Fourth quarter update
December 2015

This quarter, the world's frenetic pace continued. We've noticed that virtually all of our clients at operating at top speed and there is an air of confidence and energy in the Australian economy that's refreshing.

Overall this quarter, we were disappointed to learn that Volkswagen executives apparently have been blatantly rigging diesel engines to bypass regulations, but enlightened to learn that liquid water was found on Mars. We saw the horrific impact of terrorism in Paris, and as we head towards the close of the year and look towards the new one, we are hopeful and resolute that such extremism and terrorism will not be a part of our future.

Are you prepared for Mandatory Data Breach Notification?

Our Managing Director was delighted to participate in a diverse expert panel discussion with the American Chamber of Commerce in October on the topic of whether Australian business was prepared for possible mandatory data-breach notification. Last quarter we learned that 93% of UK consumer support mandatory breach notification laws.

During the discussion, our MD noted that businesses in other countries WITH mandatory notification laws are generally not prepared – no less those in Australia. With statistics highlighting that 7 out of 10 cyber victims were notified they were compromised by an external entity, and the fact that it took somewhere between 205 to 229 days between compromise to detection, one can readily conclude that most businesses are not only unaware they've been compromised, and when they are, it's typically after a very long period of time. Local online retailer Catch of the Day took 3 years to report a breach! But watch this space – while there were conflicting reports released on the same day, it appears that Data Breach Notification laws are still on the Government agenda. Are you prepared?

Is the Bureau of Meteorology a good lesson?

This month the ABC broke the news that the Bureau of Meteorology (BoM) had a "massive breach" of its computer systems from unknown sources originating from China. The BoM stated, "*The Bureau's systems are fully operational and the Bureau continues to provide reliable, ongoing access to high quality weather, climate, water and oceans information to its stakeholders*." It also appears that more scrutiny will be placed on the BoM from a political perspective – we suspect that's not something you'd want to be on the receiving end of.

The ability to provide factual insight around what IS known, and what is NOT known following a data breach is a "key success factor" in cyber incident response. It's essential to provide a consistent set of factual data to a diverse range of stakeholders, from customers to the press. The apparent leak of inside information and lack of detail on what was known, suggests that the BoM may not have been well prepared to respond to a cyber incident. That's not all that unusual because we often find organisations developing cyber incident PLANS, but typically neglecting to remember that a plan is worthless if one cannot MOBILISE it on a moment's notice.

A successful cyber incident response is not just an "IT issue" but about cross-functional and 3rd party coordination. These days, there is an significant external communications requirement as well. Not only do Legal, PR, HR and Operations need to be engaged, but typically multiple external vendors may be the ones actually managing the technology environments. A cyber incident plan that can be mobilised requires things like pre-prepared supplier agreements, defined service level agreements, and war gaming exercises to confirm that resources can truly respond. Drop us a note here if you'd like help developing a capability that can mobilise your incident plans.

Target breach insight – are your passwords just as vulnerable?

At the end of last quarter, we saw more insight into the infamous Target breach of 2013. In particular, the critical role of default and weak passwords was illustrated very clearly. In one week, 86% of Target's 547,470 passwords were cracked and the "Top 10" rankings of passwords clearly show systemic problems. Yes, we know it's hard to maintain complex passwords and there's always lots of pushback from staff, but if you're serious about security, it's something you'll have to address. Another good and related piece on "password entropy" was provided here, this quarter, which simply explains the power of long passwords versus complex passwords.

On a humorous note to passwords, we must highlight the survey this quarter that found "4 out of 5 people in certain European countries claim to have more pairs of underpants than they do unique passwords, which points to either a rampant recycling of passwords or to colossal collections of underpants!"

These 'cyber soft spots' are major risks, but are typically 'unseen' by general health checks, audits or reviews. Because of that, we developed "ThreatScan©". Seven "short and sharp" analytical cyber health exercises that provide our clients with hard, fact-based information to support management decision making and specifically quantify the state of an organisation's key risk areas. These exercises range from employee 'click risk' and 'cloud risk' through to password health and identity health (learned from the Target breach described above). Drop us a note if you'd like to explore how these focused efforts can provide you with meaningful, factual cyber health insight.

Should we expect that to make a difference?

We thought it was constructive to learn this quarter that the US and China were inking a cyber security truce on curbing economic cyber espionage. About the same time, we tripped across a comprehensive article on the topic of "The New Industrial Espionage" and thought it worthy of repeating one interesting paragraph:

"To Chinese and Russian ears, however, the distinction between economic and other kinds of espionage is an ideological construction, convenient only to the West. In their view, all state-sponsored espionage is by definition conducted in the national interest. In these countries, where a distinction between the public and private sectors is either non-existent or blurred..."

What's wrong with this title?

The New York Stock Exchange released a 355-page "definitive cybersecurity guide for directors and officers" of public companies. You can download it here. We applaud the effort, but we also believe the industry needs to understand how to better engage the Boards. Unfortunately no matter how engaging the book is, there aren't many directors or officers who have the time, nor desire to digest 355 pages of cybersecurity.

A common theme identified in our "Security Team of 2020" was the need to demystify security. It can be hard, but it's how we try to differentiate ourselves. If you need help digesting complex security controls or seeing the forest from the trees, we'd be delighted to have a chat. Or alternatively, some Boards find they learn more from 3 slides and a 30 minute chat with some seasoned industry professionals than they do from 365 pages of definition. If this sounds like your board, we'd be happy to chat on how to take that approach too.

The Quote of the Quarter and Salient Statistics...

- "Cyber Crime Is The Greatest Threat To Every Company In The World" (3 November 2015, Ginni Rometty, IBM Corp's Chairman, President and CEO)
- 84% of consumers think companies should be held responsible for data security, and 73% would think twice about using companies that failed to keep their data safe.

Thanks for being with us in 2015 and investing the time to read this quarter's newsletter. We wish you, your family and friends a safe and spectacular holiday season, whatever form that may take. Please feel free to pass this along to anyone who might find it of interest (or they 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