NEWSLETTER

RJ2 Technologies Monthly Newsletter
August 2024

1701 Golf Road
Suite T3-300
Rolling Meadows, IL 6000

(847) 303-1194

www.rj2t.com

In this newsletter:

Why 60% Of Data Backups Fail Businesses When They Need Them Most

From natural disasters and cyber-attacks to accidental deletion, there are many reasons a business needs to back up its data. However, Avast's latest findings on disaster recovery highlight an alarming issue for small and medium-sized businesses (SMBs): 60% of data backups are not fully successful, and half of the attempts to recover data from these backups don't work. This leads to businesses being offline for an average of 79 minutes, costing them roughly $84,650 for every hour of downtime.

Still, not all backups are created equal. It's important you're aware of backup best practices, so you're confident your backup solution will work when you need it most.

Why Backups Are Failing

There are a few common reasons backups are incomplete or a restoration fails:

• Backup products are unreliable: When it comes to backups, you get what you pay for. Free or cheap solutions may not offer the robust features of more expensive products. This can result in backups that are not as secure or reliable.

• Backup times are not optimal. If backups are scheduled during high-traffic periods or when data is being heavily modified, there's a risk that not all data will be captured.

• Compatibility issues. As your business evolves, so do your systems and software. However, new systems may not always be fully compatible with existing backup solutions. This can lead to situations where data is not properly saved or, even if it is, cannot be restored correctly because the formats or systems are no longer aligned.

• Human error. Mistakes such as incorrectly configuring backup parameters, accidentally deleting crucial files or ignoring backup schedules and alerts can lead to backup failures.

Cyber-attacks and other disasters are a constant threat. If your backup fails and you get hacked, you might lose data permanently. Additionally, health care and finance organizations have strict compliance regulations around data handling, and failed backups can result in fines, legal challenges and a damaged reputation.

Best Practices For Successful Data Backup And Restoration

Reliable data backups and successful restoration are your lifeline in times of crisis. From choosing the right backup solution to regular testing and daily monitoring, these best practices protect your data from surprise disruptions, ensuring your business doesn't miss a beat, no matter what comes your way.

1. Pick a solid backup solution.
Don't just go for the big names in backup software; some might not deliver what they promise. Digging deep and finding a solution that suits your needs is essential. For example, immutable backups are a must-have for anyone needing to meet strict compliance rules, as they can't be changed or deleted, even by a ransomware attack. Talk with your IT provider about the backup technologies they're using for you, how quickly you can expect to recover data, what kind of downtime you might face and whether your backups are on the cloud, local or a mix of both. Make sure your backup ticks all the boxes for compliance, especially if you're in a sensitive field like health care.

2. Use the 3-2-1 rule.
Once you have a reliable backup solution, consider using the 3-2-1 backup rule, a standard set of best practices for data recovery. The rule recommends storing three copies of your data in two different formats, with one copy stored off-site. This significantly reduces your risk of total data loss.

3. Make sure a backup status report is being generated daily.
Ensure someone – either you or someone on your IT team – is checking the backup status every day. Incomplete backups should be followed up on immediately. Even if your IT team receives a daily report, ask to have a weekly or monthly report delivered to you too, so you can verify that your backups are successful.

4. Do regular restore tests.
Like a fire drill for your data, do a trial run and restore some files or even the whole server every few months to ensure everything works as it should. It's one thing to have backups, but another to ensure they are in good condition and the data can be retrieved as expected.

Don't ignore your data backups! Backups might seem like one of those "set and forget" tasks, but when disaster strikes – be it a flood, fire or cyber-attack – your backup could be what saves your business. If you haven't already, start a conversation with your IT provider and make sure your backup strategy is solid and reliable.

To defend your business from cyber-attacks and other disasters, email **marketing@rj2t.com** to create a customizied plan for your business needs. We want to focus on your IT so you can focus on doing what you do best, growing your business!

Recognizing Excellence

Employee Recognition

Here at RJ2 Technologies we recognize those who put in hard work and dedication not only towards our services, but to the teamwork they build amongst themselves.

Kevin Dann - Systems Engineer

Kevin has been with RJ2 Technologies since October of 2019, but is familiar with the company as he had an internship with RJ2 back in 2008-2009. Kevin says working in the managed service industry has been a quite dynamic and rewarding experience that also comes with its own set of challenges.

Outside of work, Kevin enjoys taking his dog out to the park, playing golf, and catching up with some of his favorite TV series.

Reading Corner

Should You Verify Your Profile On LinkedIn?

In 2022, LinkedIn launched verification options where most users can submit a personal ID, employer e-mail or workplace ID to prove they're a real person amid an increasing number of fake accounts. In the second half of 2021 alone, Microsoft (LinkedIn's parent company) removed over 15 million fake accounts. If you feel weird about sharing your biometric or ID information online, that makes sense. But verification isn't a bad idea because of the number of fake accounts on LinkedIn. Although LinkedIn reports using the highest security protections, consider using the employee e-mail option if it's available (employers must have a LinkedIn page and turn on this feature) because it's the least risky.

Deepfakes Are Coming To The Workplace

Deepfakes result from people using AI and machine-learning technology to make it seem like someone is saying something they never actually said. Like every other tech on the market, it can be used with good and bad intentions. For example, David Beckham appeared in a malaria awareness campaign, and AI enabled him to appear to speak nine different languages. On the other hand, pornographic deepfakes of Taylor Swift went viral on X (to the horror of Swifties worldwide), and audio deepfakes of Biden encouraging New Hampshire voters not to cast ballots caused concern among experts.

However, deepfakes aren't happening only to high-profile politicians and celebrities – they are quickly making their way into the workplace. In April 2023, forensics research company Regula reported that one-third of businesses worldwide had already been attacked by deepfake audio (37%) and video (29%) fraud. Regula also noted that the average cost of identity fraud, including deepfakes, costs global SMBs $200,000 on average.

How Deepfakes Are Impacting The Workplace

While deepfake technology is used to commit a variety of crimes, there are two ways deepfakes currently cause harm to businesses like yours:

1. Impersonation/Identity Fraud Schemes

2. Harm To Company Reputation
One of the most common deepfake attacks is when AI impersonates an executive's voice to steal credentials or request money transfers from employees. Other attacks include deepfake videos or audio of a CEO or employee used to disseminate false information online that could negatively affect a brand. More than 40% of businesses have already experienced a deepfake attack, according to authentication experts at ID R&D.

What To Do About It
There are a few simple things you can do to prevent deepfakes from having damaging consequences on your business.

1. Review policies around technology and communication
Ensure you have transparent communication practices and that your team knows how communications are used internally. Would a company executive ever call an employee to place an official request for money or information? If not, employees should be suspicious. Also, encourage employees to verify any e-mail or phone request they aren't sure about.

2. Include deepfake spotting in cyber security awareness training
Double-check that your cyber security awareness training covers how to spot deepfakes. Things to look for include unnatural eye blinking, blurry face borders, artificial-looking skin, slow speech and unusual intonation.

3. Have a response plan
Deepfake attacks are in their infancy, and you can expect to see more attacks like this in the future. Be sure your company's leadership talks about how to respond if a deepfake attack impacts your company. Even though there's no perfect solution to the problem yet, the worst thing that can happen is to be caught unprepared.

Call **(847) 303-1194** for more information on deepfakes.

5 Tech Tips to Help Reduce Stress Related to Technology

1. Ensure Your Technology is Up to Date
Keeping your devices up to date is crucial. Outdated software and hardware can cause problems like slow performance and security issues. Regularly install updates and replace hardware when necessary.

2. Simplify your Technology
Too many different tools can lead to confusion and being
overwhelmed. Streamline your workplace technology by selecting key tools that work well together. Focus on features and functionality that enhance productivity.

3. Provide Training and Support
Invest in training and support for essential business technology. Whether in-house or outsourced, this helps users become proficient and minimizes errors and frustration. Get the most value from your technological investments.

4. Have a Back-Up Plan
Technical difficulties cause stress and hinder productivity. Always have a contingency plan for unexpected issues. Regular data backups and disaster recovery strategies are essential.

5. Take Breaks and Disconnect
Step away from screens periodically. Sunlight and nature boost mental health. Engage in centering activities to recharge and reduce stress.

For more Tech Tips, follow our social media accounts on page 5 for #TechTipTuesdays!

Vendor Partner Highlight

RJ2 Technologies is happy to share their recent partnership with Axcient, a platform that provides managed service providers (MSPs) with business continuity and disaster recovery (BCDR) solutions. By using the Axcient x360 portal, MSPs are able to protect their client data and ensure productivity while generating growth and profitability.

RJ2 Technologies will utilize Axcient x360Cloud in their IT stack. x360Cloud automatically backs up Microsoft 365 data so that it can always be located, restored, and audited for uninterrupted business continuity after a data loss incident. Data is backed up to the encrypted, tamper-proof Axcient Cloud so MSPs and their small to medium sized business clients can sleep soundly knowing the data is always available for recovery. **Call RJ2 Technologies at (847) 303-1194** for more information on how we utliize Axcient x360 Cloud.

Is Your Data *Really* Secure in the Cloud?

Are you thinking about moving all or parts of your computer network "to the cloud" but worried about who can access your data? You're not alone – but many security experts, software companies and cloud service providers alike agree that cloud computing offers a MORE secure way to store data. In fact, the US government's cyber security adviser Howard Schmidt had said that cloud computing will enable businesses to catch up on security issues.

That's because most small businesses do NOT have high-security measures in place for their data onsite and lack tight password protection policies, firewall management and backup procedures. The same business owners who verbalize their concern about putting their data in the cloud are backing up their entire network to a tape drive and leaving it in their car overnight – or are using weak passwords for important access points to their network, which are much bigger security risks than storing it in a highly secure, highly redundant cloud platform. That's like saying you'd rather stuff your money into a mattress at home than keep it in a bank because you're not sure who can see and touch your money.

Of course, with any data storage there is risk and there's no way to completely guarantee absolute security. That said, most cloud providers are far more diligent about security and invest millions of dollars into ensuring all aspects of security are as tight as possible. At RJ2 Technologies we have spent a considerable amount of time investigating various cloud solutions and vendors for our clients. If you want more information on cloud security and what to look for, **go to our website at rj2t.com today.**

Stay Connected with RJ2

Stay up to date with the latest tech trends, company updates, tech tips, and more by following us on our social media accounts below. We strongly encourage you to stay connected with the RJ2T family and show your support!

@RJ2Technologies @RJ2Technologies @RJ2Technologies

@RJ2Technologies @RJ2Technologies532