

OCTOBER 2024



TALKING TECH

HELPING YOUR BUSINESS



FROM DAMIEN'S DESK:

Well footy season is now officially over. I hope your team won the Grand Final, mine certainly did not. I am a long-term suffering Saints supporter, and we have not seen success in the Grand Final since 1966, when we won against Collingwood.

Football can be like business, there are successes and there are failures. Some things work, whilst some things are problematic. Computer software you would expect to run as described each and every time you open it. We all know that is not the case, much like our football team. Each time they take the field we are looking for them to go out there and win.

However, the team may not be operating at their peak performance, much like your computer systems. Unfortunately, in business that can cost money, by losing productivity.



Are your computer systems running at their peak? It is time to evaluate if your equipment is past its used by date. A new machine may not only allow the processing of work quicker but also energise the user by them receiving some new kit. Remember support for Windows 10 runs out this time next year. Act now, don't leave it to the last minute.

If we can help, please reach out.

Damien "Time for new hardware" Pepper



DID YOU KNOW?

Benjamin Franklin was the first to propose daylight savings time in 1784.

WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to your business friends.

Referrals help us keep costs down so we can pass on the savings to all our clients.

Simply introduce me via email damien@dspit.com.au or (03) 9001 0817 and I'll take it from there.



dSP IT Solutions
 182C Sladen Street
 Cranbourne VIC 3977
 (03) 9001 0817
sales@dspit.com.au
www.dspit.com.au

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 wide-spread 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.

• Compliance Standards

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

• 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.

• 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.

Did you know your email signature could be a security weak point?



90%

of people use a single email signature for business.



Your email signature could be a goldmine of info for cyber criminals.

They typically include a combination of:



Your name & Job title



Phone Number



Email Address



Website



Social Media Accounts

- Cyber criminals can use this information to pretend to be you.
- Then trick other people into handing over sensitive info. Or money.
- Spoofing email signatures is a common tactic used to scam businesses.
- You and your team could be tricked in the same way.

Stay protected by:

1

Including only basic info

2

Creating a standard signature for everyone

3

Teaching your team the risks

4

Implementing encryption

5

Monitoring for suspicious activity

dsp IT
SOLUTIONS

6 TIPS TO TROUBLESHOOT COMMON BUSINESS NETWORK ISSUES

Get started on keeping your network up and running smoothly:

1. Identify the Problem

Narrow down potential causes.

2. Inspect Physical Connections

Quickly rule out or identify simple problems.

3. Test Network Connectivity

Simple testing can provide valuable insights.

4. Analyse Network Configuration

Errors here can often cause connectivity problems.

5. Monitor Network Performance

This helps identify ongoing issues and potential bottlenecks.

6. Ensure Security and Updates

Regular updates and checks can prevent many common issues.



**Delivering better.
Better telecommunications.
Better service.**

**VoIP Services
Business NBN
Business Mobile Phones
SIP**

Need help with your business telecommunications or internet?

(03) 9008 6900
sales@dspcommunications.com.au
www.dspcommunications.com.au

NEED A LAUGH?

What is the latest in Pirate technology?



The I-patch!

WIN A \$25 WISH GIFT CARD

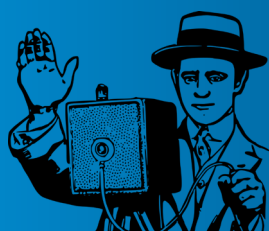
There was no winner from last month's trivia question. The answer was a) Eliza.



You could be the winner of this month's trivia question. Just contact us with the answer to the question below, no googling and good luck!

The world's first photograph required an exposure time of . . .

- a) 8 hours
- b) 16 hours
- c) 24 hours
- d) Several days



Call us with your answer
(03) 9001 0817 or email
jo@dspit.com.au