The industry's started with a bang this year. Each previous year seems to finish with a (repetitive) mantra that the it was 'the year of the breach' – only to be quickly outdated by bigger or more frequent issues then ever anticipated (like the largest 'Denial of Service' attack ever recorded, or that hackers stole A$2.3B from Australians last year!).

The (Darwinian) lesson? ADAPT! In cyber security, if you are standing still (doing nothing or just keeping the status quo), you're going backwards (because advisories are moving... and fast).

This quarter we proudly cheered our Aussie's in the Winter Olympics, and was even prouder to learn the event was not significantly disrupted by the cyberattacks that occurred in the background (the lesson: crisis planning and preparation delivers value – more on that later). Keeping on a positive note, it was also nice to see the 'bad guys' do get caught when a coordinated international effort arrested 36 (one Aussie) people responsible for well over a half a billion US dollars in fraud, and hopefully the "Carbanak mastermind" behind A$1.6B in fraud is now in jail too.

Australian Data Breach Notification laws came into effect and in the first 3 weeks, 30 notifications were received. It's nice to know that Aussie organisations are trying to do the right thing. Particularly when we saw issues this quarter like Uber using a bug bounty program to pay off hackers to keep a breach quiet, or how a former Equifax CIO is charged with insider trading by trying to dump shares just prior to announcing its massive data breach (now estimated to be the most costly breach in history).

"... it is time to stop being naïve when it comes to cyber security"

The Chair of Maersk (and ironically ex-CEO of software giant SAP), shared at the World Economic Forum, the full extent of the £$250-300M damage caused by its 'NotPetya' malware infection (here's a very good video panel discussion to share with your execs).

4,000 new servers, 45,000 new PC's, and 2,500 applications had to be rebuilt or installed over an impressive 10 day effort. We suspect that replacing technology was the (relatively) easy part – the company went into 'manual mode' to manage one fifth of the world's shipping containers... that's 1 ship laden with 10-20 thousand containers in a port somewhere in the world, every 15 minutes... manually. Do some of your executives think that cyber is simply an IT problem? The Maersk Chair said it well...

"What did we learn? Number one... We were basically average when it comes to cyber security... like many companies. This was our wake up call to become not just good... but we have a plan where our ability to manage cyber security becomes a ***competitive advantage****. That's the ambition that we have..."*

We saw that theme repeat itself often this quarter, and thus, it's worth expounding on:

- An article on how "Data Breaches Plague Organizations for Years" summarised it as: "the financial aftermath smolders, then comes the lawsuits, then shareholders arrive with flaming torches, next come the Feds, finally, got cyber insurance?".

- A NY Times opinion asked whether "Cybersecurity today is treated like accounting before Enron" ("*A complex hack may not be a C.E.O.'s fault, but it is absolutely his or her responsibility.*").

- Finally, the issue of "Cognitive Bias" ("organisations often act decisively to counter risk only once a major breach, such as a safety catastrophe or hacking event, forces them to. Part of this is because humans discount the likelihood of worst-case scenarios happening, which can blind us to obvious dangers"), was also well explained by a simple observation that "people are far more afraid of flying, than of the car ride to the airport, even though the car ride is tens of thousands of times riskier."

Okay, it's an interesting problem, but what are the practical lessons that you might apply to your organisation? First, if 'cyber' is not on your risk register, we'd suggest that for nearly all organisations it should be there somewhere. For most, it shouldn't just be one line item, but defined in greater granularity so that appropriate

'controls' can be implemented to minimise those risks. With a good understanding of your practical cyber risk, it can lay a factual foundation for doing the important basics like building a 'SecurityThinking' culture to reduce employee 'click risk' and raise awareness, patching systems, tightening access to key systems, etc.

Second, try to explain to the Board and Exec group that it's not possible (or practical) to stop a data breach or cyber event. It will happen. You can't (or don't want to) spend the amount of money needed to definitively stop it from happening. Instead, building a capability to respond and recover from an event is the key, and it requires practice. Planning for an inevitable cyber event is worth the investment, and it's a broader business exercise, not a simple IT drill. Drop us a note if you like to better understand the 'cyber crisis planning' challenges, complexities and the broader business requirements – we've developed some well-tested approaches.

Finally, evaluate how you stack up against a contemporary and comprehensive list of 'best practice'. We like the "NIST Cybersecurity Framework" because it can be easily explained to non-technical executives (at the top 5 category level), and yet it also expands to a level of detail to better understand the real state of your maturity. At a minimum, take a crack at the assessment yourself. Or if you'd like an experienced or independent view, we've got some proven tools and techniques to assist.

Heads up if you're in the financial industry...

Geoff Summerhayes (Exec Board Member of the Australian Prudential Regulation Authority), gave a spectacular speech on "Computer Terminal Velocity: APRA's Response to an Accelerating Risk". It's well laid out, and provides a solid explanation why APRA will introduce a dedicated Prudential Standard to shore up 'the ability of APRA-regulated entities to repel cyber adversaries, or respond swiftly and effectively in the event of a breach'. It's expected the Standard to land in 2019.

"The challenge requires ongoing vigilance, improvement, investment and oversight because, though this race has no finish line, it's not a contest you can afford to lose."

Significant Salient Statistics...

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

- This quarter saw the internet top 4 BILLION users. Each user has access to your website, remote access, or "IoT device". That's an exciting business population! On the other hand, if you thought there was a "1 in a million" chance someone could get access to your digital environment, that means there's more than 4,000 of those "million in one" chances!

- 1 in 5 healthcare employees would be willing to sell confidential data to unauthorised parties for as little as $500. Frightening. Sad too. Do you have the tools or processes in place to evaluate if a user is 'genuine'?

Welcome to 2018. We live in exciting times – abound with incredible opportunity. It's easy to focus only on the negative, so don't forget to embrace the positive. Just do so with the insight of the potential risk! Thank you also for being part of our community – please feel free to pass this along (or one can subscribe here).

Kind regards,

TrustedImpact
PROTECTING DIGITAL