THE CYBERSIDE BRIEF

Insider Wisdom from 20 Years of IT Defense for Your Business Prosperity and Security

INSIDE THIS ISSUE

This monthly publication is provided courtesy of Patrick Birt, President of AdRem Systems Corporation.

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 e**volves, 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.

continued on page 2...

...continued from cover

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.

FREE REPORT:

What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at www.AdRem.com/protect or Call Our Office at (703) 860-2233.

Compliancy Navigator

A Closer Look

DATA PRIVACY VS DATA SECURITY

The importance of data privacy and data security has grown exponentially as organizations today collect and store more information than ever before. Having a robust data protection strategy is critical to safeguard confidential information and to ensure smooth functioning of your business. But before we move on, let's take a step back to understand the key concepts of data privacy and data security.

The terms, data privacy and data security, are often misunderstood and are being used interchangeably. However, they are two separate concepts! Data privacy focuses on how information is handled, stored and used, while data security is concerned with protecting your organization's assets.

UNDERSTANDING DATA PRIVACY

Data privacy deals with the regulations and practices to ensure data is responsibly handled. It includes how information is collected, processed, stored and disseminated. Any organization that collects and stores data or does business across the globe should comply with several privacy regulations, such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Children's Online Privacy Protection Act (COPPA) and other privacy laws.

The aim of these regulations is to protect and enhance consumer and personal privacy. These rules give individuals the right to know what information is collected, why it's collected and how it's processed. As data privacy regulations are growing globally and becoming more complex, privacy requirements are also changing. Non-compliance to these laws could cost your business dearly. In 2019, Google was fined $57 million under the European Union's GDPR law.

Importance of Data Privacy

Data privacy is an individual's right to control who has access to personal information and how it should be used. This also protects personal information from being sold or redistributed to third parties. When organizations collect customers' data, it is the organization's responsibility to protect and preserve their clients' sensitive information. Not having a privacy policy in place or failure to comply with privacy laws can lead to serious consequences, apart from legal actions and financial loss.

UNDERSTANDING DATA SECURITY

Data security is the process of protecting information from unauthorized access, data corruption and data loss. A data security process includes various techniques, data management practices and technologies that act as defense mechanisms to protect data from internal and external threats.

Data security is concerned with what an organization does with the data collected, where and how the data is stored, and regulates who can access the information. A comprehensive data security strategy will help prevent data breaches, ensure business continuity and keep your company's data safe from cyberthreats.

Importance of Data Security

The term "Data is the new oil," coined by Clive Robert Humby in 2006, stands true in today's competitive business environment. Data security is critical for the smooth functioning of day-to-day operations and running a business successfully. Failure to protect your organization's confidential data can damage your brand's value, result in regulatory penalties or shut down your business.

The alarming rate at which cyberattacks are growing has forced organizations of all sizes to consider data security as a top priority. It is estimated that total spending on information security and risk management will exceed $215 billion, outpacing traditional IT spending nearly 5%, by 2024 – this year.

Depending upon the purpose, type of industry or geographical location, your business can implement security compliance frameworks and international standards, such as the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO) and Payment Card Industry Data Security Standard (PCI DSS). These frameworks

continued on page 4...

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.

CARTOON OF THE MONTH

"Oh, that. We beefed up security."

...continued from page 3

provide guidance and best practices for information security to help you assess IT security measures, manage risks, respond to security incidents and improve your information security management system.

DIFFERENCE BETWEEN DATA PRIVACY AND DATA SECURITY

In simple terms, data privacy and data security are two sides of the same coin. They have distinct concepts but are closely related. Achieving data security doesn't ensure data privacy and vice versa, but both are required to establish a comprehensive data protection strategy. Knowing the difference between these terms will help you strategize better, prevent data breaches and stay legally compliant.

Let's distinguish the two concepts with a hypothetical example.
Assume you own a laptop, where you store personal information. To avoid people from accessing those files, you pasted a sticker on the cover that reads 'Do Not Touch'. But in order to add an extra layer of privacy, in case people don't read or ignore the sticker, you locked the computer with a secure password.

There are two things to note here. First, the 'Do Not Touch' sticker tells people to keep away from your laptop, thereby authorizing your privacy. Second, the password ensures no one can access your data, thereby protecting your data from unauthorized access.

HOW TO ACHIEVE DATA PRIVACY AND SECURITY WHILE BEING LEGALLY COMPLIANT

Achieving data privacy and data security and complying with several laws have their own set of challenges. Even large organizations struggle to understand and implement the right security management and compliance measures.

But that shouldn't be the same for your business. To learn how you can achieve and maintain compliance for data privacy and security, contact us today.

PRESENTED TO YOU BY SHERPA, AN ADREM SYSTEMS COMPANY:

SHERPA An AdRem Company SYSTEMS

theSherpa.us | 571-360-3926 | info@thesherpa.co

Celebrating Team Achievements

Kaseya Connect Global 2024

Last week our team had the opportunity to network, explore new technologies, and advance their skills and expertise at the Kaseya Connect Global conference in Las Vegas!

We're proud to announce our dedicated techs who attended the event successfully completed and passed certifications on our vendor products. This accomplishment underscores our commitment to staying at the forefront of industry knowledge and enables us to deliver even more value and innovation to the community.

July 20, 1969, just eight years after President Kennedy made one of history's most ambitious declarations – the US would send a man to the moon and back – Neil Armstrong and Edwin "Buzz" Aldrin became the first people to set foot on the moon.

Today, Buzz is a philanthropist, author and renowned speaker who shares what being a space pioneer taught him about life on Earth: no mission is completed alone, failure is a crucial milestone of success and to never stop envisioning your next impossible dream .

Lessons From "The Moonman"

Dream The Impossible

Aldrin remembers President Kennedy's announcement in 1961, and although he wasn't sure how they'd do it, he said, "We did have a leader with that determination, the courage and the confidence that we can get there." Without a leader brave enough to share an impossible vision, ideas never get off the ground. In business, it's crucial to give your team a meaningful vision to rally around, something they want to be a part of.

Behind Every Successful Mission Is A TEAM

The "backroomers" – software engineers, secretaries and even the tailors who manufactured spacesuits – were all necessary to Apollo's safe launch and return to Earth. When Apollo 11 landed, the world cheered. "People were not just cheering for three guys but for what we represented," Buzz recalled in a speech. "That by the nation and the world coming together, we had accomplished the impossible, and the true value of it is the amazing story of innovation and teamwork that overcame many obstacles to reach the moon."

Success is rarely the story of one person. Rather, it's often the story of many people working together. "There are a lot of people out there in the universe who wish you well and want to be your friend. Let them help you," Buzz said. "You don't have to carry it all on your own."

Failure Is A Mark Of Growth

In the book *No Dream Is Too High*, Buzz explains how everyone at NASA knew the risks involved in their mission. Only by planning for failure and testing every system, component and spacesuit zipper could they improve design and functionality – failure was part of the process.

"Some people don't like to admit that they have failed or that they have not yet achieved their goals or lived up to their own expectations," Buzz wrote. "But failure is not a sign of weakness. It is a sign that you are alive and growing."

Know What's Next

What happens when you accomplish what you set out to do after all the cheers and high-fives? After Apollo, Buzz wrote in the book Magnificent Desolation, "There was no goal, no sense of calling, no project worth pouring myself into."

He sunk into severe depression for years, finally realizing, "I needed to realign my direction and find a new runway."

Today, he's a speaker, author and philanthropist for STEAM-based education to help get the next generation of heroes to the moon – and beyond. Perhaps the key to lifelong fulfillment is never to "land" for too long – to keep learning, growing and achieving impossible things.

AdRem SYSTEMS

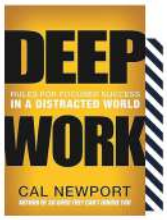
DEEPFAKES ARE COMING TO THE WORKPLACE

OUR MISSION

To apply our 20 Year Legacy of knowledge and innovation, to defend Critical IT Networks, and encourage a more secure nation of Tomorrow by delivering Today's technologies with respected, trusted, and proven individuals.

DEEP WORK

By Cal Newport



It's undeniable: we're more distracted than ever. From text messages and e-mail pings to social media and our own disruptive thoughts, the relentless influx of distractions is sabotaging our productivity and even our ability to be present in our lives. *Deep Work*, by Cal Newport, is a compelling guide to help us take back our focus and cultivate more fulfillment in our work. Newport introduces readers to four "rules" to transform our minds and habits into a hyper-focused superpower: work deeply, embrace boredom, quit social media and drain the shallows. Through engaging stories and practical advice, the book outlines a framework for cultivating a deep work ethic, promising professional growth and a more profound sense of personal fulfillment. *Deep Work* is an essential read for those looking to navigate a distracted world with grace and achieve focused success.

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.