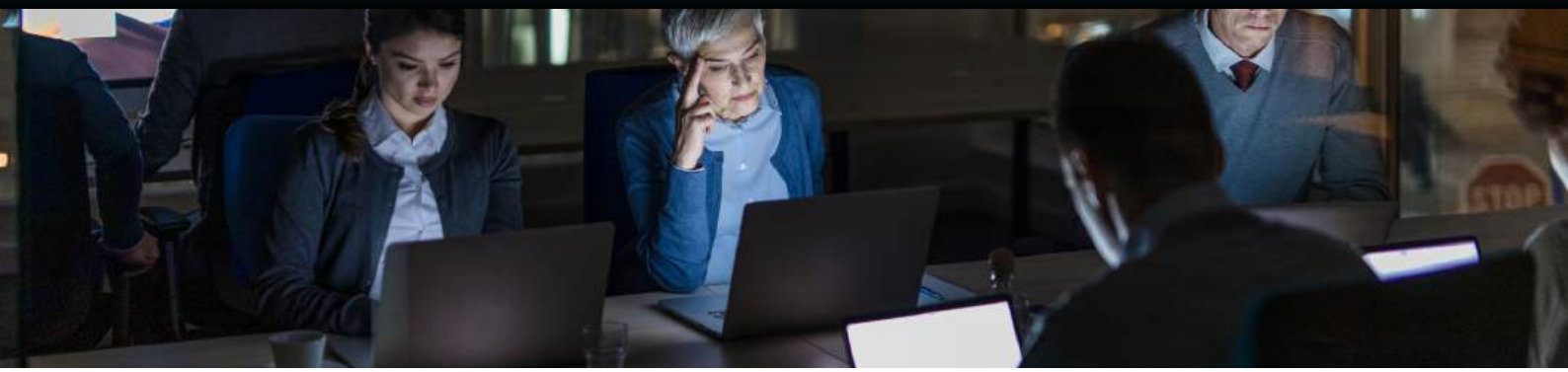
SEPT / OCT 2024

BITS & BYTES



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

INSIDE THIS ISSUE:

Why Securing Your Software Supply Chain is Critical — Page 1
Your IT Shortlisted for Top Awards — Page 1
Could an Email Signature be a Hidden Threat to your Business? — Page 2
Meet the Team — Page 2
6 Tips to Troubleshoot Common Business Network Issues — Page 2
Common Mobile Malware Traps — Page 2
8 Strategies for Tackling 'Technical Debt' at Your Company — Page 2
Announcing Our Partnership with EE — Page 2

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!

- **Lee Hewson**
Founder and MD

WHY SECURING YOUR SOFTWARE SUPPLY CHAIN IS CRITICAL

In today's world, everything's connected. That includes the software your business relies on, whether you've installed that software locally or use it in the cloud.

Protecting the entire process that creates and delivers your software is very important. From the tools developers use to the way updates reach your computer, every step matters. A breach or vulnerability in any part of this chain can have severe consequences.

A recent example is the global IT outage that happened last July. This outage brought down airlines, banks, and many other businesses. The culprit for the outage was an update gone wrong. This update came from a software supplier called CrowdStrike. It turns out that the company was a link in a LOT of software supply chains.

What can you do to avoid a similar supply chain-related issue? Let's talk about why securing your software supply chain is absolutely essential.

Increasing Complexity and Interdependence

• **Many Components**
These include open-source libraries, third-party APIs, and cloud services. Each component introduces potential vulnerabilities.

• **Interconnected Systems**
A vulnerability in one part of the supply chain can affect many systems. The interdependence means that a single weak link can cause widespread issues.

• **Continuous Integration and Deployment.**
Securing the CI/ CD pipeline is crucial to prevent the introduction of malicious code.

Rise of Cyber Threats

• **Targeted Attacks**
Attackers infiltrate trusted software to gain access to wider networks.

• **Sophisticated Techniques**
These include advanced malware, zero-day exploits, and social engineering. A robust security posture is necessary to defend against these threats.

• **Financial and Reputational Damage**
Companies may face regulatory fines, legal costs, and loss of customer trust. Recovering from a breach can be a lengthy and expensive process.

Regulatory Requirements

• **Compliance Standards**
These include regulations like GDPR, HIPAA, and the Cybersecurity Maturity Model Certification (CMMC).

• **Vendor Risk Management**
Companies must ensure that their suppliers adhere to security best practices. A secure supply chain involves verifying that all partners meet compliance standards.

• **Data Protection**
Securing the supply chain helps protect sensitive data from unauthorised access. This is especially important for industries like finance and healthcare.

Ensuring Business Continuity

• **Preventing Disruptions**
A secure supply chain helps prevent disruptions in business operations as cyber-attacks can lead to downtime.

• **Maintaining Trust**
By securing the supply chain, companies can maintain the trust of their stakeholders.

Steps to Secure Your Software Supply Chain

• **Strong Authentication**
Use strong authentication methods for all components of the supply chain. Ensure that only authorised personnel can access critical systems and data.

• **Phased Update Rollouts.**
Keep all software components up to date, but don't do all systems at once. If those systems aren't negatively affected, then roll out the update more widely.

• **Security Audits**
Assess the security measures of all vendors and partners. Identify and address any weaknesses or gaps in security practices.

• **Secure Development Practices**
Ensure that security is integrated into the development lifecycle from the start.

• **Threat Monitoring**
Use tools like intrusion detection systems (IDS) as well as security information and event management (SIEM) systems.

• **Education**
Awareness and training help ensure that everyone understands their role in maintaining security.

A breach or outage can have severe consequences. Securing your software supply chain is no longer optional; investing in this is crucial for the resilience of any business.

Your IT Shortlisted for Top Awards

Following our success of being ranked number 1 in the Midlands in the prestigious MSP 501 Awards for 2024, we have been shortlisted for a number of other Awards.

The Signature Awards take place at the end of September in London, and we have been shortlisted for the Excellence in Customer Service Award, we've also been named a finalist for the same category at the Chamber Awards, and for Employer of the Year at the Midlands Business Masters. We have our fingers crossed!!

BITS & BYTES

COULD AN EMAIL SIGNATURE BE A HIDDEN THREAT TO YOUR BUSINESS?

You're wrapping up a meeting when your phone buzzes with a new email. It's from a key supplier and looks urgent.

The message is short, direct, and ends with the familiar email signature you've seen countless times.

Without hesitation, you act on the request, but hours later, you discover that the email wasn't from your supplier at all.

The signature that convinced you it was legitimate was a clever forgery.

Now you're dealing with the fallout of a security breach that could have been avoided.

This isn't a far-fetched scenario. It's happening more often than you might think.

Email signatures, those blocks of text at the end of every professional email, are being weaponised by cyber criminals.

While you've (hopefully) invested in securing your networks and training your team, the security of your email signature might be the last thing on your mind.

But ignoring this small detail can open the door to big risks.

An email signature is more than just a formal way to sign off. It's a digital fingerprint of your business identity.

It contains crucial information such as your name, job title, contact details, and often your business's logo and links.

For your clients and colleagues, it's a mark of authenticity.

But for cyber criminals, it's a treasure trove of information that can be exploited to deceive and defraud.

What makes email signatures particularly vulnerable is their consistency and familiarity.

The more frequently someone sees your signature, the more they associate it with legitimacy.

Cyber criminals take advantage of this by creating emails that appear to come from you or your trusted contacts, complete with a forged signature that looks almost identical to the real thing.

The reality is that many businesses overlook the security of their email signatures.

They're often seen as an afterthought, something that's nice to have but not critical to protect.

This can be dangerous. Without proper security measures, your email signature can easily be spoofed, making your business – and your clients – vulnerable to attacks.

Understanding the risks is the first step toward protecting your business.

For instance, if your email signature includes links, those links can be manipulated to direct recipients to malicious websites.

Your title and contact details can be used to create highly authentic looking emails.

To safeguard your business, rethink how you approach email signatures.

Start by standardising the format across your company. When everyone's signature looks the same, it's easier to spot anomalies that could indicate a security threat.

Make sure that the links in your signatures are regularly verified to point to secure, legitimate websites.

And, while it might be tempting to include lots of information in your signature, remember that the more data you provide, the more opportunities you're giving cyber criminals to exploit it.

MEET THE TEAM
FERN RITCHIE
SECURITY & COMPLIANCE TEAM LEADER

When Fern joined us as an Apprentice back in 2019 I don't think any of us could have predicted just how quickly she would progress and how pivotal she would become to Your IT.

Having completed her Level 3 Infrastructure Technician Apprenticeship in 2022 she started to specialise in cyber security, completing her CompTIA Security+. She soon became the first member of our inhouse Cyber Team.

The team has grown and Fern has been named Team Leader as well as our Senior Security & Compliance engineer.

She's even found the time to work on an Applied Cyber Security Degree!

Fern recently appeared on Notts Today on Notts TV, talking cyber security protection for individuals and businesses.

Ferns three top tips? Long complex passwords, that you do not reuse. Turn on Multi-Factor Authentication wherever it is available and finally, take real care what you click on.

If you are unsure call the person who's emailed you, or ask your IT support provider. We'd rather confirm something is legitimate than have to help you recover if it's not!

TOP 6 SMART OFFICE TRENDS FOR AN IMPROVED WORKFLOW

Gone are the days of sterile cubicles and monotonous routines. Today's smart offices are hubs of innovation. They're designed to empower employees, optimise workflows, and foster collaboration.

This shift is driven by technology, including smart features that seamlessly integrate into the physical workspace. But with so many options available, where do you begin?

Here are the top six smart office trends you should consider adopting.

They can power productivity and boost employee satisfaction.

- Internet of Things (IoT) Devices
- Artificial Intelligence (AI) and Machine Learning
- Collaborative Technologies
- Remote Work Solutions
- Smart Furniture
- Data Analytics

COMMON MOBILE MALWARE TRAPS

Mobile malware is often overlooked. People focus on securing their laptops or desktops without paying close attention to smartphone and tablet security. Mobile malware can arrive in various forms, from sneaky apps to deceptive links. Ignorance is not bliss here. Understanding the common traps is your first line of defense.

- **Phishing Attacks**

Clicking links or downloading attachments can lead to malware infection.

- **Malicious Apps**

Always research apps before downloading.

- **SMS Scams**

Be wary of unexpected messages, especially those asking for sensitive info.

- **Public Wi-Fi networks**

Avoid accessing sensitive information on public Wi-Fi.

- **Fake Apps**

Always verify app authenticity

- **Adware**

Less harmful but can be annoying and can expose you to other threats.

8 STRATEGIES FOR TACKLING "TECHNICAL DEBT" AT YOUR COMPANY

Think of technical debt as the interest you pay on a loan you never intended to take.

As your system grows, those hasty decisions can cost you in the long run.

Here's how to address it:

- **Identify and Prioritise.** Focus on the most critical issues that will drive the most value first.
- **Integrate Debt Management into Your Workflow.** Maintain a balance between new development and debt reduction.
- **Educate and Train Your Team.** Foster a culture of quality thinking.
- **Improve Documentation.** It provides a reference for current and future team members.
- **Regularly Update and Refactor Systems.** This involves making small, manageable changes for quality.
- **Optimise Security Practices.** Helps maintain system reliability and performance.
- **Manage Dependencies.** Tracking ensures compatibility and security.
- **Foster a Culture of Continuous Improvement.** Encourage learning, celebrating successes, and regular reflection to drive ongoing enhancement.