
Fourth quarter headlines have been filled with political upheaval – top of the list is the political comeback of Donald Trump in November. Martial law was (briefly) called in South Korea and their Prime Minister was just impeached because of it. Germany, France, the list goes on for this quarter. Ultimately nearly 80 countries representing about 4 billion people, this year witnessed a decline in support for the incumbent parties, showing widespread political dissatisfaction all around.

While politicians and parties will ebb and flow, one constant remains. That's Nation States' continuing to jockey for digital advantage, and 'bad actors' continuing to make too much money preying on our businesses and citizens. So, keep the faith and the focus as we all look forward to a more positive 2025!

## "*Australia faces the most complex and challenging strategic environment since the Second World War.*

*These strategic challenges extend to the cyber threat landscape. While advancements in critical and emerging technologies offer significant social and economic benefits, they also improve the capabilities of malicious cyber actors who continue to target Australia's networks.*"

The above was the first paragraph in the Executive Summary of the Annual Cyber Threat Report 2023-24 released a few weeks ago by the Australian Signals Directorate (ASD). Total calls to the ASD hotline were up 12%, and while the 'self-reported' cost of cybercrime was up for small business, it's pleasing to see it was down for medium and large businesses. Why? We suspect it may be related to medium and large organisations finally recognising that it's not a question of 'if, but when,' and hopefully it means they are more resilient than we saw a over decade ago. It's also about planning for the inevitable – as a client eloquently quoted "Under pressure, you don't rise to the occasion – you sink to the level of your training" (thanks Jonathan!).

Do you have a robust ability to 'respond and recover'? Have you trained for an incident? Is it enough? If not, consider running our unique approach for cyber incident response simulations. It captures measurable improvements so you can better respond when it's the real thing. Either way, keep 'training'!

Another valuable insight is that the top 3 'self-reported' cybercrimes for businesses were; email compromise (20%), online banking fraud (13%), and business email compromise fraud (13%). Protecting your organisation from email issues doesn't have to be hard – it involves employing the fundamentals (MFA for everything), organisational resolve to ensure your staff are resilient and aren't just told to 'not do things'. Therefore, consider using a 'psychological behaviour change' approach to your awareness programs – don't just phish them every once in a while, but complement that with a program that is focused on changing behaviour. What does that mean? Here are some ideas.

Finally, the Threat Report also provided some good 'mitigations' for the 'Reported Top 3' incident types depending on your type of organisation (or if you're an individual). They're worth looking at to make sure you have these covered. Finally, if you value having someone 'independent' test or validate that those mitigations working well for your organisation – it's what we do, so just drop us a note.

## Australia's first standalone cyber security law

We'd be remiss if we didn't highlight the importance of several key pieces of legislation that were just passed.

First was the "Cyber Security Act 2024". In short: Mandatory reporting if you make ransomware payments; Security Standards if you're involved with making Smart Devices; and a "Cyber Incident Review Board. Nearly every law firm published a perspective on the Act, so instead of regurgitating that here, head to Lexology if you want to tap into a wealth of detailed analyses.

So too, did The Privacy and Other Legislation Amendment Bill 2024 reach 'Royal Assent' a few days ago, introducing expanded powers for the Information Commissioner. Again, a plethora of information on Lexology if you're keen to learn more. It's nice to see our legislative frameworks (slowly) catching up to address current issues – albeit, there's still a long way to go!

## Ask your employees.

We all know that we your reuse passwords, right? That might be true for you, but you might want to send an email to your 'less password savvy' staff asking if they have EVER reused their 'Meta' passwords. Why? In October Ireland officials fined Meta $101 million for storing HUNDREDS OF MILLIONS of user passwords in plaintext and making them broadly available to company employees (and who knows who else?). With 5.5 Billion global internet users, you can be guaranteed that someone is testing to see if those passwords are still valid (for both your business and their personal accounts).

## "I can go broke trying to be secure!"

We felt the hairs on the back of our necks stand up when we read the headline of an article this quarter titled "57 Tips to Secure Your Organization". Don't get us wrong, the list isn't wrong or incorrect. But it epitomises one of the biggest problems for most organisations today. Although thorough, it's frankly not very helpful. Why? The CEO of one of our clients (in frustration) said the quote above, and he was spot on. Any 'lazy' cyber professional can easily give you LOTS of tips of what to do – just pick any contemporary framework: ISO, NIST, PCI-DSS, CIS, the list goes on and on, and anyone can give you a list of things you must all do to improve your cyber posture.

But where the value lies, is NOT in giving you an exhaustive list of all things that you can never reasonably digest, manage or even resolve in a reasonable period of time. Real value lies in assessing an organisations unique BUSINESS environment and rolling up one's sleeves to help define what PRACTICAL actions can be taken that reduces YOUR greatest risks with a practical perspective on the 'effort' of resolving those issues. Effort being defined not just to cost, but the scale of impact to the organisation and other key factors like complexity to resolve, etc. Then helping you define a realistic roadmap (integrated with your technology roadmap) to help improve your organisation's cyber maturity at a pace that makes sense for your organisation.

In parallel, it's also about resilience and recognising that whatever you do, a cyber incident will still happen. So, it's also about being prepared to respond well (and quickly), and to be able to recover to minimise the negative business impact. It's about priorities, progress and resilience – NOT lists of hundreds of controls or tips!

If you get exhaustive lists from people trying to help you with your Cyber challenges, just drop us a note. A value-added approach is the foundation of our Firm – it's about helping you practically mature your cyber posture and improving your resilience – not bloody lists you can't reasonably complete!

---

'Tis the season to reflect on things that are important. And to us, you're one of those! We appreciate you being connected with us. No matter how you celebrate the season, we hope you create some positive memories with friends and family, and may your New Year be full of peace, joy, prosperity and good health! 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