APRIL 2023

dSP IT SOLUTIONS

TALKING TECH

HELPING YOUR BUSINESS

FROM DAMIEN'S DESK:

Exciting! Not many sleeps left until the easter bunny comes to visit. I am sure there will be plenty of chocolate to go around. Hopefully you get some time to relax during the easter break.

At DSP we have been working on a large project for one of our customers providing around 30 access points into their new location, coupled with integration to their AV system and providing a solid internet connection.
These types of projects are something that my team love to work on and they get satisfaction seeing the building being constructed and then ultimately connected to new equipment and technology.
This type of work allows us to demonstrate our true technical skills and goes beyond any one person, it takes the team to get this off the ground. If you have a future project that you would like to discuss please reach out.

This segways perfectly into my news, I would like to welcome David and Christian to our team of technicians. They will both be helping us to support your technology. Welcome to the team guys!

Finally, a thought to finish on. Over Easter you may take holidays but the hackers won't. We are here for you, why don't you book a 10min call with me to discuss your security protection.

You can book a time here:
https://calendly.com/dsp-damien/10-minutecall

Stay safe out there

Damien Pepper - Managing Director
dSP IT Solutions

DID YOU KNOW?

The largest chocolate easter egg was over 10 metres tall!

WE LOVE REFERRALS

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

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

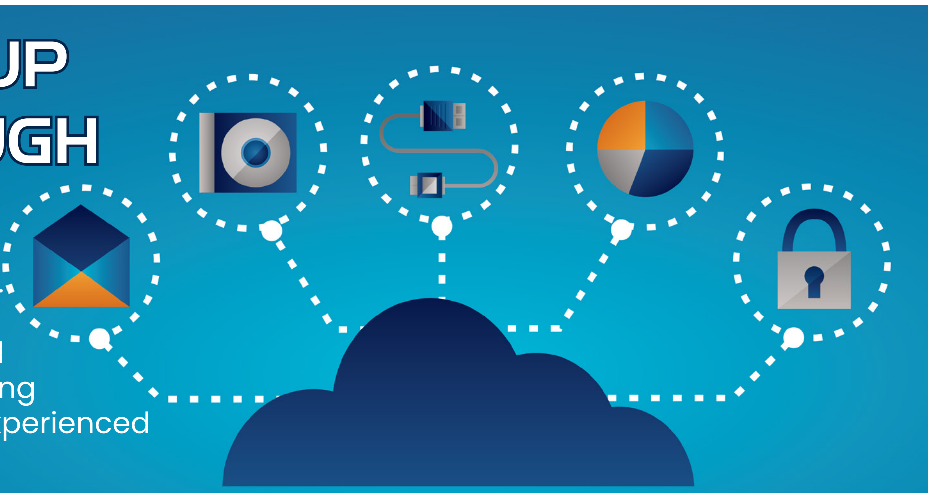
Simply introduce me via email damien@dspit.com.au or (03) 9001 0817.

I promise my team and I will take good care of them, just like we do with all our customers!

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

#SuperResponsive #WeMakeTheComplexSimple #BuildRelationships #NothingIsTooHard

DATA BACKUP IS NOT ENOUGH



The need to back up data has been around since floppy disks. Data loss happens due to viruses, hard drive crashes, and other mishaps. Most people using any type of technology have experienced data loss at least once.

Every five years, 20% of Server Message Blocks (SMBs) suffer data loss due to a major disaster. This has helped to drive a robust cloud backup market that continues to grow.

But one thing that's changed with data backup in the last few years is security. Simply backing up data so you don't lose it, isn't enough anymore. Backing up has morphed into data protection.

What does this mean?

It means that backups need more cybersecurity protection. They face threats such as sleeper ransomware and supply chain attacks. Cloud-based backup has the benefit of being convenient, accessible, and effective. But there is also a need for certain security considerations with an online service.

Companies need to consider data protection when planning a backup and recovery strategy. The tools used need to protect against the growing number of threats.

Some of the modern threats to data backups include:

Data Center Outage:

The "cloud" basically means data on a server. That server is internet accessible. Those servers can crash. Data centres holding the servers can also have outages.

Sleeper Ransomware:

This type of ransomware stays silent after infecting a device. The goal is to have it infect all backups. Then, when it's activated, the victim doesn't have a clean backup to restore.

Supply Chain Attacks:

Supply chain attacks have been growing. They include attacks on cloud vendors that companies use. Those vendors suffer a cyberattack that then spreads throughout their clients.

Misconfiguration:

Misconfiguration of security settings can be a problem. It can allow attackers to gain access to cloud storage. Those attackers can then download and delete files as they like.

What to Look for in a Data Protection Backup System

Just backing up data isn't enough. You need to make sure the application you use provides adequate data protection. Here are some of the things to look for when reviewing a backup solution.

Ransomware Prevention

Ransomware can spread throughout a network to infect any data that exists. This includes data on computers, servers, and mobile devices. It also includes data in cloud platforms syncing with those devices.

cont'd P3

cont'd from P2

It's important that any data backup solution you use have protection from ransomware. This type of feature restricts automated file changes that can happen to documents.

Continuous Data Protection

Continuous data protection is a feature that will back up files as users make changes. This differs from systems that back up on a schedule, such as once per day.
Continuous data protection ensures that the system captures the latest file changes. This mitigates data loss that can occur if a system crashes before the next backup. With the speed of data generation these days, losing a day's worth of data can be very costly.

Threat Identification

Data protection incorporates proactive measures to protect files. Threat identification is a type of malware and virus prevention tool. It looks for malware in new and existing backups. This helps stop sleeper ransomware and similar malware from infecting all backups.

Zero-Trust Tactics

Cybersecurity professionals around the world promote zero-trust security measures. This includes measures such as multi-factor authentication and application safe listing.

THINK TWICE BEFORE USING SELF-PORTRAIT APPS

It's a common theme. You begin seeing these amazing CGI images of your friends on Facebook or Instagram.

You think, "How can I make one?"

You upload about 10 photos to the app, so it can feed that data into its AI algorithm. Then, once it maps your facial features, it generates several fantasy profile pics.
It sounds like a little harmless digital fun, right?

That's what many companies making apps like this like you to think.
Vanity is an easy sell.

But for several self-portrait apps, you're paying more than you know.
The cost comes from the data privacy rights you're giving up.
And these can go far beyond the app itself.

Why Worry About Data Privacy with these Apps?

Data Used to Track You
Once you download the app, it can track your phone activity in other apps.

Data Collected
By downloading the app, you permit it to track all kinds of data, including the purchases you make online.

Loss of Rights to Your Uploaded Images
Some of these apps require you to grant a sub-licensable license to use, reproduce, modify, distribute, and create derivative works of your user content.

Get a Device Privacy Checkup
The more apps you use, the more complicated data privacy can get. Don't leave it to chance.

6 STEPS TO EFFECTIVE VULNERABILITY MANAGEMENT FOR YOUR TECHNOLOGY

Technology vulnerabilities are an unfortunate side effect of innovation. When software companies push new updates, there are often weaknesses in the code. Hackers exploit these.

Software makers then address the vulnerabilities with a security patch. The cycle continues with each new software or hardware update.

61% of security vulnerabilities in corporate networks are over 5 years old.

- Step 1: Identify Your Assets
- Step 2: Perform a Vulnerability Assessment
- Step 3: Prioritise Vulnerabilities by Threat Level
- Step 4: Remediate Vulnerabilities
- Step 5: Document Activities
- Step 6: Schedule Your Next Vulnerability Assessment Scan

WINDOWS 8.1 JUST LOST ALL SUPPORT HERE'S WHAT YOU NEED TO KNOW

The latest operating system to lose all support is Windows 8.1.
Microsoft released the OS in 2013, and it was officially retired on January 10, 2023. Microsoft issued the following warning for companies:
“Continuing to use Windows 8.1 after January 10, 2023 may increase an organisation’s exposure to security risks or impact its ability to meet compliance obligations.”

Here are a few facts you should know:
- The OS Will Still Technically Work
- Your System Will No Longer Receive Security Patches
- Options for Upgrading are Windows 10 or 11

What Happens if you don’t upgrade?
- Security & Compliance Issues
- Slowed Productivity
- Incompatibility With Newer Tools

NEED A LAUGH?

What did the computer have during its break time?

A byte!

WIN A $20 BUNNINGS GIFT CARD!

BUNNINGS warehouse

There was no winner from last month’s trivia question.
The answer was a) Mechanical computer.

We are now offering a $20 Bunnings Gift Card and you could be this month’s winner!
Just contact us with the answer to the question below, Good Luck!

Which of these public domain name sales was the most expensive?

a) Internet.com
b) Carinsurance.com
c) LasVegas.com
d) Porn.com

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