First quarter update
March 2015

This quarter we saw the American Health Insurance industry lose an excessive amount of personal data. Anthem Inc, the US's second largest health insurer lost upwards to 80 million health records, and Premera, Blue Cross lost 11 million records. Since health records are apparently 10 times more valuable than credit card numbers, the motivation is clear. We also learned of 'one of the largest bank heists ever' ... apparently $1 billion from over 100 financial institutions and 30 countries. Bottom line – don't lower your guard. Threats and compromises are clearly on the rise and organisations that think they're not a target are kidding themselves.

Mandatory breach notification by the end of the year?

Data retention laws were just passed forcing Telco's and ISP's to store telephone and internet metadata for two years. However, while many people were furiously debating metadata and the privacy issues, one interesting item may have slipped into the fray. Apparently, to gain support for data retention, the government agreed to 39 recommendations from the Parliamentary Joint Committee on Intelligence and Security. One of these recommendations (#38) states "the introduction of a **mandatory data breach notification scheme by the end of the 2015**." Details are unclear, but irrespective of the form it takes, if your organisation needed to notify customers of a data breach, would you be prepared to do so? We think it should be interwoven into a well-defined cyber incident (crisis) management plan. If you'd like to understand what we've done in this space with a range of clients, simply drop us a note.

Personal liability for Directors and Officers?

We saw an interesting legal position in regards to personal liability for Directors and Officers coming from the US which may be worthy of note. As with mandatory breach notification above, it's reasonable to assume that the likelihood of similar situations occurring on our local shores may be on the horizon at some point. This article noted:

> *The Caremark case has become a beacon across the corporate world for director conduct and now covers officers, including general counsel. Directors and officers* ***must not demonstrate a "conscious disregard" for their duties or ignore "red flags" – failure to do so can result in a director or officer being held personally liable for a corporation's losses****. This is because, as the Delaware Supreme Court later clarified in Stone v. Ritter, conduct that evidences* ***a lack of good faith may violate the fiduciary duty of loyalty****. And, although Delaware law allows a corporation to waive or limit a director's liability for violations of the duty of care,* ***such waivers or limits are not allowed for the duty of loyalty****.(emphasis added)*

While we read about the possibility of PERSONAL liability on one hand, on the other hand from an unrelated article in January, we found it frightening to learn that only "23% of directors were confident in their boards' ability to manage cyber risk". Then again, in February we also heard that 78% of company Boards are NOT briefed on cybersecurity. These divergent issues (eg, personal liability, yet little confidence or information) signal potential disaster. If you think your Board would value having some independent perspectives from a firm focused exclusively in information security, don't hesitate to give us a call.

Lessons from Hillary

We experience the 'cultures' of many organisations with respect to security. One of the most important indicators of a 'leader' in information security, is just that – the C-Suite and Board LEAD BY EXAMPLE and have a sound awareness of risk. Therefore, we were disappointed (albeit, not surprised) to learn that the US Secretary of State, and potential US presidential candidate Hillary Clinton, "opted to use her personal email account as a matter of convenience." This made us wonder about three key questions:

1) Who are the 'system admins' that had open access to her every email?

2) Didn't anyone question whether someone from "@clintonemail.com" was actually Hillary? No wonder we know many examples of "CEO Fraud" and email scams resulted in $215M in fraud over the past 14 months, and

3) Do the 'actions' of your organisation's leaders contradict what they advocate? For example, Obama just budgeted $14B to bolster the security of the US Government, but the Secretary of State is able to use a personal email address for State business?

Actions speak louder than words, and we have found a direct correlation between organisations who have mature security programs and whether the senior executives 'walk the talk.' Nonetheless, there's a good parody on the Hillary issue here that you might enjoy. And to be fair, it's not just an executive-level issue, as humorously shown in this Jimmy Kimmel segment.

Overall, we think this issue should be tackled as a cultural change issue from the lowest levels to the highest levels. If you'd like to discuss the 'culture change' approach to our SecurityThinking© program, just drop us a note.

Just the facts ma'am…

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. This quarter we found these found these interesting:

- 57% think their organization does not consider privacy and the protection of personal information to be a corporate priority ... yet (same source) 71% of customers would leave an organisation after a data breach
- 66% of IT experts believe cloud computing will result in less security
- Over 90% of the data breaches reported to the FBI were entirely avoidable.
- 53% felt there would be a significant impact due to their organisation not being sufficiently prepared to manage cyber threats.
- 43% of companies experienced a data breach last year... 66% say their company experienced more than one data breach in the past two years

How's that $100M Melbourne public WiFi rollout going?

If you've ever done anything 'important' (ie, banking, buying, or checking email) on your smartphone or tablet over a free or open WiFi connection? Think again. Does your company use the same usernames and passwords for their WiFi as they do their internal systems? Think again.

For $99.99, the 'wifi pineapple' sits quietly between you and the WiFi connection – give us a call if you'd like to see how it works. And that's just one of a number of methods we typically use in our WiFi penetration testing. In fact, even a 7 year old girl from the UK demonstrated she could do it in less than 10 minutes. Really – call us if you'd like to confirm you're not a sitting duck.

Thanks for investing the time to read this quarter's newsletter. Please feel free to pass this along to anyone who might find this of interest (or subscribe them 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