TALKING TECH

HELPING YOUR BUSINESS

FROM DAMIEN'S DESK:

Merry Christmas! The year end is nigh. I hope you are able to take a well-earned break and spend time with your family. Some people will travel for family holidays and some will have to work. However you decide to spend the Christmas break, I hope you enjoy the festive season.

Here at DSP IT, we love giving back to our community. This quarter we went with the most appropriate theme for this time of year; Christmas presents for children who benefit from the efforts of Backpacks 4 Vic Kids. https://www.backpacks4vickids.org.au (See the picture of donations collected)

As promised, we have created a checklist outlining the most important things you should make sure you have ticked off before you head off on the festive holiday.
You can download the check list by going to:
https://www.dspit.com.au/christmas-closure-checklist/
I hope you find it useful, even if it jogs your memory for one thing that you hadn't thought about.

Please remember that the bad guys don't take a break and we will continue to see cyber events over the holiday season. Don't let your guard down after having one too many egg nogs, continue to be vigilant at checking the links in the emails you receive, or responding to the dodgy looking TXT messages. Without a doubt we will see more scams, phishing attempts and phoney TXT messages in the new year, this is going to get worse and the holiday season is perfect timing for the hackers to try to suck you in whilst your guard is down.

If you need something to read over the holiday period, why not grab a copy of a book I have put together called **“CYBERSECURITY ESSENTIALS FOR BUSINESS OWNERS”** to which I am happy to send over a copy to you for **FREE,** no obligation, no hard sell, just plain old **FREE**. To get your hands on a copy please go to https://www.dspit.com.au/cybersecurity-essentials/

Merry Christmas, stay safe and enjoy family time

Damien Pepper - Managing Director
dSP IT Solutions

DID YOU KNOW?

The total number of gifts given in the carol, ‘The Twelve Days of Christmas’ is 364.

Christmas gift donations for a local charity

dSP IT Solutions
182C Sladen Street
Cranbourne VIC 3977

WHAT TO INCLUDE IN A YEAR-END TECHNOLOGY INFRASTRUCTURE REVIEW

When the year is coming to a close, it's the perfect time to plan for the future. Most businesses begin the year with the hope of growing and improving operations. Much of how a business operates depends on technology.

So, it makes sense to look to your IT for areas of optimisation.

A year-end technology review provides an opportunity to look at several areas of your IT. The goal is to take time to focus on improvements you can make to boost your bottom line. As well as what tactics to take to reduce the risk of a costly cyberattack.

Small businesses that make smart use of technology are well ahead of their peers.

Here are some of the ways they excel:

- Earn 2x more revenue per employee
- Experience year-over-year revenue growth nearly 4x as high
- Had an average employee growth rate over 6x as high

The bottom line is that companies that use technology well, do better. They are also more secure.
According to IBM, businesses that have an incident response plan reduce the costs of a data breach by 61%. Using security AI and automation can lower costs by 70%.

This year-end, take some time to do a technology review with your IT team or managed IT provider.

This will set you up for success and security in the coming year.

The goal of a year-end technology review is to look at all areas of your IT infrastructure. Security, efficiency, and bottom-line considerations will be the keydrivers for future initiatives.

Technology Policies

When technology policies get outdated, people stop following them. Review all your policies to see if any of them need updating to reflect new conditions. For example, if you now have some staff working from home, make sure your device use policy reflects this.

When you update policies, let your employees know. This gives them a refresher on important information. They may have forgotten certain things since onboarding.

Disaster Recovery Planning

When is the last time your company did an incident response drill? Is there a list of steps for employees to follow in the case of a natural disaster or cyberattack?

Take time to look at disaster recovery planning for the new year. You should also put dates in place for preparedness drills and training in the coming months.

IT Issues & Pain Points

You don't want to go through a big IT upgrade without considering employee pain points. Otherwise, you might miss some golden opportunities to improve staff productivity and wellbeing.

cont'd P3

cont'd from P2

Survey your employees on how they use technology. Ask questions about their favorite and least favorite apps. Ask what struggles they face.

Let them tell you how they feel improved technology would make their jobs better. This, in turn, benefits your business. It can also help you target the most impactful improvements.

Privileged Access & Orphaned Accounts

Do an audit of your privileged accounts as part of your year-end review. Over time, permissions can be misappropriated. This leaves your network at a higher risk of a major attack.

You should ensure that only those that need them have admin-level permissions. The fewer privileged accounts you have in your business tools, the lower your risk.

Compromised privileged accounts password open the door to major damage.

APPS TO IMPROVE CUSTOMER EXPERIENCE

In today's world, people can order something on their phones and see it on their doorstep the next day.

Keeping up with expectations means leveraging the right technology.

As 2023 is on the horizon, it's the perfect time to improve your customer experience. Thanks to cloud technology, you don't have to spend a fortune to do it. Just put in place some of the applications below.

These apps focus on making leads and customers happy:

· Online Survey Application
· Smart Chat Bot
· Business Mobile App
· Facebook Messenger Support
· VoIP Phone System with Good Mobile App
· Text Notification Apps
· All-in-One CRM & Sales Platform

ADVANTAGES OF CONDITIONAL ACCESS

It seems that nearly as long as passwords have been around, they've been a major source of security concern.
Eighty-one percent of security incidents happen due to stolen or weak passwords. Additionally, employees continue to neglect the basics of good cyber hygiene.
Access and identity management have become a priority for many organisations.
Once a cybercriminal gets a hold of an employee's login, they can access the account and any data that it contains. Using conditional access policies can mitigate the risk of an account breach.

What Is Conditional Access?

Conditional access is also known as contextual access. It is a method of controlling user access.
You can think of it as several "if/then" statements, meaning "if" this thing is present, "then" do this.
Conditional access allows you to add many conditions to the process of user access to a system. It is typically used with MFA. This is to improve access security without unnecessarily inconveniencing users.

Some of the most common contextual factors used include:
· IP address · Geographic location · Time of day · The device used · Role or group the user belongs to

The Benefits of Implementing Conditional Access for Identity Management:

· Improves Security · Automates the Access Management Process · Allows Restriction of Certain Activities
· Improves the User Login Experience · Enforces the Rule of Least Privilege
· Get Help Implementing Conditional Access Today!

SIX MOBILE DEVICE ATTACKS YOU NEED TO WATCH OUT FOR

Smartphones and tablets are often the preferred device for communications, web searching, and accessing many types of apps. They're more portable and can be used from anywhere.

You need to be on the lookout for the most prevalent mobile device threats that allow your data to be leaked or breached. Here's a roundup of what those are.

- Mobile malware hidden in Apps
- Unprotected communications
- Public Wi-Fi & man-in-the-middle attacks
- Juice jacking on public USB charging stations
- Non-updated devices
- Text-based phishing (smishing)

SIX IMPORTANT IT POLICIES ANY SIZE ORGANISATION SHOULD IMPLEMENT

Many smaller businesses make the mistake of skipping policies. They feel that things don't need to be so formal. But this way of thinking causes issues for business owners.

Employees aren't mind readers. Things that you think are obvious, might not be to them. IT policies are an important part of your IT security and technology management.

Here are some of the most important to have in place:

1. Password Security Policy
2. Acceptable Use Policy
3. Cloud & App Use Policy
4. Bring Your Own Device Policy
5. Wi-Fi Use Policy
6. Social Media Use Policy

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 on to our clients.

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

NEED A LAUGH?

What do you get if you cross Santa with a duck?

A Christmas Quacker!

WIN A $30 AMAZON GIFT CARD!

The winner of last month's trivia question was Pauline from Grace Professional Services. The answer was d) 248 metres.

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

When was the first SMS text message sent?

a) December 1992
b) June 1984
c) September 1989
d) August 1998

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