FROM DAMIEN'S DESK:

It's February. In most cases holidays are over and the kids are back at school. People are starting to get back into the groove at work and it won't be long before people start to think they didn't even have a holiday.

DID YOU KNOW?

Valentine's Day was first declared a holiday by a pope in 496 A.D.

Prior to Christmas you will have seen in the media the information relating to the Optus hack. What is interesting with this particular hack is that the bad guys didn't lock the company out of their files like traditional Ransomware. They just stole the data and asked Optus to pay a ransom to stop the bad guys releasing the data to the dark web.

Whilst none of this is new, it does raise a great question. Why did Optus have data on customers that had left some years prior? It was identified that there was data taken from Optus that had significantly aged and the customer was no longer current.

Maybe this is something you need to consider for your organisation. Are you storing data that you no longer need? My recommendation is that you create a policy with strict processes in place that provide guidance to your staff about aging data. Some organisations will have a mandated timeline that they need to keep data for, that may be 7 years or it may be longer. Other organisations may need to be able to access data for a lifetime.
What is your requirement?

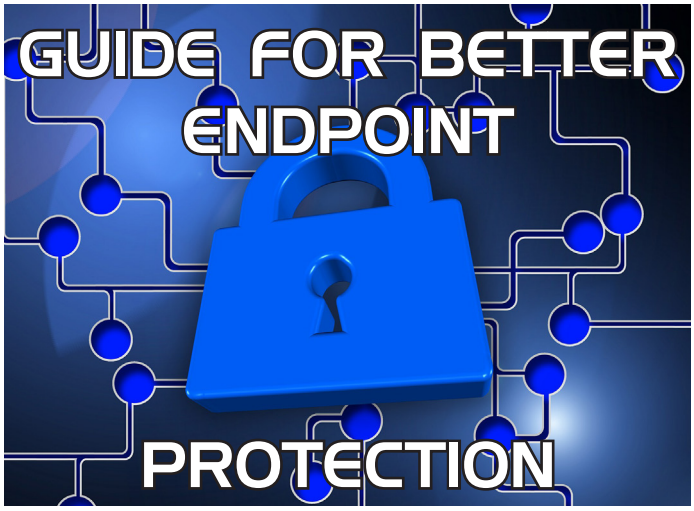
Once you know if you have a mandated requirement for keeping data then implement a process to keep within the mandated period. Do not keep data for the sake of keeping data. With any really old data you would have to question whether it is at all still valid.

Stay safe out there.

Damien Pepper - Managing Director
dSP IT Solutions

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

#SuperResponsive #WeMakeTheComplexSimple #BuildRelationships #NothingIsTooHard



Endpoints are the collection of computers, mobile devices, servers, and smart gadgets that make up your company's network and IT infrastructure.

Each of those devices is a chance for a hacker to penetrate a company's defences.

Many organisations have experienced one or more compromising endpoint attacks.

The following solutions are focused on the protection of endpoint devices:

Address Password Vulnerabilities

Passwords are one of the biggest vulnerabilities when it comes to endpoints.

Poor password security and breaches make credential theft one of the biggest dangers to cybersecurity.

Address password vulnerabilities in your endpoints by:

- Training employees on proper password creation and handling
- Look for password-less solutions, like biometrics
- Install multi-factor authentication (MFA) on all accounts

Stop Malware Infection Before OS Boot

USB drives (also known as flash drives) are a popular giveaway item at trade shows.

But an innocent-looking USB can actually cause a breach.

Hackers can use them to gain access to a computer is to boot it from a USB device containing malicious code.

There are certain precautions you can take to prevent this from happening.

One of these is ensuring you're using firmware protection that covers two areas: Trusted Platform Module (TPM) and Unified Extensible Firmware Interface (UEFI) Security.

TPM is resistant to physical tampering and tampering via malware.

It looks at whether the boot process is occurring properly and also monitors for the presence of anomalous behaviour.

Additionally, seek devices and security solutions that allow you to disable USB boots.

Update All Endpoint Security Solutions

You should regularly update your endpoint security solutions. It's best to automate software updates if possible so they aren't left to chance.

Firmware updates are often forgotten about. But they are just as important for ensuring your devices remain secure and protected.

Use Modern Device & User Authentication

How are you authenticating users to access your network, business apps, and data?

If you are using only a username and password, then your company is at high risk of a breach.

cont'd P3

cont'd from P2

Use two modern methods for authentication:
· Contextual authentication
· Zero Trust approach (Trust but Verify)

Apply Security Policies Throughout the Device Lifecycle

From the time a device is first purchased to the time retires, you need to have security protocols in place.

Examples of device lifecycle security include when a device is first issued to a user. This is when you should remove unnecessary privileges.

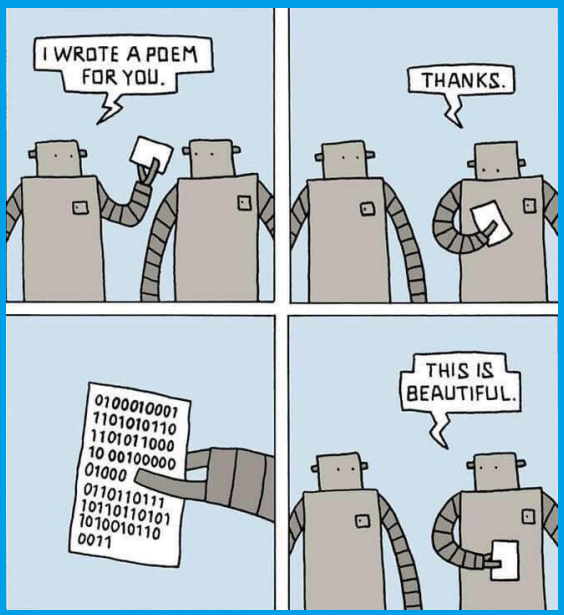
When a device moves from one user to another, it needs to be properly cleaned of old data and reconfigured for the new user.

When you retire a device, it should be properly scrubbed.

Prepare for Device Loss or Theft

Unfortunately, mobile devices and laptops get lost or stolen. When that happens, you should have a sequence of events that can take place immediately. This prevents company risk of data and exposed business accounts.

FEBRUARY FUNNY!



TRENDS IN DATA PRIVACY THAT MAY IMPACT YOUR COMPLIANCE

Data privacy has been a growing requirement ever since the internet age began. So much personal information is flying around through computer networks. Protecting it has become a mandate. By the end of 2024, 75% of the world's population will have their personal data protected. It will fall under one or more privacy regulations. Privacy requirements hit all sized companies.

AI Governance

AI is running many of the algorithms responsible for keeping data protected. But what happens when there is a problem with the AI? This is the question that AI governance is working to address.

Consumer Privacy UX

A trend that we've seen over the last several months is putting more privacy power into the consumer's hands. Consumer privacy portals tell people what data is being collected, how it is collected, and what is done with it.

Increased Scrutiny of Remote Employee Monitoring

Monitoring remote employees opens a can of worms when it comes to data privacy. Organisations need to ensure that they aren't encroaching on the rights of their staff.

Data Localisation

Increasingly, organisations look at where their cloud data is being stored because the location governs the privacy rules and regulations that it may fall under.

Privacy-Enhancing Computation (PEC)

Data privacy by design is a fairly new term. Using privacy-enhancing computation is a way that AI is helping cyber-security.

By using PEC as a built-in component of software and apps, developers provide value to clients. They address privacy concerns by making data protection more automated.

Laptops today boast ridiculously powerful batteries, a far-cry from the roughly 2-3 hours we used to get. Most laptops nowadays can easily provide up to 12 hours of battery life.

So, if you're laptop battery doesn't seem to get you past a few hours of use, try the following tips:

- Lower the Display Brightness
- Reduce PC Battery Use in Power/ Sleep Settings
- Enable Battery-Saver Mode
- Use the Manufacturer's Battery Calibration Tool
- Use Microsoft Edge Browser on PC or Safari on Apple for their Efficiency Settings
- Turn Off Unnecessary Apps
- Don't install updates unplugged
- Don't Expose Your Laptop to Extreme Temperatures

Portable projectors are no longer a thing of science fiction or a concept of a distant future. The Nebula Capsule 3 is around the size of your average tall canned beverage and can project an image with stunning 1080p resolution.

With its 52Wh battery, you can watch movies for up to 2.5hours on a single charge (or plug in for longer use). And, with a fully-fledged Android 11.0 OS you have all ofyour favourite streaming services loaded right on the device!

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

NEED A LAUGH?

Computers are like air conditioners; they stop working when you open Windows.

WIN A $30 AMAZON GIFT CARD!

The winner of last month's trivia question was Tony from Unique Building Services. The answer was b) Russia 2018.

You could be the winner of this month's trivia, just contact us with the answer to the question below, Good Luck!

QR codes were invented in 1994 as a way to track what?

a) Packages behind the scenes at UPS
b) Vehicles as they were assembled
c) As an alternative to website URLs
d) To initiate phone calls

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