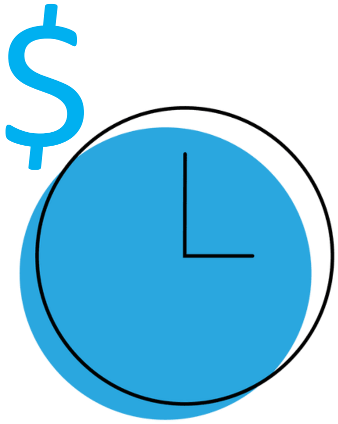
THE REAL COST OF DOWNTIME

THE COST OF DOWNTIME



The majority of businesses today rely on a robust interconnected infrastructure featuring databases, hardware and software. These features are designed to help businesses streamline their operations and improve overall efficiency levels. However, it can come at a cost when an IT incident occurs.

Despite advances in infrastructure robustness, businesses will always be at risk of suffering downtime. This can bring all business activity to a halt, lasting anywhere between a few hours to days or weeks. When a company cannot carry out its business functions and staff are left with the inability to trade, immediate and detrimental revenue losses are inevitable. As the saying goes, time is money.

How costly exactly? Depending on the size of the organisation, the cost per hour of downtime is anywhere from $10,000 to over $5 million[1]. When you factor in how long it can take to resume normal operations, the impact is apparent. According to IDG, it takes around 7 hours to resume normal operations after a data loss incident, with 18 per cent of IT managers saying that it takes 11 to 24 hours, or even longer[2]. The numbers clearly speak for themselves.

Depending on the size of the organisation, the cost per hour of downtime is anywhere from $10,000 to over $5 million[1]

But it’s not just a numbers game. Downtime has associated soft costs, including damaged brand reputation, lost business opportunity, and lowered employee morale. Losing customer trust is another. The accountability associated with losing customer data during downtime is further heightened by the introduction of new data compliance legislations, such as the General Data Protection Regulation (GDPR) in Europe and the mandatory Data Breach Notification in Australia, as it requires businesses to make public when a data breach occurs. This requirement itself can only be further damaging to a business’ brand and customer trust.

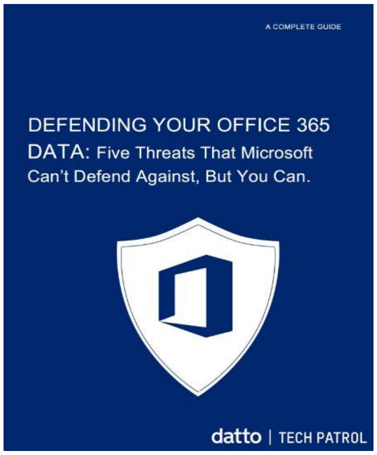
Or, in even more dire scenarios, the cost of downtime can have much more serious repercussions, such as when a medical institution that relies heavily on accessing patient information through its database suffers an outage. This happened to the UK’s National Health Service system when it was overtaken by ransomware, leaving critical private medical information suspended for cryptocurrency[3].

For this reason, data backup and business continuity solutions are essential for businesses to implement, regardless of size, industry, and geographic location. The downtime costs that businesses suffer without protections in place justify the need to invest in them.

What causes downtime?

The increase of downtime events experienced in the past five years by IT professionals is due to a combination of factors[4]. One study indicates that power outages account for 33 per cent, followed by hardware and human error at 23 per cent and 15 per cent, respectively. Meanwhile, natural disasters account for just 9 per cent of downtime. As it turns out, businesses should be warier of their own employees and hardware than of natural disasters.

You may also be interested in:



A COMPLETE GUIDE

DEFENDING YOUR OFFICE 365 DATA: Five Threats That Microsoft Can’t Defend Against, But You Can.

datto | TECH PATROL

Defending Office 365 White Paper
DOWNLOAD NOW

Ransomware and malware attacks are increasingly responsible for downtime. This is when cybercriminals actively attempt to get into a business' servers and hold their data for ransom. Across Australia and New Zealand, an estimated 6 per cent of small-to medium-sized businesses (SMBs) fell victim to malware from 2016-2017. The total amount of ransom paid for these attacks during the period was $12.6 million. However, it's not the ransom that breaks the bank of businesses; it's the downtime and data loss that cuts the deepest. As a result of a ransomware attack, 79 per cent of managed service providers report clients experienced business-threatening downtime[5].

But it's not just the SMBs that are being impacted. We can just look to the Australian Bureau of Statistics (ABS) as an example. During the 2016 Census night, the ABS was forced to shut down its website and was offline for two days because it was subject to a distributed denial of service (DDoS) attack. The ABS estimated the cost of that outage billed close to $30 million[6].

Safeguarding your business from downtime

Thinking about data backup is a good first step. But what good is backup data without a quick and reliable solution for restoring that information if needed? A business continuity solution ensures your organisation can get back up and running in a timely matter if disaster strikes. To truly protect your business from costly downtime, you need to implement both.

Using local backup for business continuity works well for quick restores because the data is right there, fast and easy to restore back to its original location. But what happens if the power goes out? If the device fails? If the data or server is stolen or destroyed in a natural or man-made disaster? Storing data in the cloud is more attractive for all of these reasons. But cloud-only backup is risky because you can't control the reliability of bandwidth. Restores tend to be difficult and time-consuming. After all, the cloud can fail, too.

This is why a hybrid-cloud solution is ideal. Your data is first copied and stored on a local device. That way, if something happens, you can do a fast and easy restore from that device. With a hybrid-cloud solution, your data is also replicated in the cloud. So if anything happens to that device, you've got off-site cloud copies of your data. This means you won't need to move copies of your data offsite physically. With a hybrid-cloud solution, no matter when disaster strikes, your business can continue operating while the IT professionals are resolving the issue.

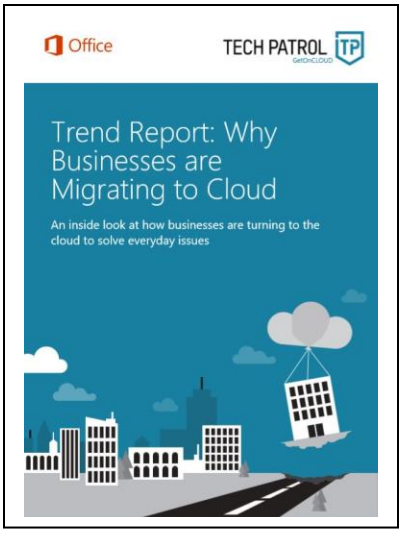
When talking about business continuity, it can be thought of in terms of a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO).

- **Recovery Time Objective (RTO):** The duration of time within which a business must be restored after a disruption to avoid unacceptable consequences.

- **Recovery Point Objective (RPO):** The maximum tolerable period of time in which data might be lost due to a disaster.

79 per cent of managed service providers report clients experienced business-threatening downtime[5]

You may also be interested in:



Office

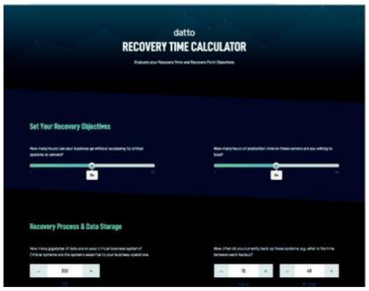
TECH PATROL

Trend Report: Why Businesses are Migrating to Cloud

An inside look at how businesses are turning to the cloud to solve everyday issues

Trend Report

DOWNLOAD NOW



datto

RECOVERY TIME CALCULATOR

Set Your Recovery Objectives

Recovery Process & Data Storage

Datto's Recovery Time Calculator

DOWNLOAD NOW

Calculating your desired RTO helps determine the maximum time that your business can afford to be operating without access to data before it's at risk. Alternatively, by specifying the RPO, you know how often you need to perform data backups. You may have an RTO of a day, and an RPO of an hour depending on what your business requires. But calculating these numbers will help you understand what type of data backup solution you need.

Taking lessons from real-life learnings

Queensland's Whitsunday Regional Council (WRC), which provides local government resources and support to major townships including Airlie Beach, Bowen, Cannonvale, Collinsville and Proserpine, witnessed the need for business continuity first-hand when Cyclone Debbie hit the region in early 2017, and saw the genuine possibility of losing its 64 servers across two sites located in Proserpine and Bowen.

As such, in anticipation of the Cyclone's arrival, WRC together with Mangano IT, Datto and Telstra BTS, ensured all servers were backed-up locally to secure onsite appliances, and also replicated to the cloud. The servers were also spun up in the cloud in readiness for a full-scale disaster recovery. Telstra was instrumental during this phase as they increased the available bandwidth to ensure the initial transfer to the cloud completed before the cyclone hit.

The project ensured the uninterrupted delivery of IT services for WRC. These IT services facilitate the delivery of essential council services to the community, such as town planning and demographic information for the region, plus key plant and infrastructure information used to deliver water and manage sewage.

In another example, while Civil Contractors Federation South Australia (CCFSA), a member-based representative body of civil engineering contractors in Australia, was not faced with an imminent natural disaster, it did fall victim to a targeted social engineering attack. This was whereby an employee opened a link in a well-crafted and convincing email that spread a CryptoLocker virus throughout the organisation's network. As a result, nearly all CCFSA's files were encrypted, including several databases.

Fortunately, CCFSA worked with Datto partner and MSP shop, Geek IT, on an ongoing basis, which meant it had deployed Datto's Business Continuity and Disaster Recovery (BCDR) solution months before and was able to minimise CCFSA's downtime. Geek activated its business continuity plan and within 30 minutes CCFSA's core services were restored, with all services restored within two hours. During the restore process, CCFSA staff experienced minimal interruptions, and were able to instantly access their files through the cloud.

Geek activated its business continuity plan and within 30 minutes CCFSA's core services were restored, with all services restored within two hours.

Had Geek IT not deployed Datto's solution for CCFSA, the estimated downtime would be 15 hours 22 minutes. Factoring in employees affected, average wage, overhead costs and revenue lost, Geek estimated downtime would cost CCFSA $3,955 per hour. Altogether, the total cost of this event with legacy systems was estimated to be $65,000. However, because Geek had implemented Datto, the cost to the business was less than $3,000 – meaning Geek saved CCFSA more than $60,000.

Conclusion

While IT budgets vary in size for different businesses, the data risks they face are the same. This is why it needs to be a priority for businesses to implement business continuity and disaster recovery (BCDR). This ensures businesses can continue trading whenever a crisis strikes – whether it's a natural disaster, a malicious attack, hardware failure, or software corruption –- while the IT teams work on addressing the backend issue.

Regular, company-wide backups of control systems ensure that all information will be safeguarded against worst-case scenarios. Older versions of information will always be better than starting from scratch.

Given malicious attacks are on the rise, and new legislations including the General Data Protection Regulation and the Notifiable Data Breach scheme are in place, the pressure is on businesses to specifically look at their anti-virus, firewall and overall security hygiene. The easiest way to understand this is to carry out regular risk audits to highlight problem areas that need to be addressed.

As it turns out, your employees are more likely to be the cause of downtime than natural disasters, therefore businesses need to train and empower employees to be able to diagnose and problem-solve issues on their machines to minimise the impact of company-wide downtime.

While IT outages are sometimes unavoidable, downtime doesn't have to be. Being proactive rather than reactive will save your business a lot of pain. Having the correct preparation strategy in place will ensure that businesses are able to mitigate, and sometimes even prevent, the impacts of any failures. Expect to be prepared for an outage but never accept downtime.

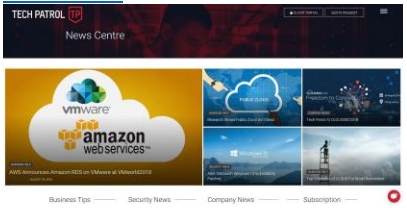
About TECH PATROL

Tech Patrol is a skilled organisation that is committed to delivering professional technology Services mixed with corporate level solutions to consistently meet all the IT requirements of an Australian or International business.

You may also be interested in:

New Blog Page

VIEW NOW



Corporate Headquarters
TECH PATROL PTY LTD
Suite 101, 24-30 Springfield Ave
Potts Point, NSW 2011.
Australia
Sales@techpatrol.com.au
www.techpatrol.com.au

[1] https://www.statista.com/statistics/753938/worldwide-enterprise-server-hourly-downtime-cost/

[2] http://resources.idgenterprise.com/original/AST-0064964_ExaGridQuickPulse_71112.pdf

[3] https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/

[4] https://www.linkedin.com/pulse/disaster-recovery-statistics-every-organization-know/

[5] https://www.datto.com/au/blog/datto-state-of-the-channel-ransomware-report-anz

[6] http://www.abc.net.au/news/2016-10-20/census-may-cost-another-$30m,-committee-hears/794840