Once again, it's the time of year for reflection. Many thought COVID would disrupt things for only a year, so the persistent lockdowns throughout 2021 made it another tough one for organisations of all types.

In fact, McKinsey tells us that 3 out of 5 Australian employees are at least somewhat burned out (or worse) – and they say that number is likely underrepresented! So listen to the numbers and look for ways to address this problem. Particularly for the security or technology teams if they had to spend some part (all?) of the holidays looking for the 'Log4j' issue which 'set the internet on fire' with the 'design failure of catastrophic proportions' just a few weeks ago.

Log4j vulnerability: what should boards be asking?

Our friends in the UK often provide good insight for non-technical audiences. This is a pretty good list of the TOP 10 questions for Boards to ask about Log4j (or for IT people to be ready to answer them).

The Log4j issue is evolving fast, so it's VERY important to keep up to date HERE. At this link there are some simple, well-explained steps (and tools) provided that you can use to assess the issue in your organisation.

Consider it a TOP priority, because it's in response to "active, worldwide exploitation by numerous threat actors". The scale of the problem is also still unclear, for example "initial analysis suggests the threat to telco network core platforms is severe".

Also, it's not just important for your bespoke software systems or software, but it's also about the technology your organisation may be using. Here's the 'Affected Vendor & Software List' of 660 known technology vendors impacted by Log4j and they cover the alphabet from Amazon to Zscaler.

Finally, some sound advice comes from the 'SysAdmin, Audit Network and Security (SANS) Institute:

> **If you're patching … on an Internet facing service, you need to be doing an incident response too. The reality is that someone else almost certainly beat you to it. Patching doesn't remove the existing compromise. [Also,] if you scan for this vulnerability and discover your system is patched, make sure it was you who applied that patch. Criminals are known to patch systems they compromise to prevent others from doing the same.**

The Big Picture Outlook for Executives and Boards

This quarter we brought together seasoned Cyber Security experts from across key industries such as health, financial services, education, logistics, academia, information technology and consulting. They shared their insights during our Leadership Series on The Reboot Show, providing practical guidance on the journey to developing Cyber Maturity and achieving Cyber Resilience.

Our Leadership Series is available for you to watch now (no registration required) by clicking here or you can watch individual segments depending on which area of focus is most important to your organisation right now.

We kicked the Series off with a focus on our mantra that 'cyber is a LEADERSHIP challenge' – the fact is that technology alone, will not protect an organisation and it's the tone that is set at the top of any organisation that is the difference between the protected and the vulnerable.

> **Segment 1 - Embedding Cyber Security into Executive Agendas and Budgeting**
>
> Featuring the Chairman of AISA, Damien Manual, and the General Manager of Cyber Security and Technology Risk at IOOF Holdings Ltd, Ashutosh Kapse, alongside our Managing Director, Tom Crampton. Click here to watch

For our second piece, we wanted to emphasise the critical role of the organisation's staff. 95% of cybersecurity breaches are caused by human error. But it's not just about 'training' but using psychologically-oriented 'behaviour change' approaches that use techniques such as personality learning types, operant conditioning, and gamification. If you 'just had five dollars' to spend on cyber, you probably should be spending at least one of them on improving the resilience of your staff to social engineering techniques. Drop us a note (here) – we do a lot of that kind of work with our clients.

Segment 2 - Creating Sustained Employee Behaviour Change

Featuring the Head of Security Awareness and Enablement at Bupa Health, Jasmin Krapf, and the Director of Technology Innovation at St Leonard's College, Timothy Barlow, alongside our Research Analyst Charline Quarre. Click here to watch

Third, the world (finally) recognises that you simply cannot rely solely on 'protecting' yourself against a cyber incident. No one ever won a Grand Final (or more often, just a game) without having a clear plan, and practicing that plan so you know roles, responsibilities, etc. Once again, if you 'just had five dollars' to spend on cyber, you should probably be spending one of those on having a plan and simulating an incident so that you can respond and recover from 'the inevitable'. This is worth considering.

Segment 3 - Ensuring Your Organisation Can Recover From a Cyber Crisis

Featuring the Information Technology Manager at RightShip, Ian McKenzie, and the General Manager at Continuity Matters, Ben Scheltus, alongside our Principal Consultant Genio Maiolo. Click here to watch

Looking forward – what to include on your summer reading list

Looking forward, it's clear that organisations need to consider different 'models' to protect against tomorrow's cyber threats. One model that's gained momentum is the concept of "Zero Trust Architectures". McKinsey aptly noted this as one of the top 10 trends in technology (as a function of investment, news mentions, and patents granted).

There's a very good National Institute of Standards and Technology (NIST) paper HERE if you want to learn more. In fact, if you're cyber nerds like we are, it might be a good document to put on your summer reading list while sipping that pina colada at the pool or beach.

But bear in mind that it quietly notes that "Organizations need to implement comprehensive information security and resiliency practices for zero trust to be effective," and not many are at that stage yet. We can help you get you there if interested – just drop us a note.

Significant Salient Statistics…

Used sparingly and in the right context, statistics can often improve a conversation with executives. Here are 134 Cybersecurity Statistics and Trends for 2021!.

Tis the season to reflect on things that are important, and you're one of those things. We appreciate you taking the time to read our Quarterly Review and thanks for being part of our community. We hope your holiday season is safe and filled with family, friends and fun, and cheers to health, happiness, and prosperity in 2022!

If you're not already, please 'follow us' on LinkedIn and/or Twitter, and feel free to send this to others (or have them subscribe here).

Kind regards,

TrustedImpact
PROTECTING DIGITAL

we're **independent** consultants – it's about **your** business and **your** success
with a **singular focus** – cyber security is all we do
leveraging **experienced** professionals – credentials, not checklists