Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Resilience through backup and recovery

Jon Fielding, Apricorn

Securing data is a critical component of any business strategy. But having a backup of that data has not always been at the top of the priority list. Until now.

As a result of the pandemic, organisations have had to accelerate their remote workforce support, digital transformation journeys and migration to the cloud. IT leaders must ensure they have data protection strategies in place to address these new requirements.

This change has generated a distributed and highly complex ecosystem resulting in a data sprawl that’s putting enormous pressure on businesses to not only secure that data, but also ensure that they have a backup and recovery plan in place. Backing up data keeps information safe and enables fast response, restoration and recovery in the event of a disaster.

Unfortunately, organisations often forget to back up, assume that the data is already protected or simply cross their fingers. The recent OVH Cloud datacentre fire is a prime example of a failed backup and recovery procedure and the need to be resilient in the face of any digital disruption. While OVH had its customer data backed up, it had done so in the same location, so both sets of data were destroyed.

It is important to remember that having one backup copy is not enough. The 3-2-1 rule for backing up data remains a tried-and-tested method for ensuring the integrity of copied data and is essential to disaster recovery efforts. This rule says there should be at least three copies of data stored on two different types of media, one of which is offsite. Having at least three different versions of your data ensures that you can recover from accidents that affect multiple versions, and you should not have both copies of your data on the same media.

It’s critical to have an offline copy in addition to on-premise and cloud storage options, back up locally on hardware-encrypted storage devices, and mandate employees to do this every day. With removable (and encrypted) media that is always available and independent of your computing environment, you will have a backup that you have complete control over, is local to you and is offline.

By deploying removable storage devices with built-in hardware encryption, a business can also roll this approach out across the workforce, ensuring that all data can be stored or moved around safely offline.

If your organisation is attacked, data backups are an effective way to recover. In the case of a ransomware attack for instance, where data is encrypted and inaccessible, practising proper data backup hygiene is a must. It is critical to store regular backups offline. Employees can then back up to a hardware device and store their data locally, offline. In the event that they have a hardware failure or a malware attack, they have a quick way to restore from a clean, protected data set.

Data recovery capabilities should be considered as critical functions of an organisation’s business continuity plans. In the event of a data loss, being able to recover and restore quickly is imperative. Organisations cannot afford to wait long periods to get up and running again. Implementing a recovery plan allows users to proactively prevent or recover quickly from disasters, ensuring that data is safe and that mission-critical business applications are available.

Business data is at risk wherever it is housed but retaining multiple copies of data provides the insurance and flexibility to restore to a point in time not affected by data corruption or malicious attacks and will bolster your cyber resilience and recovery process, should disaster strike.

Due to the Covid-19 pandemic, many conferences are being cancelled, postponed or converted into virtual events. The events listed here were still planned to proceed at the time of publication.

8–12 November 2021
OWASP Global Appsec USA
Virtual event
https://owasp.org/events/

14–15 November 2021
THOTCON
Chicago, IL, US
https://thotcon.org/

15–19 November 2021
Hack in Paris
Virtual event
https://hackinparis.com

16–18 November 2021
European Cyber Week
Rennes, France
https://en.european-cyber-week.eu

5–8 December 2021
Security Weekly Unlocked
Florida, US
https://events.securityweekly.com/unlocked2021

9–10 December 2021
ICCS
Cardiff, UK
https://iccs2021.iaasse.org/index.html

10–13 January 2022
FloCon
Virtual event
https://bit.ly/2F0WyUm

2–4 February 2022
IT-Defense 2022
Berlin, Germany
https://bit.ly/3mh1Ahj

2–3 March 2022
Cloud & Cyber Security Expo
London, UK
www.cloudsecurityexpo.com