The AvTek Chronicle

Wayne's World Where in the world is WAYNE?

Ingram Micro and HPE's Partner Summit 2024
April 29 – May 2,
Asheville, North Carolina

TBA Annual Conference
May 8-10,
Arlington, TX

TXCPA Spring Accounting Expos
May 21-22,
Spring, TX

Wayne's Deep Dive Episode 5
May 28
1pm CST

May 2024

Wayne Hunter is the President and CEO of AvTek Solutions, Inc. where he concentrates his efforts on providing the best solution to customers.

Wayne has over 30 years of experience in Information Technology, focusing on implementing storage and data systems, IT management, and systems integration.

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,

Continued on pg. 2

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.

Maintain Regulatory Compliance for Business

It is essential for entities in highly regulated industries, such as healthcare, finance and manufacturing, to have checks and balances in place to ensure compliance with critical regulations. A lapse in compliance standards can be costly, not only in the form of assessed penalties but also in terms of security vulnerabilities.
Insider threats should be a consideration in any complance strategy. Insider threats are employees or contractors who pose a risk to an organization by mishandling sensitive data or violating security policies, whether intentionally or not.

KEEP INSIDER THREATS IN CHECK

CONDUCT ROUTINE COMPLIANCE AUDITS

Organizations that do not regularly audit their adherence to compliance standards are more vulnerable to cyberattacks perpetrated by insiders or other threat actors, which can be costly financially and reputationally. There is also the possibility of compliance violations, which can result in additional financial penalties.

TRACK ACCESS

Organizations need to track access to their critical data and systems to prevent insider threats. Tracking access is a primary element of compliance that helps organizations protect themselves from a number of risks. Patient data from a leading hospital was once leaked to the public due to poor access tracking. As a result, the patients and their insurers sued the hospital for failing to maintain the necessary security measures.

HAVE PROPER DOCUMENTATION

Regulators may audit your compliance at any time. Inadequate proof of compliance documentation can cause delays, force you to incur rush fees with an external auditor, and can potentially result in additional fees from regulating agencies.

OTHER CONSIDERATIONS TO REMEMBER

1

Rather than just assuming you are compliant with safety regulations, a ROUTINE COMPLIANCE AUDIT will ensure you know where you stand.

2

Most industries require businesses to adhere to some level of compliance. Depending on the industry, these requirements can vary greatly.
It's critical to BE AWARE of all the compliance egulations that apply to your business.

3

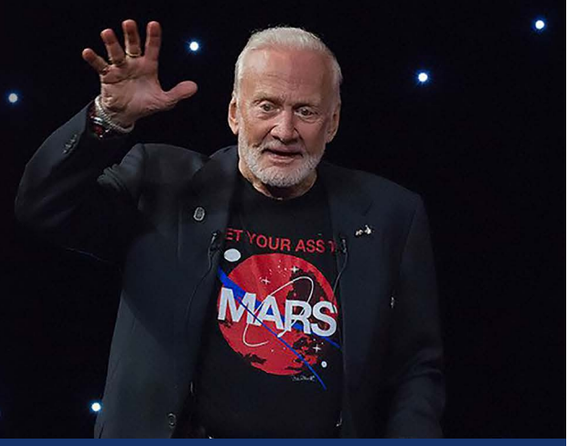
When faced with an audit from a regulatory body, demonstrate to them that you have made a strong effort to COMPLY with stringent regulations such as HIPAA. This will likely increase the possibility of the regulators being lenient during the audit process.

PARTNER FOR SUCCESS

It is critical for businesses to maintain compliance with regulatory requirements to survive and thrive in today's business environment. By partnering with an IT service provider, you can ensure that your resources and processes are set up to meet all industry-specific compliance needs.

WE CAN HELP YOU MAINTAIN COMPLIANCE. CONTACT US TODAY.

Astronaut Buzz Aldrin's Lessons To Achieve Impossible Dreams



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.

Shiny New Gadget Of The Month

Amazon Basics 8-Sheet High Security Micro-Cut Shredder

Your recycling and garbage bins are a jackpot for identity thieves. Even if you don't handle CIA-level classified documents, criminals can use your recycled mail – like bank or credit card statements – to steal personal information. A shredder like the Amazon Basics 8-Sheet High Security Micro-Cut Shredder is an easy and affordable way to secure your information.

You can shred up to eight pieces of paper simultaneously, with a five-minute continuous run time. Recycle the shreds, use it as packaging material or add it to your cat's litter box. Either way, a shredder keeps your information out of the hands of criminals.

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.

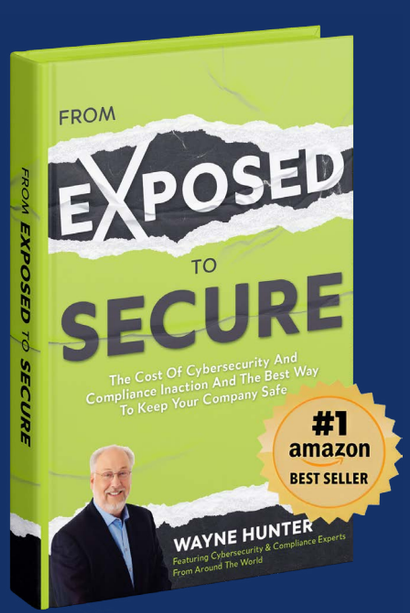
2. **Include deepfake spotting in cyber security awareness training.** Double-check that your cyber security awareness training covers how to spot deepfakes. Things to look for include unnatural eye blinking, blurry face borders, artificial-looking skin, slow speech and unusual intonation.

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.

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.

Protect Your Business and Assets from Hackers!



Here's What You'll Learn From The New Book, From Exposed To Secure:

- The biggest cyberthreats that could take your company down. Page 18.
- How to take the confusion out of compliance. Page 32.
- The incorrect perceptions on compliance that could be putting you in danger. Page 41.
- 8 best practices to minimize risk. Page 63.
- The surprising first line of defense. Page 72.
- How to protect yourself from fines…and jail. Page 141.
- 10 strategies you must have in place to be considered for insurance. Page 174.
- Critical steps to take immediately if you are hacked. Page 182.
- How an IT expert keeps her own kids safe online. Page 205.

And much more.

CHECK IT OUT NOW