Fourth quarter update
December 2018

This quarter definitely finished with a BANG. Just in this month alone, we've seen riots in Paris to dramatic swings in share markets. One day the US share market saw the 'biggest one-day point drop ever', and the next minute it's booking a gain. The dust still hasn't settled in the US, but fortunately, and true to form, Australia is less spasmodic and the wheels continue to turn with the 'she'll be right' positive attitude and strong local economic indicators.

Clearly 2019 will be a year filled with more of the same (turmoil that is). Whether it's the local impact of global trade wars, or global cyber wars, the three key learnings this quarter (at least in cybersecurity terms) are to: 1) not be distracted by the noise and keep a tight focus on the basics (ie, patching, passwords, back up), 2) plan for the unexpected but inevitable (ie, cyber insurance, data breach crisis planning), and finally, c) 'people' and cyber culture change should be a key focus in any cyber program next year. A breach is inevitable – becoming a headline doesn't have to be.

Mandatory Notification Laws... just the beginning.

This year could be easily called the year of cyber legislation. We saw the European Union's "GDPR" come into effect, which means businesses must report breaches within 72 hours and can be fined up to €20 million or 4% of revenue. Locally, the "Notifiable Data Breach" scheme has racked up 550 data breach notifications from its start on February 22nd to the end of September (by the way, that's nearly 2.5 breaches every day!). And, as highlighted here – US legislation continues to be introduced at a frenetic pace.

Locally, you'll be in the hot seat next year if you're in the financial industry. In January we highlighted the Australian Prudential Regulatory Authority's speech, on "APRA's response to an accelerating risk", with the great quote "*The [cyber] 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".* As flagged, the final version of its "Prudential Standard CPS 234" was released in November and will take effect in July 2019. Key highlights (emphasis added) include:

1. "The **Board**... is ultimately responsible for the information security of the entity."
2. "Where information assets are managed by a... **third party**, the... entity must assess the information security capability of that party, commensurate with the potential consequences of an ... incident"
3. "[The]...entity must test the effectiveness... through a **systematic testing** program"
4. "[They] must have **robust mechanisms** in place to detect and respond to... incidents"
5. "[An entity] must **notify APRA... no later than 72 hours**, after becoming aware of an... incident"

Not only is CPS 234 'short and sharp', but it's poised to be wielded when connected with the related observation that the Government committed an additional $60 million to APRA to "strengthen" its enforcement powers "after the regulator was criticised in the royal commission's interim report for rarely taking wrongdoers to court". Forewarned is forearmed, so don't wait until July to get ahead of the game (and call us if you need a 'Coach' or 'Personal Trainer" to help you win at that game). Are you prepared? If you want an independent, experienced perspective, perhaps we can help by running a 'measurable' executive data breach crisis management workshop to identify strengths *and* improvements (not just an interesting exercise that wastes your C-suite's time).

Cyber – now a business advantage and competitive differentiator

This year we saw numerous examples where consumers, and businesses alike, are recognising the measurable business value from demonstrating that one has a sound cybersecurity program. In yesterday's world, cybersecurity was a cost and often considered the necessary evil that reluctantly had to be incurred by an organisation. In today's world, it's one of the key variables to drive 'top line revenue growth'.

How so? From a business perspective, the above APRA regulation highlights the critical role of third parties and their cyber posture. This was further reinforced this month when Australia joined the other 'five eyes countries' to highlight China's use of "the cloud to step up spying on Australian business", where "Tens of thousands' of Australian firms could be affected". It was highlighted that third parties, also known as "managed service providers (MSPs), are trusted by other firms to store, process, and protect commercial data, helping run every aspect of

Australian businesses, from human resources to accounts management." So, if you provide services to another business, expect the questions about your cybersecurity program and posture to increase. By 2020, Gartner thinks that 60% of organisations engaging in mergers and acquisitions will consider cybersecurity posture as a critical factor in their due diligence process. Therefore, consider your ability to answer the relatively simple 'TOP 10' Due Diligence Questions for services providers we put together for several of our friends and clients.

From a consumer perspective we just need to reflect on "Data, distrust, and the disastrous My Health Record". Or perhaps this quarter's astonishing news of the four year old, 'half a billion' guest, data breach by Marriott, who "now faces a class-action suit and shares have subsequently fallen 5.6%. On top of this, Marriott says for about 327 million victims, compromised data may include names, addresses and passport numbers — prompting [US] Senator Chuck Schumer to demand that it "foot the bill" for new passports." As further noted in that Forbes article, "CEOs won't take protecting our data seriously unless their own jobs are on the line," says Senator Elizabeth Warren, adding that "Congress should focus on holding them accountable for these giant screw-ups".

Cyber: it's a 'top line' issue and Boards should evaluate expenditures in the context of revenue retention, acquisition, or potential loss perspective. In fact, Accenture just quantified the impact of trust on a company's competitiveness and bottom line. As they say "trust is anything but soft". And if you're a CEO it might help minimise the career risk behind "Eight reasons more CEOs will be fired over cybersecurity breaches".

Multi-Factor – do it NOW!

We're fortunate to have worked with a number of great companies over the last few years performing 'red team's', where we are engaged to 'prove we can get into a company's digital environment'. Something we're seeing on an all too consistent basis is the relative ease and ability to get access via 'password spraying'.

Therefore, we wanted to highlight that to you, because from hard, project-based statistics, it's as a significant risk that's prevalent across in most industries; large to small, Government to Commercial. An effective way to minimise this risk is through the use of "Multi-factor authentication". If you are not using it for your external, internet-facing systems, you should. Simply: do it and do it now – particularly for 'privileged accounts'. We can help you think through the best approach, but for many it's simply a matter of turning the functionality on. With over half of the world's population online (51.2%), the prevalence of smart phones in the workplace, and the significant risk of exposure, it's worth any potential 'user push back' to get it going.

Significant Salient Statistics (and notable articles)...

Used sparingly and in the right context, statistics can improve a discussion with senior executives or those less exposed to the industry... this quarter we learned that:

- 74% of businesses can expect to be hacked this year, and by 2020 $3 trillion will be lost to cybercrime (and a great video worth the five minutes to view and support).
- Every 60 seconds, $1.1 million is lost to cyberattacks, and (different source) each year Australians fall victim to identity crime with an estimated cost of over $2 billion annually.

Thank you for being part of our community and taking the time to read our quarterly update. We wish you all the best for a safe and prosperous 2019. Please 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