data are most important.

In short, CISOs need to make sure their disaster recovery plans are synchronized with their business's priorities and engage all departments in deciding what these are. Risk assessment is vital: IT managers and their teams are obliged to evaluate the risk of data loss and the impact that any given incident can have on the organization in both the short term and the long term. Many organizations can ensure they are prepared for an incident by regularly backing up their systems and data across the cloud and in air-gapped copies, leveraging automation where possible. Companies utilize different types of data protection products (backup and recovery software, mirrors, and replicas) alongside disaster recovery tactics to ensure data recovery in case any failure happens.

Factoring in the physical

Businesses need to prepare themselves for the worst, and IT teams bear that strain. Proactively seeking out trusted partners and investing in a managed DR service before disaster strikes allows businesses to ensure business continuity and peace of mind, even at the worst moments.

The consequences of climate change are being felt globally and these physical threats to business continuity are becoming impossible for IT teams to ignore. The new laws around climate-related corporate disclosure[5] should mean that UK businesses are already considering these impacts, but they need to play a growing role in recovery planning from the outset.

Be mindful of the geographic risks that your on-premises and cloud data centres may be operating in, be proactive in planning disaster recovery strategies for each disaster event that your risk assessments indicate, and be persistent in testing and refreshing your backups.

Reference

[1] Carrington, D. (20 April 2023), 'Frightening': record-busting heat and drought hit Euorpe in 2022, The Guardian. Available at: https://www.theguardian.com/environment/2023/apr/20/frightening-record-busting-heat-and-drought-hit-europe-in-2022

[2] Goodwin, P. (May 2022), The State of Ransomeware and Disaster Preparedness: 2022, IDC. Available at: https://www.zerto.com/wp-content/uploads/2022/05/idc-the-state-of-ransomware-and-disaster-preparedness-2022.pdf

[3] The Copernicus Climate Change Service (2022) ESOTC 2022 Europe Temperature. Available at: https://climate.copernicus.eu/esotc/2022/temperature

[4] DiDio, L. (30 September 2021), The Cost of Enterprise Downtime, TechChannel. Available at: https://techchannel.com/IT-Strategy/09/2021/cost-enterprise-downtime

[5] HM Government, (29 October 2021), 'UK to enshrine mandatory climate disclosures for largest companies in law'. Available at: https://www.gov.uk/government/news/uk-to-enshrine-mandatory-climate-disclosures-for-largest-companies-in-law