It seemed like it was a long, cold winter quarter. But contrary to opinion, the Bureau of Meteorology says it was a warm winter last quarter (in fact, the 5th warmest on record!). That reminds us of the power of "analytical insights" rather than gut feel or opinion (shameless plug... drop us a note if you want to know more about our powerful 'analytical insights' to quantify the health of your cyber security posture – factual insight for decision making!).

Another big event this quarter was seeing the immense power of international cooperation, when the soccer team was rescued in Thailand. It was a heart-warming outcome given initial expectations and the very sad loss of the brave Thai Seal, Saman Gunan. The power of this type of international cooperation demonstrates that building walls is most often not the solution. Similar cooperation would go a long way to dent international cyber crime!

We also found it interesting this quarter when privacy issues lead to the single, largest, one day loss of a company's market value in ALL of corporate history! The share price of Facebook dropped almost 20 percent ($119B) after it revealed that 3 million users in Europe had abandoned the social network since the Cambridge Analytica scandal. The share price still hasn't recovered. Could your company (or Board) withstand a 20 percent drop in market value if consumers thought their data was being misused? It's worth posing that question to your Executive team.

Finally, we're delighted to announce our new and (hopefully) improved website (here) – crisper, cleaner, and more aligned to our strengths. We'd be thrilled to hear your reactions! Good or bad; please send us a note! Onto the key cyber insights for the quarter...

MyHealth Record... Did you opt out?

This quarter, the industry was overwhelmed by the press surrounding the security of the "MyHealth" Record system. One of the greatest challenges of the MyHealth system, which many organisations face today with complex supply chains or extended digital 'eco systems', is the nature of distributed access to a common source of sensitive information. PEXA learned that lesson earlier in the year when a solicitor had their mail system hacked, and details for conveyancing proceeds of $250,000 were diverted to a fraudster's bank account. Purportedly, "*another homeowner had more than $1 Million stolen in a similar theft*."

In other words, one individual's poor 'cyber hygiene' (often several layers removed) may expose an organisation's data and it's the original organisation's reputation that gets shattered, not the source of the breach. For example, in the MyHealth context, the health industry is notoriously lax with basic cyber hygiene (drop us a note if you want proof). It's the hundreds or thousands of diverse health practitioners who access your data on the MyHealth system who may inadvertently expose your details. It can often be less about the 'controls' in place at the source (Australian Digital Health Agency (ADHA)).

To be clear, we don't want to join the 'opt-out' bandwagon – in fact, we really believe MyHealth Record is sound, a relatively low risk for many citizens, and will definitely improve health outcomes. In fact, the ADHA has done more than most to very competently articulate the security controls in place to protect the system from compromise.

The **important message** for YOU, is to consider the possible analogy for YOUR organisation. If you have a complex digital supply chain or digital ecosystem; 1) have you and your Board accurately discussed the possible risk of connected / distributed 'third parties' who may be the source of your next data breach? Think about what might be done ACROSS the ecosystem and don't simply focus on the (legal, IT, or security) controls you have in place within your own business walls (we can help with this type of risk assessment), 2) raise cyber awareness across this ecosystem – it's an investment worth considering. Our 'SecurityThinking' team has experience and industry recognised tools to help, 3) assume a breach will occur – make sure your executive team AND key suppliers have performed multiple cyber data breach exercises – we have some unique approaches and proven frameworks to help here too if needed.

However, before we leave this topic, we value a good sense of humour and 'The Chaser' did an exceptional piece on the security of the MyHealth Record... Very funny... their tongue-in-cheek article is worth a 5 minute read (a very small snippet below):

"[The Health Minister] implored people to give the government a chance to prove that it can keep your information safe online. 'You can trust the Government with your data. According to the 2016 census, all four people who managed to fill it out think government websites are reliable," he said."

The facts support the risk

This quarter saw an FBI, Public Service Announcement that quantifies 'business e-mail compromise' (BEC) at $12 Billion – that's big! If that was market capitalisation, it would make it the 23rd largest company on the ASX! Even closer to home, Australian online payments fraud in 2017 was nearly one half of a billion dollars ($476 Million – up from $418 in 2016). That's big too! And it seems to be happening everywhere – four detainees from the Villawood detention centre were charged with over $3 Million in online fraud (why does this old favourite saying from Sergeant Schultz come to mind?). One last fact: since the Notifiable Data Breach scheme commenced in February of this year to the end of last quarter (only 4 months), there have been over 300 breach notifications!

What does it mean to you? 1) Cyber crime is on the rise. Does your organisation's risk register accurately reflect the 'likelihood' that a cyber crime will occur? 2) BEC is pervasive: make sure your accounting department has verification methods – not only for strange requests from the CEO - but more important, changes in supplier bank account details. Also, make sure your human resources department has similar verification methods for changes in an employee's bank account details for regular pay, 3) invest in your organisation's 'SecurityThinking'. We have online tools and tailored approaches to drive measurable 'culture change', 4) prepare for a breach to occur – is your executive group exercised in the ability to respond and recover from a data breach? (we can help).

Why spill Cyber??

In 2016, we were proud to be part of, and see considerable progress when Australia released its Cyber Security Strategy. Yet only two years later, we see the cyber security and digital transformation ministries are scrapped! We appreciate that Ballarat's Prime Ministers Avenue can't afford to keep up with the quick succession of leaders, but the 'bad guys' don't particularly care about our politics, and the loss of visibility at senior Government level is concerning. Particularly when allies are significantly ramping up the ability to conduct 'offensive cyber operations'?

Significant Salient Statistics (and notable articles)…

It's a 'lengthy read' but just like their exceptional article on the Unprecedented Hack of Ukraine's Power Grid, Wired has outdone themselves to bring to life the untold story of the Most Devastating Cyber attack in History. Distant cyber attacks can go unappreciated by your Executive team. Perhaps suggest they put these two articles on their summer reading list – Wired does a great job making cyber 'real'.

Each quarter we trip across a wealth of statistics published from diverse sources. When used sparingly and in the right context, statistics can often improve a discussion with senior executives or those less exposed to the industry.

- Websites experience an average of 58 attacks per day – 16% increase over Q1 2018
- 2,308 breaches, exposing 2.6 billion records have been reported in the first half of 2018

Thank you for being part of our community and taking the time to read our quarterly update. If you'd like to send this to others who might enjoy it, please pass it along or subscribe them 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