Second quarter update
June 2017

Every quarter, the team at Trusted**Impact** reviews the previous quarters' industry news for data that provides our clients and colleagues with unique perspectives as they seek to improve their cybersecurity maturity. To quote Sun Tzu, "The opportunity to secure ourselves against defeat lies in our own hands"... and perhaps a little help from us.

There's been a fair amount of turmoil on the world stage this quarter. Terrorism struck very close to home, one of our country's largest television stations went into voluntary administration, and the world's democratic political system took (another) wild turn with unexpected voter results in the UK. Perhaps just another "COVFEFE" moment in world politics? (here for a good list of hilarious covfefe memes).

Cyber Trust as a Competitive Advantage

Trusted**Impact** turned 10 this year. When we reflect on how far the industry has come, it's exciting to see the major shifts which have occurred in that short time. Ten years ago, the term 'cyber' was barely used, and security was seen as a 'necessary evil' that organisations had to pay for the possibility that something might go wrong.

These days we're proud to have a number of clients who see 'Cyber Trust' as a fundamental strategic advantage. It's a key part of their strategy to grow revenue by keeping clients longer, and win new customers over competitors who can't explain how they protect a client's data. In line with that thinking, this quarter we enjoyed some good thinking from SAP (here) that aptly noted:

> *"...categorized as risk to avoid rather than opportunity to pursue, cybersecurity has never been a terribly sexy topic in the C-suite... Even as companies have embarked on their digital transformation efforts, security has remained an afterthought... Very soon, however, that reactive approach will seem antiquated."*

Many still learn the hard way. An engaging story of the real world impact of bad cybersecurity, is the small family owned production studio in the US that was ransomed $50,000 for unreleased versions of a popular Netflix series.

> *"...Once I was able to look at our server, my hands started shaking, and I almost threw up... Upon hearing the news, some studios decided to take their business elsewhere... [we] spent months trying to mend relationships... [and] the company is struggling with the perception that it is at the heart of all of Hollywood's security woes.*

It's a topic of interest to us. In fact, we were honoured to be asked to host a panel discussion on that topic for 'Cyber in Business' conference in Melbourne last year. Another is planned for July 28th in Sydney. We get excited about the topic because we think cyber is a business problem, not just a technology issue. Drop by if you can.

Why Executives Underinvest in Cybersecurity

You know Cybersecurity has gone mainstream when Harvard Business Review (HBR) starts writing about it. As always, the HBR has interesting perspectives, and the article by Alex Blau is worth reviewing if you have challenges getting executive support for cybersecurity. Simply stated, "In the case of cybersecurity, some decision makers use the wrong mental models... the problem with these mental models is that they treat cybersecurity as a finite problem that can be solved, rather than as the ongoing process that it is". Instead of regurgitating the work here, it's worthwhile spending 10 minutes to read this thoughtful piece.

The speed of exploitation

This quarter, we were frightened to see how quickly personal data on the internet is accessed and exploited. In a recent test, by the Federal Trade Commission in the US, and summarised by CNN here, found that in NINE MINUTES between the time when test confidential data was posted on the internet, thieves began using this information. "All told, there were over 1,200 attempts to access accounts belonging to face consumers. That includes a total of $12,825.53 attempted credit card purchases and 493 attempts to access emails".

The top 10 Cybersecurity myths

This quarter, Marc Wilczek wrote a comprehensive piece perspective on the common myths. What made this work refreshingly unique, was that behind each myth, there is a well-referenced piece of factual analysis that supported his 'myths'.

Too often, cybersecurity personnel 'shoot from the hip' and use 'gut feel' for their perspectives or company's investments in cyber. If you need analytical support to build the case in your organisation – it's worthwhile having a quick read here. In fact, that's one of the reasons why we developed our 'analytical insights' approach to our health checks – small, but specific pieces of analysis that can be conducted to provide the factual insight into the 'health' of an organisation's cyber posture – if you like to support your organisation's program with factual insight, drop us a note to speak more about this unique approach.

The ransomware that rattled the world

This quarter the world was reminded how far-reaching and potentially devastating cyber risk can be – particularly if one doesn't maintain a rigorous 'patching' program to update their systems (since Microsoft had released a patch a few months prior). The pervasiveness of the impact of the "WannaCry" ransomware was captured in some interesting pictures summarised here. But best of all was the humorous take that Charlie Pickering had on "The Weekly"... a good laugh worth the 2 minute video!

Son of Stuxnet – or worse.

If you worry about 'Nation State' threats or critical infrastructure make sure you read Wired's piece on CrashOverride. "If this is not a wakeup call, I don't know what could be"... and its more thorough piece on Russia's "Test Lab for Cyberwar"

Significant Salient Statistics...

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.

- The cost of Cyber Risk to hit $US8 Trillion in 2020. That's with a "T"! To put that into perspective, that's nearly SIX TIMES Australia's entire Gross Domestic Product. It's also a massive jump from their same estimate only two years ago, when they estimated cyber risk would cost $US2 Trillion in 2019!
- 90% of Australian organisations have faced some sort of cybersecurity compromise during the 2015-16 financial year. Organisations faced numerous malicious cyber threats on a daily basis — through spear phishing emails alone, organisations are affected up to hundreds of times a day (Australian Cyber Security Centre 2016 Survey)

Thank you for taking the time to catch up with us, and being part of our community. Please pass this along to someone who might find it useful (or they can subscribe directly here).

Kind regards,

TrustedImpact
PROTECTING DIGITAL

we're **independent** consultants – it's about **your** business and **your** success
with a **singular focus** – information security is all we think about
leveraging **experienced** professionals – credentials, not checklists