JUNE 2024

dSP IT SOLUTIONS

# TALKING TECH

## HELPING YOUR BUSINESS

## FROM DAMIEN'S DESK:

Last month, I recorded our tech update on Password managers. What does your organisation do for managing passwords? I guess you have a little black book with important passwords noted there. I bet some employees use the same password repeatedly, the same one on each website or application.

Using a password manager allows you to store all your usernames and passwords securely so you don't have to remember them. You just need to remember one, the master password. A password manager also provides a random password generator so that you no longer have to think of a password for yourself.

I highly encourage you to implement password managers across your organisation. If you need help, please let me know.

Check out our YouTube channel for all sorts of tips and tricks - www.youtube.com/@dsp-it

And . . . Here comes 30th June, a closure to another financial year. I hope yours has been successful.

Stay safe

Damien Pepper - Director
dSP IT Solutions

## DID YOU KNOW?

The first-ever computer virus to spread via email, the "Morris Worm," infected thousands of computers in 1988.

dSP IT SOLUTIONS

CYBERSECURITY ESSENTIALS FOR BUSINESS OWNERS

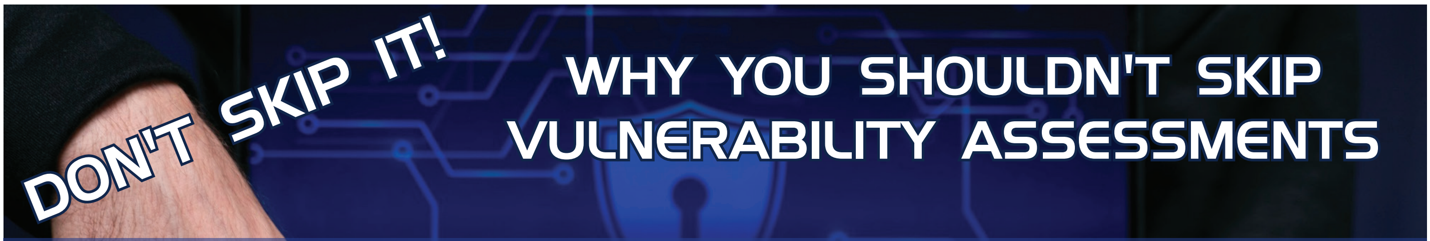
FREE!

OWN IT. SECURE IT. PROTECT IT.

For your FREE copy of this book, go to:
https://www.dspit.com.au/cybersecurity-essentials/

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

#SuperResponsive #WeMakeTheComplexSimple #BuildRelationships #NothingIsTooHard



# WHY YOU SHOULDN'T SKIP VULNERABILITY ASSESSMENTS

Cyber threats are a perpetual reality for business owners. Hackers are constantly innovating. They devise new ways to exploit vulnerabilities in computer systems and networks.

For businesses of all sizes, a proactive approach to cybersecurity is essential. One of the most crucial elements of this approach is regular vulnerability assessments. A vulnerability assessment is a systematic process. It identifies and prioritises weaknesses in your IT infrastructure that attackers can exploit.

Some businesses may be tempted to forego vulnerability assessments. They might think it's too costly or inconvenient. Small business leaders may also feel it's just for the "big companies." But vulnerability assessments are for everyone. No matter the company size. The risks associated with skipping them can be costly.

## Why Vulnerability Assessments Matter

The internet has become a minefield for businesses. Cybercriminals are constantly on the lookout for vulnerabilities to exploit. Once they do, they typically aim for one or more of the following:

- Gain unauthorised access to sensitive data
- Deploy ransomware attacks
- Disrupt critical operations

Here's why vulnerability assessments are crucial in this ever-evolving threat landscape:

- *Unseen Weaknesses:* Many vulnerabilities remain hidden within complex IT environments.
- *Evolving Threats:* Experts discover new vulnerabilities all the time. Regular assessments ensure your systems are up to date.
- *Compliance Requirements:* many industries have regulations mandating regular vulnerability assessments.
- *Proactive Approach vs. Reactive Response:* Identifying vulnerabilities proactively allows for timely remediation. This significantly reduces the risk of a costly security breach. A reactive approach is where you only address security issues after an attack.

## The High Cost of Skipping Vulnerability Assessments

- *Data Breaches:* Unidentified vulnerabilities leave your systems exposed.
- *Financial Losses:* Data breaches can lead to hefty fines and legal repercussions as well as the cost of data recovery and remediation.
- *Reputational Damage:* A security breach can severely damage your company's reputation. It can erode customer trust and potentially impact future business prospects.
- *Loss of Competitive Advantage:* Cyberattacks can cripple your ability to innovate and compete effectively. This can hinder your long-term growth aspirations.

## The Benefits of Regular Vulnerability Assessments

- *Improved Security Posture:* Vulnerability assessments identify and address vulnerabilities.
- *Enhanced Compliance:* Regular assessments help you stay compliant with relevant industry regulations.
- *Peace of Mind:* Knowing your network is secure from vulnerabilities gives you peace of mind.
- *Reduced Risk of Costly Breaches:* Proactive vulnerability management helps prevent costly data breaches.
- *Improved Decision-Making:* Vulnerability assessments provide valuable insights into your security posture.

## Investing in Security is Investing in Your Future

Vulnerability assessments are not a one-time fix. Your business should conduct them regularly to maintain a robust cybersecurity posture.

By proactively identifying and addressing vulnerabilities, you can:

- Significantly reduce your risk of cyberattacks
- Protect sensitive data
- Ensure business continuity

*Remember, cybersecurity is an ongoing process.*

# Recovering from a cyber attack

Many business owners believe that cyber criminals only target big businesses. In fact, cyber criminals assume smaller businesses are easier to crack thanks to lax security.

**46%** of breaches impact businesses with fewer than 1,000 employees.

**37%** of companies hit by ransomware had fewer than 100 employees.

Small businesses receive the highest rate of targeted malicious emails:

**1 in 323**

21

The average cyber attack disrupts businesses for around 21 days.

Companies with frequent downtime have 16 times higher costs than other businesses.

**Only 14%**

of small and medium sized businesses have a cyber security plan in place.

## DSP IT SOLUTIONS

## GUIDE TO IMPROVING YOUR COMPANY'S DATA MANAGEMENT

Data is the lifeblood of modern businesses. It fuels insights, drives decision-making, and ultimately shapes your company's success. But in today's information age, data can quickly become overwhelming.

*Here are some strategies for effective data management:*

- **Conduct a data inventory**
  Identify all the data your company collects, stores, and uses. Understand the purpose of each data set and how the organisation is using it.

- **Invest in data management tools**
  Technology can be your ally in data management. Explore data management solutions.

- **Develop data policies and procedures**
  Document your data management policies and procedures.

- **Foster a data-driven culture**
  Encourage a data-driven culture within your organisation. Emphasize the importance of data quality and responsible data usage.

- **Embrace continuous improvement**
  Data management is an ongoing process. Regularly review your data management practices.

## NEED A LAUGH?

What do you call a computer superhero?

A Screensaver!

## WIN A $25 WISH GIFT CARD

There was no winner from last month's trivia question.
The answer was d) 908kgs.

You could be the winner of this month's trivia question. Just contact us with the answer to the question below, good luck!

What is the percentage of Australian's using the internet regularly?

a) 86.5%
b) 93%
c) 81.5%
d) 89%

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