This quarter was an active one with cyber incidents occurring in sectors ranging from airlines (Qantas - 6 million customers), health (NSW Health - 600 medical staff), telecommunications (iiNet / TPG - 200,000 customers) to education (Loyola College in Victoria, University of Western Australia). And unfortunately, Optus was back in the headlines with news that a firewall upgrade led to a 13 hour outage of emergency services. Clearly, 'RESILIENCE' should be the key word for this quarter!

A bellwether worth watching

The Australian Prudential Regulatory Authority (APRA) made a few positive strides this quarter. While we all know that APRA is focused primarily on our financial industry, APRA is also a good 'bellwether' to watch for sound cyber requirements. So even if you're not a financial institution, there's still a lot of valuable advice that you should be following.

For example, APRA contacted all superannuation board chairs reinforcing expectations around authentication controls following recent credential stuffing attacks. We've gone on and on about the importance of **using Multi-Factor Authentication** (high risk reduction, low cost/complexity to implement) for **EVERYTHING** that either; you access from the internet, or if you have any systems that are used by your customers, suppliers or partners for your organisation.

Also this quarter, APRA's cross-industry Prudential Standard (CPS) 230 went into force, requiring banks, insurers, and superannuation funds to meet higher standards of operational risk management. CPS 230's a bit broader than CPS 234, and requires APRA-regulated entities to be well-prepared to ensure continuity of critical services to the community and respond to business disruptions by:

- identifying important business services and determining the extent to which these services can continue during severe disruptions;
- testing their business continuity planning to identify vulnerabilities to ensure they are positioned to overcome severe disruptions; and
- enhancing third-party risk management by ensuring risks from material service providers are identified and appropriately managed.

Sound advice for not just our financial industry, but for all! Let us know if you want help getting there!

Simple change – big impact: Accountability!

In the above letter to Superannuation Chairs, was another important item worth highlighting. APRA was pushing for each organisation to designate their 'accountable person(s)' who would have the responsibilities related to CPS 234 compliance.

To be blunt, most employees do what they are measured against, so having someone accountable is a key step in the right direction. Simple question… do any (even better – ALL) of your 'Chief' executives have KPI's associated with cyber?

Once again – it's a pretty simple thing to do, which almost always results in significant improvement just by being clear on who has 'accountability'. While a 'designee' is a good step; from our experience with over 400 clients over the last 19 years. KPI's associated with cyber and resilience should be explicitly and consciously 'owned' by the entire C-Suite – not just a CIO or head of Technology.

So you can imagine our delight with the news from Qantas when they announced they had cut executive bonuses by 15% after the July cyber attack. We applaud the 'first' Chair (that we've noticed) who 'gets it' … John Mullen said

"Despite the strong [financial], the Board decided to reduce the annual bonuses by 15 percentage points as a result of the impact the cyber incident had on our customers. This reflects their shared accountability, while acknowledging the ongoing efforts to support customers and put in place additional protections for customers."

Lessons the European Airline hack

As we write this, Europe is still recovering from a cyberattack relating to a third party of check-in and boarding systems. Third-party risk is tricky and common / best-of-breed solutions can often result in multi-site outages.

But the interesting TWIST to this story and what we all can learn from, was that the company found and rebuilt/relaunched their systems after discovering a first attack – only to later find the hackers had maintained access!

This highlights how critical a comprehensive, well documented 'Cyber Incident Response Plan' is for your organisation. It's human nature, and understandable that most IT professionals would simply jump in and quickly restore things to get the business and its customers back up and running, but a little forethought goes a long way. Resilience also requires planning and practice. Remember the saying we love: Under pressure, you don't rise to the occasion, but sink to the level of your training! What level of training would your organisation 'sink to'? If you think you could be better prepared, consider our unique approach for cyber incident response simulations, and just drop us a note here.

Legal lessons learned?

The positive impact that Artificial Intelligence (AI) will have is enormous. But the old saying 'every rose has a thorn' is also true. The lead line in an article this quarter said it all: As artificial intelligence tools become more embedded in legal practice, courts around the world are beginning to confront the consequences of their misuse. While there are other examples, we noted that the Federal Court of Australia ordered a Melbourne law firm to pay indemnity costs after a junior solicitor used Google Scholar to generate citations that were either incorrect or referred to non-existent documents.

Have you set the rules (aka 'policy') about the use of AI in your organisation? Do you have an effective level of Governance to coordinate how your organisation uses AI? Are accountabilities defined or clear?? Just drop us a note if you want help to put the building blocks into place – if nothing else, do it BEFORE you find yourself in court!

Parting thoughts: Does your Board need a change of perspective?

We loved the quote from head of the National Association of Corporate Directors (NACD) who, in a McKinsey article, said:

"Corporate boards and the C-suite used to think of cyber-risk management as an investment in avoiding loss—of data, money, and, importantly, trust. That view has evolved, and today cybersecurity is increasingly recognized as a driver of competitive advantage and critical-asset protection." Hallelujah!

We appreciate you being connected with us and taking the time to read this quarter's update. If you're not already, please 'follow us' on LinkedIn and/or X (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