Virtual DataWorks

TECH BYTES

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

We have a passion for technology and a genuine desire to assist people.

"Call us for a brief, genuine conversation to see how we can enhance your technology stack!"

- **Matthew Dewees**
President

HOW CAN YOUR BUSINESS BE IMPACTED BY THE NEW SEC CYBERSECURITY REQUIREMENTS?

Cybersecurity has become paramount for businesses across the globe. As technology advances, so do the threats. Recognizing this, the U.S. Securities and Exchange Commission (SEC) has introduced new rules. They revolve around cybersecurity. These new requirements are set to significantly impact businesses.

UNDERSTANDING THE NEW SEC CYBERSECURITY REQUIREMENTS

The SEC's new cybersecurity rules emphasize the importance of proactive cybersecurity measures. These are for businesses operating in the digital landscape. One of the central requirements is the timely reporting of cybersecurity incidents. The other is the disclosure of comprehensive cybersecurity programs.

The rules impact U.S. registered companies. As well as foreign private issuers registered with the SEC.

Reporting of Cybersecurity Incidents

The first rule is the disclosure of cybersecurity incidents deemed to be "material." Companies disclose these on a new item 1.05 of Form 8-K.

Companies have a time limit for disclosure. This is within four days of the determination that an incident is material. The company should disclose the nature, scope, and timing of the impact. It also must include the material impact of the breach. One exception to the rule is where disclosure poses a national safety or security risk.

Disclosure of Cybersecurity Protocols

This rule requires extra information that companies must report. They report this on their annual Form 10-K filing.

The extra information companies must disclose includes:

- Their processes for assessing, identifying, and managing material risks from cyber-security threats.
- Risks from cyber threats that have or are likely to materially affect the company.
- The board of directors' oversight of cybersecurity risks.
- Management's role and expertise in assessing and managing cybersecurity threats.

POTENTIAL IMPACT ON YOUR BUSINESS

Here are some of the potential areas of impact on businesses from these new SEC rules.

1. Increased Compliance Burden – Businesses will now face an increased compliance burden as they work to align their cybersecurity policies with the new SEC requirements.

2. Focus on Incident Response – The new regulations underscore the importance of incident response plans. Businesses will need to invest in robust protocols. These are protocols to detect, respond to, and recover from cybersecurity incidents promptly. This includes having clear procedures for notifying regulatory authorities, customers, and stakeholders.

3. Heightened Emphasis on Vendor Management – Companies often rely on thirdparty vendors for various services. The SEC's new rules emphasize the need for businesses to assess vendor practices. Meaning, how vendors handle cybersecurity. This shift in focus necessitates a comprehensive review.

4. Impact on Investor Confidence – Cybersecurity breaches can erode investor confidence and damage a company's reputation. With the SEC's spotlight on cybersecurity, investors are likely to take note. This includes scrutinizing businesses' security measures more closely. Companies with robust cybersecurity programs may instill greater confidence among investors.

5. Innovation in Cybersecurity Technologies – As businesses strive to meet the new SEC requirements, they will seek innovation. There is bound to be a surge in the demand for advanced cybersecurity solutions. This increased demand could foster a wave of innovation in the cybersecurity sector.

What is your Disaster Recovery Plan?

Data backups are crucial in any network environment, but not all backups are equal. Flawed backup systems, software, and procedures are common. For instance, we often encounter servers backed up to external drives that remain on-site indefinitely.

By partnering with Virtual DataWorks, you gain access to the necessary resources to ensure uninterrupted business continuity. We offer secure data access on-site, in transit, and in the cloud, providing you with peace of mind.

DATA LOSS HAPPENS. EVEN IN THE CLOUD.

Can your organization afford the risk of losing critical emails, contacts, calendars, and work documents? Our solution provides peace of mind by ensuring all your Microsoft 365 and Google Workspace data is securely backed up, easily recoverable, and thoroughly protected against loss or compromise.

Ransomware

Ransomware is an unfortunate reality that many organizations face. If your Microsoft 365 or Google Workspace data is ever encrypted, our solution allows you to quickly restore pre-infected data to a new domain, getting you back up and running in a matter of minutes.

Keep Tabs on Your Data

We provide a comprehensive backup overview, including a seamless navigation dashboard for your organization's data.

Data Loss

With Virtual DataWorks, Your data is securely backed up in our cloud with AirGap technology, ensuring it is always available. The inability to delete data, coupled with unlimited storage and retention, guarantees your Microsoft 365 and Google Workspace data will never be lost.

Prevent Data Disasters

User errors, flawed data migrations, and other issues can wreak havoc on your Microsoft 365 and Google Workspace information. Our s

Never Experience Downtime

Cloud-to-cloud backup for Microsoft 365 and Google Workspace ensures your vital data is protected and easily recoverable. This efficient system allows for quick restoration of emails, contacts, and calendars, maintaining your data's integrity and your business's operations.

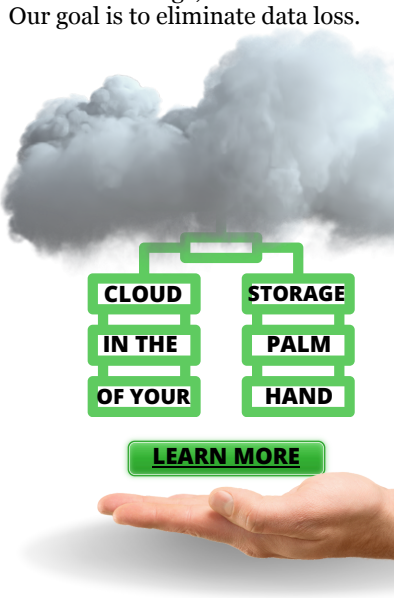
Standardizing on Microsoft 365 or Google Workspace may give the impression that your data is secure in the cloud, but is it truly?

Over 30% of small businesses have shifted from on-premise Exchange servers to Microsoft 365, with Google Workspace adoption also on the rise. Yet, there's much they may not know about these cloud services.

- 'Microsoft doesn't ensure against data loss and only keeps deleted data for 14 days.
- Google doesn't promise to prevent data loss, holding deleted data for only 20-25 days. Google Vault, while optional, excludes Calendar, Contacts, Sites, and Shared Drives data.

Microsoft notes that account compromises are a frequent security issue.

Their limited data retention may breach industry compliance and cause business disruptions. Third-party backups are essential for robust disaster recovery, ensuring data availability with AirGap, unlimited storage, and retention. Our goal is to eliminate data loss.



BEWARE OF THESE 2024 EMERGING TECHNOLOGY THREATS

The global cost of a data breach last year was USD $4.45 million. This is an increase of 15% over three years. As we step into 2024, it's crucial to be aware of emerging technology threats. Ones that could potentially disrupt and harm your business.

Data Poisoning Attacks

Data poisoning involves corrupting datasets used to train AI models. Businesses should use AI-generated data cautiously. It should be heavily augmented by human intelligence and data from other sources.

5G Network Vulnerabilities

The widespread adoption of 5G technology introduces new attack surfaces. IoT devices, reliant on 5G, might become targets for cyberattacks.

Quantum Computing Vulnerabilities

Quantum computing poses a threat. Its immense processing capabilities could crack currently secure encryption methods.

Artificial Intelligence (AI) Manipulation

AI, while transformative, can be manipulated. Cybercriminals can exploit AI algorithms to spread misinformation. Vigilance is essential as AI-driven threats become more sophisticated. It demands robust detection mechanisms to discern genuine from malicious AI-generated content.

Ransomware Evolves

Ransomware attacks have evolved beyond simple data encryption. Threat actors now steal sensitive data before encrypting files.

Biometric Data Vulnerability

Biometric authentication methods, such as fingerprints or facial recognition, are becoming commonplace. But users can't change biometric data once compromised. Protect biometric data through secure encryption.

READ MORE

TECHNOLOGY TRENDS CHANGING THE WAY WE WORK

Technology is reshaping the world of work at an unprecedented pace. From artificial intelligence to web3, from the metaverse to the hybrid work model. We are witnessing a series of technological revolutions. They are transforming how we communicate, collaborate, create, and innovate.

Let's explore some of the most impactful technology trends that are changing the way we work in 2024 and beyond.

1. Artificial Intelligence
2. Remote Collaboration Tools
3. Hybrid Work Model
4. Web3: The Decentralized Internet
5. Internet of Things (IoT) in the Workplace
6. Augmented Reality (AR) and Virtual Reality (VR)
7. Cybersecurity Advancements

These transformative technology trends are not just fleeting novelties. They are shaping the future of work.

14 HELPFUL TIPS FOR DIGITAL DECLUTTERING

These days, it's easy to feel overwhelmed at the sight of an endless inbox or app library.

It's the perfect time for a digital declutter. A clean and organized digital environment can help you improve your productivity. It also reduces stress. Here are some practical tips to help you declutter your digital space.

- Start with a digital inventory
- Focus on your most-used digital spaces
- Organize your files and folders
- Clean up your email inbox
- Clean up your social media
- Review your subscriptions
- Review and delete unused apps
- Clear your desktop and downloads folder
- Secure your digital identity
- Evaluate your digital habits
- Create digital detox days
- Streamline notifications
- Invest in digital tools
- Practice regular maintenance

READ MORE

11 WAYS TO RESPONSIBLY GET RID OF E-WASTE AT YOUR HOME OR OFFICE

In our tech-driven world, electronic devices have become indispensable. But with constant upgrades, what happens to the old gadgets? They tend to pile up and eat up storage space. But you can't just throw them in the trash. E-waste poses a significant environmental threat if not disposed of responsibly.

E-waste can contain hazardous materials. Such as lead, mercury, cadmium, and brominated flame retardants. These can harm the environment and human health.

Here are some tips to responsibly get rid of e-waste at your home or office:

- Understand what makes up e-waste
- Reduce your e-waste
- Explore retailer recycling programs
- Use e-waste recycling centers
- Consider donating or selling functioning devices
- Dispose of batteries separately
- Try manufacturer take-back programs
- Opt for certified e-waste recyclers
- Educate your office or household
- Repurpose or upcycle
- Encourage manufacturer responsibility

TALK TO AN IT EXPERT TODAY

BOOK A CONSULTATION

REQUEST A QUOTE