Fourth quarter update
December 2019

The conflict continues in Hong Kong, Trump's become the third president to be impeached in US history, and Boris Johnson won by a landslide. Closer to home, fires rage across the country and it looks like we're in for a long, smoky, challenging summer. Cyber's likely to be the same!

It's that time of the year again! Sincere thanks for reading our newsletter and for being connected with us. We really appreciate you taking the time to be involved with us. However you celebrate, we hope your holidays are safe and special and wish you all the success in achieving your goals in 2020.

Looking back before looking forward to the new decade

As we enter a fresh, new decade, we thought we'd look back over the past decade to see what we might have learned with the hope that we don't (continue to) make the same mistakes in 2020. There are lots of breaches in other parts of the world in the last decade. This often makes locals think "it won't happen here', so the team compiled our list of the AUSTRALIAN TOP 5 in the last 10 years. That said, it's interesting to note that the big ones have been in just the past few years – perhaps a sign of the accelerating risk of cyber:

1. **The eCensus (2016)**: Poor planning and communication, and an overdependence on one outsourcer was found to contribute to a disastrous eCensus that was exacerbated by the lack of a comprehensive security framework and independent validation.

   "*While the ABS and IBM had a library of incident management documents to guide them through the events of 9 August, they were impractical, poorly tested and none outlined a comprehensive cyber incident response or communications plan that could be effectively implemented*". These days, an incident is inevitable: becoming a headline doesn't have to be. **Invest the time planning AND testing for a cyber crisis.**

2. **Red Cross (2016)**: It shouldn't always be about 'shaming'. In fact, the October 2016 Red Cross Blood Donor data breach, we heralded by many as a great example of how to manage a cyber incident well. 550,000 donor details were leaked, yet they took a proactive approach.

   The OAIC found "Overall, the Blood Service acted appropriately and in a timely manner to rectify the data breach, and its response to the data breach provides a model of good practice for other organisations". Could your organisation respond in a timely manner? The day after a data breach is not the time to ask procurement to 'go to market' for a panel of experts!

3. **PageUp (2018)** – Local HR software company PageUp was considering a public listing before it experienced a breach that impacted its clients, and their clients' recruiting candidates. Businesses that have customers who use software to assist with *their* customers face the 'double whammy' exponential impact when one customer who may use it for tens, hundreds, or even thousands of other impacted individuals. It is one thing to lose customer data, but it's another if you lose a customer's, customer data. Particularly where your customer must incur the reputation hit and incur additional expense to respond to your data breach.

   What can we learn? Cloud applications and SaaS businesses face a range of technical and configuration issues (how many times do we need to read about breaches due to "open Amazon S3 Buckets" before we do something about them?). In a separate example, one company exposed a directory of their application to a traveling developer (and forgot to close it) – it was running outdated software (which was a beacon to the internet) – and they used a poor password (making it easy to crack). Furthermore, forensics were difficult because no one ever considered monitoring. Conduct independent testing, confirm cloud configurations, and develop secure development practices. It doesn't have to be hard – it just needs to be well thought through!

4. **LandMark White (2019)** (ASX:LMW). The local asx-listed valuer stared into the brink of extinction due to the loss of 100,000 property valuations and related borrower, lender, homeowner and property data. There are a lot of important lessons learned, here, and here. While it was found that there was a malicious insider, there were a number of other systemic issues we all much learn from. For example, it was believed that vulnerabilities were known, but not resolved prior to the breach (among others). Memories are short, so we it was interesting to note the company is rebranding to distance itself from the tarnished name.

The overarching issue from our perspective, is the 'the **leadership challenge**' that Boards and Executive Officers must accept to respond to the risks of cybersecurity. The tone and priorities of an organisation are set and reinforced at the top. Cyber isn't a technical problem, but a business challenge that should be faced head-on and with open eyes. The story of LMW isn't theoretical – particularly for those unfortunate execs who are now out of a job and who learned the hard way.

5. **Victorian Public Hospitals (2019)**. Several years ago Trusted**Impact** was fortunate to assist a Government Department with a cybersecurity assessment of the Victorian Public Health Sector. One of the major issues identified was the woeful inability to recover from a cyber incident. About a year and a half later and only a few months before a catastrophic ransomware attack, the Victorian Auditor General's Office also found that the regional Victorian hospital network was highly vulnerable. When patients and paramedics are left waiting hours, as whiteboards are used to triage emergency patients, you can be guaranteed that patient outcomes will be negatively impacted!

   In today's rampant environment of ransomware it is simply unacceptable not to have a comprehensive and frequently tested disaster recovery or back up regime. Every time you read about someone paying a ransom, it highlights that they're just not doing the basics. A "stich in time saves nine" and perhaps your entire business.

And, if you think that isn't good enough, there's a good summary of this year's other 82 Australian-only data breaches (here).

More than 10 years of cyber - business insights!

It struck us that we've been writing Quarterly Updates for more than **TEN YEARS** - phew!! We'd like to think there are some great nuggets of wisdom in the archive [here], but instead of inflicting you with this task, we thought we'd troll through them to find the most meaningful quotes from the last 10 years worthy of reminding you of.

- **"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 2016: How the Government Jeopardized Our National Security for More than a Generation)
- **Cyber crime is the greatest threat to every company in the world"** (Ginni Rometty, IBM Chairperson, President and CEO, Nov 2015)
- **Cyber risk... [is] the most serious threat to businesses... and it's... not going to go away."** (Inga Beale, CEO, Lloyds, Apr 2015)
- **There are two types of companies: those that have been hacked, and those who don't know they have been hacked**" (John Chambers - Chair and CEO of Cisco, Jan 2015)

But since we're looking into a new decade, we thought one of Benjamin Franklin's quotes might be appropriate. In 2020, may you:

"BE AT WAR WITH YOUR VICES, AT PEACE WITH YOUR NEIGHBORS, AND LET EVERY NEW YEAR FIND YOU A BETTER PERSON"

(slightly adjusted to reflect our belief in diversity!)

Thanks again for being part of our community. Please 'follow us' on LinkedIn or Twitter to keep connected. Also, don't hesitate to send this to others, or simply 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