Already the third quarter of 2016! Wow, time is flying. We were reminded of just how quickly in July, when we saw the last remaining manufacturer of VHS recorders cease production... It seems like only yesterday that Blockbuster Video was a household name. In the year 2000, it turned down the chance to purchase Netflix for $50 million (now a market cap of over $40B), and in its heyday had 60,000 employees and a US$6 Billion turnover. We live in 'interesting times' and the pace of change is increasing.

Another reminder arose this quarter. Just 8 years ago the first commercially available smartphone running Android was released. We now learn that nearly one BILLION Android devices are vulnerable, and "fixing them will be no easy task". The pace of change in 'the digital age' is exciting, yet sometimes horrifying from a security perspective.

19% of shoppers would abandon a retailer that's been hacked...

Let's just assume that only HALF of that number was correct (i.e., thus, 9.5% to be very conservative). Simply multiply that number times your organisation's revenues (or net income). What does that equal for your organisation? The survey (summarised here) also found that another one third (33%) said it would keep them from shopping at the breached retailer for more than three months. Using the conservative 9.5% revenue loss estimate for one of the largest retailers in Australia, equals a whopping A$5.9 Billion.

Now, contrast that with the other survey finding that over half (55%) had NOT spent money on cybersecurity in the past year...

Mismatch? We think so, because the revenue impact of a data breach is only one piece. Another 11 tangible cost areas were explained well here. Even more, *"For all the quantifiable costs, there is also a range of hard-to-measure costs like brand reputation, consumer loyalty, board and stakeholder relations, distraction from normal business activities, regulatory finds and potential class action lawsuits"*. Hmmm, one possible approach could be to link CEO compensation to effective cybersecurity (see next)....

CEO compensation to be linked to effective cybersecurity?

The Brits may have cottoned onto one way to align the security effort to potential business loss. A UK Parliamentary report released in July suggested that:

> *"cyber security should sit with someone able to take full day-to-day responsibility, with Board oversight... To ensure this issue receives sufficient CEO attention before a crisis strikes,* ***a portion of CEO compensation should be linked to effective cyber security*** *[emphasis added]...."*

However, the UK isn't alone. The US Senate proposed a somewhat similar bill (summarised well here) requiring publicly traded companies to disclose whether *"any member of their board of directors is a 'cybersecurity expert.' If a company lacks a cybersecurity expert, the proposed bill would compel the company to explain... why an expert is not necessary and the additional measures the company is taking to improve cybersecurity."*

We question whether it's practical (or even preferential) to have security 'experts' on the board. Security is a business problem that should be managed by business people on the Board. Nonetheless, we appreciate the driver behind the bill – the originating Senators reported that "only 11 percent of public company boards reported a high-level understanding of cybersecurity... [and] 30 percent... never talk about cybersecurity at all".

Regulated accountability was a theme this quarter. Another US bill gives the US Office of Management and Budget (OMB) the power to demote, fire or monetarily punish an Agency Head if a data breach occurs under their purview. It goes so far as to define that the OMB Director can ensure the agency head doesn't get "any cash or pay awards or bonuses for a period of one year after submission of the explanation for the incident".

On local shores, breach notification has been on the cards for a few years... yet, discussion seems to be focused more on defining what 'serious' means in terms of a data breach, while the rest of the world appears to have

leapfrogged us to focus more on accountability – a notable and important difference. So, how do you think your executive suite would respond to the UK or US requirements? We'd be keen to hear your thoughts.

What's your number?

Ransomware proliferates this quarter to the extent that the US FBI urges victims to report infections to get a more comprehensive view of the threat and impact. Infections are at an all-time high, with the FBI release noting that one particular variant compromised an estimated 100,000 computers a day in the first weeks of its release.

This is one reasons why we run 'phishing campaigns' for clients, who want to understand the magnitude of the risk they face from staff simply clicking on links, or providing sensitive information. It's one of a few 'analytical insights' we have in our 'kit bag' to help clients leverage factual statistics to support meaningful cybersecurity investments across all aspects of 'people, processes, and technology'. We also keep a running total of the results so organisations can compare themselves against a relative local peer group.

Executives are often surprised to learn that overall, **84% of employees who read the phishing email, actually click on a nefarious link** (think Ransomware infection). But even worse, **14% provide us with their valid username and password**. Ever wonder what your numbers would be? Drop us a note (here), if you'd like to measure it.

We hate to say "we told you so", but...

In 2008 our "M&A due diligence" brochure started with "Experts from accounting, venture capital, consulting, and law firms can be good at assessing the profitability and synergies of a merger or acquisition. Yet little, if any, attention is often paid to the security posture of the organisation under scrutiny – often with disastrous results."

That rang true last week when Yahoo announced that it lost details for a half a billion users. The magnitude of that breach is significant, but also just as relevant is that Yahoo is in acquisition discussions with Verizon for a proposed $4.8 billion... So, just what dollar impact will a breach have on the acquisition's valuation? Maybe it collapse the entire deal? Is your organisation acquisitive? Maybe we should talk about our Security Due Diligence Diagnostic?

Salient statistics and sayings (say that 3 times fast...)

When used in the right context, statistics can really improve a discussion with senior executives. Did you know that:

- Cyber incidents affecting US federal agencies have grown 1,300 percent from 2006 to 2015.
- While 60% of Australia and New Zealand IT professionals expect a cyberattack this year, more than half (57%) say they're NOT prepared.
- "The longstanding failure of OPM's leadership to implement basic cyber hygiene... despite years of warnings... **represents a failure of culture and leadership, not technology**. (The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation)

Many thanks for investing the time to read this quarter's newsletter. Please feel free to pass it along – or colleagues can subscribe here.

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