The fourth quarter review
December 2023

Welcome to the fourth quarter review! Our aim is, and always has been, to try to provide you with a unbiased, business perspective on the key cyber events shaping our world. Hopefully empowering you to make better informed decisions to improve your organisation's cyber posture.

Right as most of us were thinking of the holidays, St Vincents Health began responding to a cyber incident. Details are still scant, but you can be sure that many have spent countless hours trying to assess the damage. Here's to those 'defenders of digital' whose friends and families missed their presence over Christmas and likely New Years too!

November sets the tone for the next several years

A cascade of significant Federal Government and Regulatory reports were published in November. When taken together, it's clear these will set the tone for the industry next year and several to come.

On the 1st, the Cyber and Infrastructure Security Centre (CISC) released its first annual report on the security risks faced by our critical infrastructure sectors. There's not much really new or different in it (ie, foreign principal threats increasing in sophistication and the risk from trusted insiders), but it does highlight the increased level of scrutiny that critical infrastructure sectors should expect in the next few years. Particularly the 'less traditional' critical infrastructure industries such as health and food supply, where risk management processes have often been less mature in the past. A greater pace of improvement and level of risk rigour should be anticipated if you work in these industries.

Thanks to the Optus network outage, on the 13th it was announced by the Government that Aussie Telco's would be hit with new rules classifying them as critical infrastructure, and further flagged that mandatory ransomware reporting is on its way.

Ironically also on the 13th, ASIC released its "Cyber Pulse Survey 2023" which showed that over half (58%) of Australian businesses have limited, or no capability to protect confidential information adequately. 44 percent also do not manage third-party or supply chain risk, and one third do not have a cyber incident response plan!?

Then, on the 14th, the Australian Signals Directorate (ASD) published its 'Annual Cyber Threat Report 2022-23". In summary: the problem is BIG, getting BIGGER, affecting MORE Australian businesses and individuals on a MORE FREQUENT basis.

Finally on the 22nd, the Cyber Security Minister released the "2023 – 2030 Cyber Security Strategy". It defines six 'shields' that will deliver "a future where stronger cyber protections enable our citizens and businesses to prosper, and to bounce back quickly following a cyber attack".

What does all of that likely mean to you?

1) Growing intolerance - expect fines and court cases. FTI aptly noted in their 2024 predictions, that "Australia thus far largely managed to avoid significant fines despite inadequate proactive cybersecurity measures, but recent changes to legislation and associated fines will soon have Australia following suit with Europe and the United States". November's OAIC's court case against Australian Clinical Labs reinforces that view.

2) Possible 'individual' prosecution. There's a growing trend to prosecute individuals, like the SEC case against SolarWinds' Chief Information Security Officer for fraud and misleading investors, or the FTC case that found former Uber security chief guilty of concealing a data breach. While these examples are US-centric, more Australian executives will find themselves facing legal scrutiny for insufficient cybersecurity protection of their company and/or their clients.

Reflecting on the 'new' cyber strategy

When we reflect upon the previous two previous incarnations of the country's Cyber Security Strategies, one wonders at which point do we stop reiterating a 'strategy' and should we focus more attention on effective implementation and accountability?

We've had several sound National Strategies in the past few years, but as painfully illustrated in the previous section, the size, scale, and velocity of the 'cyber problem' is increasing.

The importance of effective 'implementation' rather than just creating a 'strategy' was suggested by one of our team to 'the then Prime Minister' when the previous Federal strategy was released… the reaction of disdain was deafening. Isn't it time we have an independent review to measure accountability for 'outputs' (or results) and not simply 'inputs' or activities? Perhaps also critically assessing what's working (and do more of it), and what is not working (and do less of it)?

Basic security hygiene protects against 99% of attacks!

It's worth highlighting this quarter's "Digital Defence Report 2023" from Microsoft. It's a big read at 131 pages. But the most powerful message was the simple fact that "Basic security hygiene still protects against 99% of attacks". And in particular, the study from Cornell University that found the use of Multi-Factor Authentication reduces the risk of compromise by 99.2%.

Why is basic hygiene still so poor? The ShadowServer Foundation found 20,000 publicly available MS Exchange Servers running software that's no longer supported. The SANS 'NewsBites" it's worth following – there's always great editorial notes like John Pescatore's apropos comment: if your company cafeteria still serves sandwiches using mayonnaise with a "Use before April 12th, 2007" warning, you should probably fire the cafeteria manager. The same is true for whoever made the decision to continue using Exchange Server 2007.

Prepare for the inevitable

Optus was in the headlines again this quarter. While the extended network outage apparently was not the result of a cyber attack, one lesson is clear: prepare for an incident (cyber or not) and practice how to respond and recover.

An organisation is like a sporting team – if you don't have a game plan, haven't discussed who's in what position, and never stepped onto a field to practice that game, you can be guaranteed to lose against a skilled and well drilled opponent. Consider our 'Trusted**Response**' platform for cyber incident response 'war gaming' - it's significantly more insightful and useful than the 'old school' approaches.

Significant Salient Statistics…

Each quarter we trip across a wealth of statistics. Used sparingly and in the right context, they can often improve a conversation with your executives and colleagues. This quarter:

- HALF of the digital forensics and incident response (DFIR) matters handled by Aon in 2022 related to social engineering and phishing – Awareness is important, but focus on behaviour change!

- Net Sales at Clorox dropped 28% due to a cyber attack that led to product shortages – if you struggle to get resources for your cyber program, what's 28% of your revenues?

_____

'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 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