The third quarter review
September 2023

As we reflect on this quarter's key issues, it's clear that while Cyber Security issues continue to be a 'hot' topic, so too is the issue of global warming. In August the world's oceans reached a new record high temperature, exceeding the previous record in 2016. And the world had its hottest month of July in 174 years! Mother Nature was not happy this quarter with earthquakes, floods, and now El Nino has been declared for Australia!

On a brighter note, it was ~~global~~ heart warming to see Australia place so well in the Women's FIFA World Cup – the overwhelming wave of support for the Matilda's was great to see!

The need to raise the bar

This quarter saw the appointment of Australia's first Cyber Security Coordinator – there is a lot for Darren Goldie to do…

For example, we read about concerns that the Attorney-General's department and about the "persistent 'optimism bias'" that the Australian National Audit Office identified across Commonwealth entities when they self-assessed the status of their cybersecurity compliance to the Protective Security Policy Framework. Political niceties aside, use of obtuse definitions like that might be better served if it was bluntly announced as constantly understating their IT vulnerabilities!

In addition, Australian Prudential Regulation Authority released the gaps from over 300 'tripartite cyber assessments' which found; incomplete identification or classification of critical information assets, limited assessment of third-party security capability, inadequate definition and execution of control testing, incident response plans that are not regularly reviewed or tested, limited internal audits of infosec controls, and the inconsistent reporting of material incidents in a timely manner. Yikes!

Not to be outdone, perhaps that's also why the Australian Securities and Investments Commission (ASIC) Chair, Joe Longo, urged boards to prioritise cyber. He noted quite clearly that "*ASIC expects directors to ensure their organisation's risk management framework adequately addresses cyber security risk, and that controls are implemented to protect key assets and enhance cyber resilience.* ***Failing to do so could mean failing to meet your regulatory obligations***".

One of his key points was, *"There is a need to go beyond security alone and build up resilience – meaning the ability to respond to and recover from an incident. It's not enough to have plans in place. They must be tested regularly – alongside ongoing reassessment of cyber security risks, including within the supply chain"*.

If you need help to address most of those gaps and issues (and meet your legal obligations), just drop us a note (here). We've helped hundreds of commercial and government clients with those challenges. For example, we've defined comprehensive control frameworks, undertaken independent testing of those frameworks, tailored 3rd party cyber assessment approaches, and our innovative 'Trusted**Response**' platform for cyber incident response testing (aka War Gaming or Simulation) is significantly more valuable than the 'old school' approaches.

Only 27% of Australian companies report an incident?!?!

A study of over 4,000 cybersecurity decision makers in Asia Pacific found that half (50%) had experienced TEN or more cybersecurity incidents just over the past 12 months. And nearly three quarters (72%) of those surveyed, forecast an increase in the volume of incidents. Yet, how is it that only about one third (38%) felt they were highly prepared?

One other key statistic tucked away in the detail of the study really stood out for us. In the Australia-only results, it found that only 27% of Australian organisations disclosed cyber incidents to the authorities. If true, the implication to some of the most key Australian Cyber Security Centre (ACSC) statistics is daunting. The ACSC said in 2021-22 there were 76,000 cybercrimes, or 1 every 7 minutes. If that only reflects 27% of the number of 'real' incidents, it would mean there were over 280,000 cybercrimes, or ONE every TWO minutes!

Those findings were somewhat corroborated in July by the IBM Cost of a Data Breach Report which studied over 550 global incidents. Not only are data breach costs escalating, but it also found that organisations were apprehensive to engage law enforcement during a ransomware attack due to the perception that it will only complicate the situation. Although it found evidence to the contrary, nearly 4 out of 10 (37%) organisations impacted never involved law enforcement.

In short – it's fair to say our industry's efforts to measure the significance and scale of the 'cyber' problem, may be woefully understated.

Cyber is a leadership challenge.

We frequently rant about the stark contrast that we see between those sound cyber security programs, and those that are fledgling. From our perspective working on more than 3,000 projects across over 330 clients, one of the most important factors behind programs that are successful, versus those that are doomed to fail, is the approach of the organisation's Leadership Team. The ENTIRE C-suite 'walks the talk' and recognises that cyber is not just a technology problem, but a whole-of-business problem. The newspapers are littered with examples where a cyber incident impacts an organisation's legal team, accounting and finance team, operations teams, etc.

So our ears perked up when we read a recent post from Brian Krebs that found while 88% of the 'Fortune 100' companies listed Human Resources professionals in their executive leadership ranks, only FIVE (5) companies listed a security professional in their top executive hierarchies. Of particular note was the insightful table that illustrated the characteristics of what cyber maturity looks like in an organisation from the perspectives of philosophy, people, process and technology.

Because that's where the money is!

Willie Sutton's famous quote in the above title rang true again this quarter when we learned the attack on law firm, HWL Ebsworth impacted over 65 Australian Government entities (and most of the banks).

So how is it then that the 2023 State of Cyber Security in Law Report found that out of 85 Australian law firms surveyed, over HALF were not ready to handle a cyber incident? Or that 43% were either unsure or didn't believe their firm was doing enough to protect itself against a cyber attack?

"It won't happen to us" must be the perspective since the choice of "Improving Cyber Security Posture" took a back seat to Operational Efficiency, Revenue Growth, and Staff Retention as the main strategic priorities for FY24. Wow! Expect more law firm data breaches if those findings are true.

____

Thank you for investing the time to catch up with us this quarter. 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