The Cost of Downtime

The majority of businesses today rely on a robust, interconnected, infrastructure featuring databases, hardware and software. These features 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 IT infrastructure, 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 hourly cost 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.

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. Disclosing a data breach can be further damaging to a business' brand and customer trust.

[1] https://www.statista.com/statistics/753938/worldwide-enterprise-server-hourly-downtime-cost/
[2] http://resources.idgenterprise.com/original/AST-0064964_ExaGridQuickPulse_71112.pdf

The cost of downtime can have even more serious repercussions, 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 your business 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 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.

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.[5]

However, it's not the ransom that breaks the bank of businesses; it's the downtime and data loss that cuts the deepest, particularly when the average annual turnover of an Australian business is less than $2 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.

At a minimum, your business continuity plan should ensure that your company can perform basic operations such as communicating via email and phone, processing orders and issuing cheques. It also should provide a detailed, easy to follow plan for returning to normal business operations.

[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.abs.gov.au/ausstats/abs@.nsf/mf/8165.0

Using local backup for business continuity works well for quick restores because the data is right there. 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, too.

It's important for businesses to note that not every cloud service is made equal. While cloud services are nearly always stored in an encrypted form that would need to be cracked before an intruder can access any stored information, this does not mean it's entirely out of reach from the bad guys. Businesses need to understand that just because it's in the cloud does not mean they're automatically protected. According to Skyhigh, only one in ten out of the 20,000 cloud service providers in market follow industry best practice for encrypting data and enterprise grade security controls.[7]

As with any contract, it's important to be aware of software-as-a-service terms and conditions. A common misconception is believing a business' data is protected if they have adopted cloud services. This is often not the case! The onus to keep any data secure is on the business – not the service provider. As businesses rely so heavily on technology partners, it pays to understand their organisation's security posture, as it can be a reflection on the way you operate and your reputation in the market.

This is why a hybrid-cloud solution is ideal. Your data is first copied and stored on a local device. 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. If the device is compromised,, you've got off-site cloud copies of your data. This means you won't need to move copies of your data offsite, physically. A hybrid cloud solution, ensures that no matter when disaster strikes, your business can continue operating while 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.

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.

[7] https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/

Taking Lessons From Real-Life learnings

Civil Contractors Federation South Australia (CCFSA), a member-based representative body of civil engineering contractors in Australia, fell victim to a targeted social engineering attack. This occurred when 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, which meant it had deployed a Business Continuity and Disaster Recovery (BCDR) solution months before and was able to minimise CCFSA's downtime. Geek IT 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.

Had Geek IT not deployed Datto's solution for CCFSA, the estimated downtime would have been 15 hours 22 minutes. Factoring in employees affected, average wage, overhead costs and revenue lost, Geek IT 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 IT had implemented Datto, the cost to the business was less than $3,000 – meaning Geek IT saved CCFSA more than $60,000.

Conclusion

Whether it's a natural disaster, a malicious attack, human error, hardware failure, or software corruption regular, company-wide backups of control systems ensure that all information will be safeguarded against worst-case scenarios.

While IT outages are sometimes unavoidable, downtime doesn't have to be. Whether it's a natural disaster, a malicious attack, human error, hardware failure, or software corruption, being proactive rather than reactive will save your business a lot of pain. The correct preparation strategy - which includes regular company-wide backups of control systems - will ensure that your information is safeguarded against worst-case scenarios, allowing you to mitigate, and sometimes even prevent, the impacts of any failures. Be prepared for an outage, but never accept downtime.

For more information please contact:
Steve Naugle | President
Phone: 7272350484
Email: steve.naugle@mynetcraft.com
MyNetCraft Corporation | https://www.mynetcraft.com
6835 9th Avenue North, Saint Petersburg, FL, 33710