

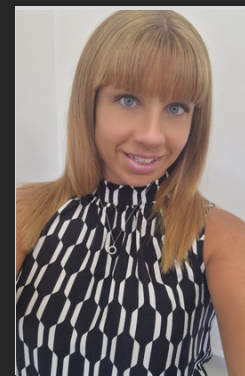


# TECH TALK

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

## INSIDE THIS ISSUE:

The Updated NIST 2.0 Cybersecurity Framework	Page 1	A Culture of Cyber Awareness	Page 2
#ESPDuck - Missy's Summer Travels	Page 1	Tech Tip of the Month	Page 2
Is Your Business Losing Money?	Page 2	Continuous Monitoring is a Cybersecurity Must	Page 2
Microsoft Copilot for Finance	Page 2	ESP Projects Meet the Team	Page 2



Summer is on the horizon and holidays are approaching. Wouldn't it be good to know your IT is in good hands while your away!! Nows a good time to make those changes to your business and update your IT! **Give me a call today 0330 2020 101 for a quick chat to find out more.**  
**Donna Aplin**  
Marketing Manager

## A SIMPLE GUIDE TO THE UPDATED NIST 2.0 CYBERSECURITY FRAMEWORK

Staying ahead of threats is a challenge for organisations of all sizes. Reported global security incidents grew between February and March of 2024. They increased by 69.8%. It's important to use a structured approach to cybersecurity. This helps to protect your organisation.

The National Institute of Standards and Technology (NIST) created a Cybersecurity Framework (CSF). It provides an industry-agnostic approach to security. It's designed to help companies manage and reduce their cybersecurity risks. The framework was recently updated in 2024 to NIST CSF 2.0.

CSF 2.0 is a comprehensive update that builds upon the success of its predecessor. It offers a more streamlined and flexible approach to cybersecurity. This guide aims to simplify the framework.

### Understanding the Core of NIST CSF 2.0

At the heart of CSF 2.0 is the Core. The Core consists of five concurrent and continuous Functions. These are: Identify, Protect, Detect, Respond, and Recover. These Functions provide a high-level strategic view of cybersecurity risk. This allows for a dynamic approach to addressing threats.

Here are the five Core Functions of NIST CSF 2.0.

- Identify** – This function involves identifying and understanding the organisation's assets, cyber risks, and vulnerabilities.
- Protect** – The protect function focuses on implementing safeguards. These protections are to deter, detect, and mitigate cybersecurity risks.
- Detect** – Early detection of cybersecurity incidents is critical for minimising damage. The detect function emphasizes the importance of detection.
- Respond** – The respond function outlines the steps to take in the event of a cybersecurity incident.
- Recover** – The recover function focuses on restoring normal operations after a cybersecurity incident.

### Profiles and Tiers: Tailoring the Framework

The updated framework introduces the concept of Profiles and Tiers. These help organisations tailor their cybersecurity practices. They can customise them to their specific needs, risk tolerances, and resources.

**PROFILES** – Profiles are the alignment of the Functions, Categories, and Subcategories. They're aligned with the business requirements, risk tolerance, and resources of the organisation.

**TIERS** – Tiers provide context on how an organisation views cybersecurity risk as well as the processes in place to manage that risk. They range from Partial (Tier 1) to Adaptive (Tier 4).

### Benefits of Using NIST CSF 2.0

- Improved Cybersecurity Posture:** By following the guidance in NIST CSF 2.0, organisations can develop a more comprehensive and effective cybersecurity program.
- Reduced Risk of Cyberattacks:** The framework helps organisations identify and mitigate cybersecurity risks.
- Enhanced Compliance:** NIST aligned CSF 2.0 with many industry standards and regulations.

- Improved Communication:** The framework provides a common language for communicating about cybersecurity risks.
- Cost Savings:** NIST CSF 2.0 can help organisations save money. It does this by preventing cyberattacks

### Getting Started with NIST CSF 2.0

- Familiarise yourself with the framework
- Assess your current cybersecurity posture
- Develop a cybersecurity plan
- Seek professional help

By following these steps, you can begin to deploy NIST CSF 2.0 in your organisation. At the same time, you'll be improving your cybersecurity posture.



### Missy #ESPDuck is out visting the world this summer...

Look out for your Missy Duck Summer Package coming through the post in the next few weeks... This is your chance to enter our summer competition and win a £50 Amazon Voucher. Simply take Missy and your goodies on Holiday post a picture having fun in the Sun to our Socials tagging #ESPDuck... Lets see what you come up with!!

# IS YOUR BUSINESS LOSING MONEY BECAUSE EMPLOYEES CAN'T USE TECH?

Shiny new tech can be exciting! It promises increased efficiency, happier employees, and a competitive edge. But that promise can turn into a financial nightmare if you neglect employee training and change management.

- Lost Productivity
- Costly Errors
- Demotivation and Resistance

### Failing to Manage the Change

New technology disrupts workflows. Without proper change management, employees feel overwhelmed and insecure. The goal is to help them transition successfully with proper training and support.

When companies neglect change management, the following can happen:

- Low Morale
- Use of Shadow IT
- Resistance to Future Improvements

### Building a Bridge to Success

So, what is the key to unlocking true value of new technology? It lies in effective training and change management.

Here's how to avoid the negative costs and get the full benefits from your tech.

- **Invest in Comprehensive Training** - Don't treat training as an afterthought. Yes, some tools say they're easy to use. But people have different tech literacy levels. Develop a tailored training program that goes beyond basic features. Include video tutorials, hands-on workshops, and ongoing support resources.
- **Focus on User Adoption, Not Just Features** - Training shouldn't just explain how the software works. It should focus on how the new system will benefit employees in their daily tasks and improve workflow efficiency. If employees don't adopt the new solution, the project fails.

- **Embrace Change Management** - Communicate the "why" behind the change. Explain how the new technology will make everyone's jobs easier. Encourage open communication and address concerns throughout the transition.

### THE TAKEAWAY

New technology is a powerful tool, but it's only as valuable as its users. Prioritise employee training and change management. This will help you bridge the gap between a shiny new system and a real return on investment.

Happy, well-trained employees using the right tools are your secret weapon. They can help you maximise efficiency, boost morale, and stay ahead of the curve.

When employees have trouble using their business tools, productivity drops. Mistakes can be made, and customer service can fall.

### Lack of Technology Training

Imagine investing in a top-of-the-line CRM system. Then you see your sales team floundering instead of excelling. They can't find key features, struggle with data entry, and miss deadlines. Why? Because they haven't been properly trained on the new software. It leads to the following costs:

## HOT OFF THE DIGITAL PRESSES... LEARN ABOUT MICROSOFT COPILOT FOR FINANCE

Microsoft Copilot has been heading up the business AI charge. This genAI-powered app is showing up in various function-related activities. The latest is finance processes.

- Outlook
- Excel
- Microsoft Teams
- Other Microsoft 365 applications

### Benefits of Using Copilot for Finance

Copilot for finance offers several benefits to those in financial roles. These include:

- Breaking Free from the Manual Grind
- AI-Powered Insights at Your Fingertips
- Tailored for Your Team
- Seamless Integration for a Frictionless Experience
- Built with Trust in Mind

### A Glimpse into the Future of Finance

Copilot for Finance represents a significant leap forward in financial technology. It's more than just automation. It's about harnessing the power of AI to augment human expertise. As well as transform the way finance operates.

Microsoft Copilot for Finance is a game-changer. It injects the power of next-generation AI into the heart of your everyday workflow. Imagine having an AI companion that understands the intricacies of finance and collaborates seamlessly with you.

It can help a seasoned financial analyst or a curious learner. It automates repetitive tasks and provides real-time insights. Copilot is poised to revolutionize how we navigate the fiscal realm.

### WHAT IS MICROSOFT COPILOT FOR FINANCE?

Copilot for Finance is a new Copilot experience in Microsoft 365. It connects to business financial systems. Such as Dynamics 365 and SAP. It provides finance-based insights and guided actions in:

## 10 EASY STEPS TO BUILDING A CULTURE OF CYBER AWARENESS

Cyberattacks are a constant threat in today's digital world. Phishing emails, malware downloads, and data breaches. They can cripple businesses and devastate personal lives.

Building a cyber awareness culture doesn't require complex strategies or expensive training programs. Here are some simple steps you can take to make a big difference.

1. Start with leadership buy-in
2. Make security awareness fun, not fearful
3. Speak their language
4. Keep it short and sweet
5. Conduct phishing drills
6. Make reporting easy and encouraged
7. Security champions: empower your employees
8. Beyond work: security spills over
9. Celebrate successes
10. Leverage technology

## IPHONE RUNNING SLOW? SPEED IT UP WITH ONE OF THESE TIPS

Let's face it, iPhones are amazing devices. But even the sleekest, most powerful iPhone can succumb to the dreaded slowdown. Apps take forever to load and scrolling feels sluggish. Pretty soon, simple tasks become frustrating ordeals.

If your iPhone has gone from speedy sidekick to sluggish snail, don't despair!

Here are some easy tips to get your iPhone back in tip-top shape:

- Give it a restart: The digital power nap
- Clean out the digital clutter
- Tame background app refresh
- Turn off location services where you can
- Reduce motion effects
- Update your apps and iOS
- Nuclear option: Reset your iPhone (Back up first!)
- Check your battery health

## WHY CONTINUOUS MONITORING IS A CYBERSECURITY MUST

Cyber threats are constantly evolving, and traditional security measures are no longer enough. Continuous monitoring acts as your vigilant digital guard. It's constantly checking for weaknesses. It sounds the alarm before attackers exploit them.

Here's why continuous monitoring is a cybersecurity must:

- Breaches Happen Fast
- Advanced Threats Need Advanced Defenses
- Compliance Requirements Often Mandate It

- Peace of Mind and Reduced Costs
- Improved Threat Detection Accuracy
- Faster Incident Response
- Enhanced Security Posture
- Compliance Reporting

In today's threat landscape, continuous monitoring is not a luxury. It's a security necessity.

Don't wait for a security breach to be your wake-up call. Embrace continuous monitoring and take control of your cybersecurity posture. An ounce of prevention is worth a pound of cure, especially in the digital world.

## Meet the Team...Introducing James Greaves Support Manager at ESP Projects



James is our Support Manager here at ESP Projects and has been here for the last 17 years.

James helps look after our team of Support Engineers keeping the team in check, ensuring that all the work is done and all tickets are in hand. He also helps our customers have working systems and high levels of support.