Cirrus IT Services

TECH TALK

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

INSIDE THIS ISSUE:

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

- **Scott Magee**
Managing Director

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.

Cirrus IT Services is now an Official OPNsense Reseller!

We're proud to announce that we are now an official reseller of OPNsense firewall hardware & licenses.

OPNsense produce cutting-edge firewalls to keep your business protected & secure. Read more here: cirrusits.co.uk/opnsense-firewalls

HOW CAN YOU LEVERAGE THE NEW MS TEAMS PAYMENT APP?

There is now another option to streamline the payment process. Microsoft has launched the Teams Payments app. This is a new feature that allows you to request and receive payments from your customers. You do it within Microsoft Teams meetings.

The Teams Payments app is currently available in the United States and Canada. Subscribers to Teams Essentials and Microsoft 365 Business get it at no charge.

How Does the Teams Payment App Work?

You can get the app from the Microsoft AppStore. You add it to your Teams account and connect it to your preferred payment service. You can choose from:

- Stripe
- PayPal
- GoDaddy

How Do You Send a Payment Request?

To send a payment request, you just need to open the meeting chat. Then, select the Payments icon from the messaging extensions. Then, you can fill out a simple form. It includes the amount, currency, description, and recipients of your request.

Your customers will see the same card in their meeting chat. They can click on the Pay Now button to complete their payment. You will receive a notification that your payment has been processed.

BENEFITS OF USING THE TEAMS PAYMENT APP

It saves time and hassle.

You don't need to switch between different apps or websites. You can do everything within Teams meetings.

It increases customer satisfaction and loyalty.

Your customers will appreciate the ease of paying you through Teams meetings.

It boosts your revenue and cash flow.

You can get paid faster and more securely by using the Teams Payments app. You don't need to wait for invoices or checks to clear. You can receive your money within minutes of completing a service. Either directly into your bank account or PayPal account.

It enhances your professional image and credibility.

You can show your customers that you are using a reliable and trusted payment platform. You can also add a seller policy to your payment requests.

It helps you keep track of payments.

With the Teams Payments App, you can track transactions in real-time. You'll receive instant notifications for successful payments.

It's seamlessly integrated with Microsoft 365.

The Teams Payments App seamlessly integrates with Microsoft 365.

It increases productivity.

Efficiency is the key to productivity. You reduce the time spent on payment-related tasks by integrating Payments into Teams.

The Teams Payments app marks a significant leap in digital business transactions. By leveraging this powerful tool, you're simplifying payments.

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.

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 NEW YEAR DIGITAL DECLUTTERING

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

As the new year begins, 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

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

TECHNOLOGY TRIVIA TIME

Each month you have a chance to win an Amazon Gift Card! Our December competition winner (randomly selected from correct entries) was:

Tania Walton of Southerns Solicitors!

Congratulations, Tania!

The question this month is:

What year was the first iPhone released?

To enter the competition, please go to this link and enteryour answer by 15th January 2024:

cirrusits.co.uk/tech-trivia