It's the season to reflect upon things that are important, and you're one of those things. We appreciate you taking the time to read our newsletter and we thank you for being a friend, colleague, or valued client (or all the above!). We hope your holiday season is safe and filled with family, friends and fellowship!

Looking ahead...

2017 should be an interesting one for cybersecurity! Speculation is rife with anticipation of a new, seemingly irrational and often volatile US president. Wired's perspective on what Trump's win means for cybersecurity is worth a quick read for those in the industry. Clearly, Trump's pre-election statement that the US must have "unquestioned capacity to launch crippling cyber counter attacks ('...and I mean crippling')" will set a tone for the next four years, and is relevant since we just saw (for a second time) that Russia hacked the Ukraine power grid. So perhaps not a big stretch when global consulting firm, AT Kearney predicted "the first crippling cyberattack will be launched on critical infrastructure in a major economy" in 2017.

Reflecting on the lessons of 2016

Since it's that time of the year, we thought it might be worthwhile reflecting on the major headlines in 2016 as a potential sign of things to come. We saw a number of major themes throughout the year. Some of these included:

- **Whaling paid well**. Billions were defrauded from companies transferring funds at the behest of criminals posing as senior executives (BEC Scam). The scams are extremely well-researched, but with companies like FACC who lost €50 million (and then fired its CFO and CEO), it's an investment of effort the bad guys are willing to make to quietly get on the inside and learn a company's inner workings.

- **The IoT came alive**. We experienced the 'botnet that broke the internet'. The exponentially growing universe of internet-connected devices (aka IoT) from as webcams to baby monitors, were harnessed to clog the internet in the largest "DDoS attack to date" and purportedly knocked one country offline.

- **Cyber's billion dollar Due Diligence**. In the M&A space, dealmakers learned the value of cyber due diligence. Yahoo realised it lost data for more than one billion accounts. Shares of the internet pioneer fell more than 6 percent, and now Verizon, which agreed to buy Yahoo for $4.8 billion is asking for a $1 Billion discount.

- **Health, the new Retail**? Healthcare organisations were caught "in the cross hairs of cyber attackers as evidenced in the 2016 State of Cybersecurity in Healthcare Organizations Study". We were pleased to help develop the Victorian public health care cybersecurity strategy, and it's not just about private health data, but patient lives. The global health industry needs to lift its game as a fundamental business problem, not just an IT issue.

- **Ransomware rife**. The malicious software that encrypts files and requires payment to make them readable again gained significant notoriety in 2016. San Francisco's transit system was forced to offer free rides until the mess was resolved (losing $559,000 each day in revenue), and local Australian examples were numerous.

As we enter into the New Year, we thought about some of the root causes behind these issues and found a few recurring lessons that were worthwhile pointing out for your plans in 2017.

- The BEC scam and whaling examples highlight the importance of knowing who might be on the inside of your technology environment, simply watching, listening and learning. We've helped a number of clients analyse the 'health' of their user's system accounts, and in particular, 'privileged user accounts' who have free reign as IT administrators. Minimising these types of accounts and making sure they align to only one approved individual is a basic principal, but one we see frequently disregarded. In one situation, we found that two thirds of an organisation's privileged user accounts were dormant. In other words, a significant number of old, unused super-user accounts just sitting idle for any nefarious users to exploit. **Do you know the facts behind the health of your privileged system accounts? If not, you really should.**

- The IoT botnet once again highlighted the importance of passwords. The Mirai botnet software used 'hard coded' or default passwords to access thousands of IoT devices. Similarly, the account 'health' analysis (mentioned in the previous point) found passwords for (the most important) privileged accounts are infrequently changed. Our statistical database of more than 500 privileged accounts for more than a dozen organisations, shows that 44% of privileged accounts use old, unchanged passwords. A recent 'Red Team' project used a reused LinkedIn password from 2012 to gain privileged access within 2 hours of effort. **Passwords are hard, but worth the time and effort to keep them sound!**

- The Yahoo data breach highlights just how important it is to have a capability to recover and respond to a cyber incident. The eCensus debacle is a good local example, and the Office of the Cyber Security Special Advisor eloquently noted that it's not just about writing procedures: "*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*". As we've said for a long time: These days, getting hacked or having a data breach is inevitable... becoming a headline doesn't have to be. **Invest the time planning AND testing for a cyber crisis.**

- Finally, the root cause of the San Francisco transit system problem was outdated software with an old, well known and published vulnerability. We conduct thousands of 'penetration tests' and far too often, we find issues because of old, unpatched or unsupported systems. **Patching: It's basic, boring, but one of the basics if you want to survive in the digital age.**

These were just a small sample of the major events in 2016. But they'll likely be representative of what we'll see in 2017. What did make 2016 different, however, was the frequency and magnitude of cyber incidents, and the accelerated pace in which they're occurring. More and more information (and system availability) will be held to ransom and for larger payouts. The bad guys are becoming more skilled, experienced, motivated by larger payouts and becoming more brazen in their attempts because of it.

As an astute colleague mentioned the other day, cyber is not a static 'consequence' and 'likelihood' rating on a traditional corporate risk matrix. What often isn't recognised is the 'velocity' of change behind both the likelihood and consequence. Keeping ahead of the cyber risk in 2017 will require a concerted effort. But don't lose sight of the basics (learned from above), that if followed, would have thwarted many of the issues behind the headlines of 2016.

Salient, Stunning Stats...

Each quarter we see 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.

- On 24 October, the internet reached more than one half of the world's population (3,675,824,813 users or 50.1% of the world's population)
- A total of 3,154,135,541 records were exposed in 2016 (good data breach and cyber attack list here)
- 41% of all security breaches in the UK were from the health sector, and in the past 2 years, data breaches have cost the US healthcare industry over $6.2 Billion dollars.

We're privileged to have worked with some great clients and help them deal with some difficult cyber challenges. 2016 was a great year and we look forward to reconnecting with you in 2017. Many thanks for being part of our community, and please pass this along to someone who might find it useful (or they can subscribe directly 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