FROM DAMIEN'S DESK:

How quickly has that come around? It seems that Christmas arrives much quicker nowadays. Most businesses will be starting to set up for their summer break. Yes, I know, not all businesses close down for Christmas! If you are one of the ones that does, I hope you and your team have a great break.

I was recently discussing cybersecurity with one of our vendors in the USA and the owner said he would like to come to Australia to run a cybersecurity conference in January. I politely laughed and said, I wouldn't if you want people to attend, in January the only thing business owners are thinking about is the summer holidays. So true in the Aussie way!

With the holiday period fast approaching please stay vigilant, you will see an uptick in Phishing emails and attempts to compromise your business. It is a known fact that hackers make the most of this time to try to catch you off guard or when you are not watching. Please make sure you have talked to your staff about what to look for in regard to fake emails. I would also suggest a checking procedure for being able to confirm bank transfers, that they are in fact going to the correct recipient. It is well noted that bank fraud continues to increase.

Of course, if you need some help or just want to check whether what you are doing is going to provide protection please reach out to us.

Wishing you a Merry Christmas & Stay safe out there

Damien Pepper - Director
dSP IT Solutions

DID YOU KNOW?

Coca-Cola played a big role in shaping the image of Santa.

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 our clients.

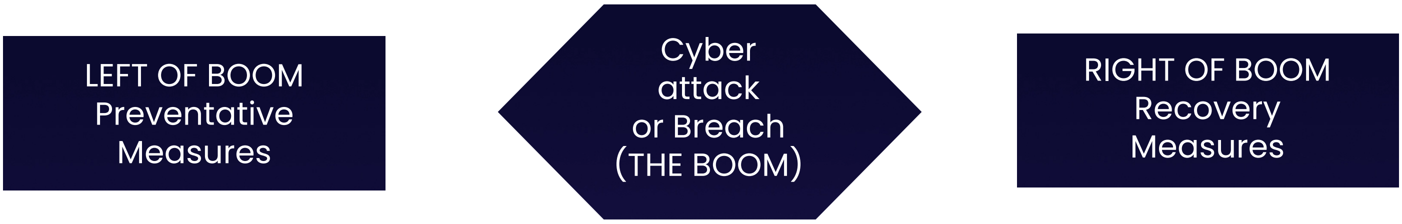
Simply introduce me via email shane@dspit.com.au or (03) 9001 0817 and I'll take it from there.

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

#SuperResponsive #WeMakeTheComplexSimple #BuildRelationships #NothingIsTooHard

HOW TO ORGANISE YOUR CYBERSECURITY STRATEGY INTO LEFT AND RIGHT OF BOOM

In the pulsating digital landscape, every click and keystroke echoes through cyberspace.The battle for data security rages on. Businesses stand as both guardians and targets. Unseen adversaries covet their digital assets. Businesses must arm themselves with a sophisticated arsenal of cybersecurity strategies. On one side, the vigilant guards of prevention (Left of Boom). On the other, the resilient bulwarks of recovery (Right of Boom). Together, these strategies form the linchpin of a comprehensive defence. They help ensure that businesses can repel attacks. And also rise stronger from the ashes if breached.


LEFT OF BOOM
Preventative
Measures

Cyber
attack
or Breach
(THE BOOM)

RIGHT OF BOOM
Recovery
Measures

What Do "Left of Boom" and "Right of Boom" Mean?

In the realm of cybersecurity, "Left of Boom" and "Right of Boom" are strategic terms. They delineate the proactive and reactive approaches to dealing with cyber threats.

"Left of Boom"

Refers to preemptive measures and preventative strategies. These are things implemented to safeguard against potential security breaches. It encompasses actions aimed at preventing cyber incidents before they occur.

"Right of Boom"

Pertains to the post-breach recovery strategies. Companies use these after a security incident has taken place. This phase involves activities like incident response planning and data backup.

Together, these terms form a comprehensive cybersecurity strategy. They cover both prevention and recovery aspects.

Left of Boom: Prevention Strategies

User Education and Awareness
One of the foundational elements of Left of Boom is employee cybersecurity education. Regular training sessions can empower staff.

Robust Access Control and Authentication
Access control tactics include:
- Least privilege access
- Multifactor authentication (MFA)
- Contextual access
- Single Sign-on (SSO) solutions

Regular Software Updates and Patch Management
Left of Boom strategies include ensuring all software is regularly updated.

Network Security and Firewalls
Firewalls act as the first line of defence against external threats. Install robust firewalls and intrusion detection/prevention systems.

Regular Security Audits and Vulnerability Assessments
Conduct regular security audits and vulnerability assessments. This helps to identify potential weaknesses in your systems.

cont'd P3

cont'd from P2

Right of Boom: Recovery Strategies

Incident Response Plan

Having a well-defined incident response plan in place is crucial.

It should include things like:

- Communication protocols
- Containment procedures
- Steps for recovery
- IT contact numbers

Data Backup and Disaster Recovery

Regularly backing up data is a vital component of Right of Boom. Another critical component is having a robust disaster recovery plan.

Forensic Analysis and Learning

After a security breach, conduct a thorough forensic analysis. It's essential to understand the nature of the attack. As well as the extent of the damage, and the vulnerabilities exploited.

Legal and Regulatory Compliance

Navigating the legal and regulatory landscape after a security breach is important.

9 SMART WAYS FOR SMALL BUSINESSES TO INCORPORATE GENERATIVE AI

There is no escaping the relentless march of AI. Software companies are rapidly incorporating it into many business tools.

Leveraging Generative AI, small businesses can unlock a world of possibilities. This includes everything from enhancing customer experiences to streamlining operations.

Here are some smart and practical ways to incorporate GenAI.

- Personalised Customer Experiences
- Presentations & Graphics Creation
- Chatbots for Customer Support
- Data Analysis and Insights
- Product Design and Prototyping
- Supply Chain Optimisation
- Dynamic Pricing Strategies
- Human Resources and Recruitment
- Predictive Maintenance

MOST SECURE WAY TO SHARE PASSWORDS WITH EMPLOYEES

Breached or stolen passwords are the bane of any organisation's cybersecurity. Passwords cause over 80% of data breaches. Hackers get in using stolen, weak, or reused (and easily breached) passwords.

But passwords are a part of life.

Since you can't get around passwords, how do you share them with employees safely? One solution that has gained popularity in recent years is using password managers.

Why Use a Business Password Management App?

Here are some of the reasons to consider getting a password manager for better data security:

· **Centralised Password Management**
A primary advantage of password managers is their ability to centralise password management. They keep employees from using weak, repetitive passwords. And from storing them in vulnerable places.

· **End-to-End Encryption**
Leading password managers use robust encryption techniques to protect sensitive data.

• **Secure Password Sharing Features**
Password managers often come with secure password-sharing features. They allow administrators to share passwords with team members. And to do this without revealing the actual password.

• **Password Generation and Complexity**
Password managers typically come with built-in password generators. They create strong, complex passwords that are difficult to crack.

· **Secure Sharing with Third Parties**
Password managers offer secure methods for sharing credentials with third-party collaborators or contractors.

NEED A LAUGH?

What is a Christmas tree's favourite candy?

Ornamints!

WIN A $20 BUNNINGS GIFT CARD!

The winner of last month's trivia question was Ann from Showtime Attractions. They had the correct answer, c) It might explode.

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

Which country started the tradition of putting up a Christmas tree?
a) England
b) Norway
c) Germany
d) Sweden

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