Second quarter update
June 2014

This quarter marks the one year anniversary of the Edward Snowden exposure and we continue to hear lots of noise from the nation-state space. For example, we've learned that the US military academies are grooming elite cyber troops, and how the US government is reving up the hacking fight.

However, closer to home and worth highlighting was the interview of Ian McKenzie, the ex-Director of the Australian Signals Directorate written by Chris Joye. We agree with McKenzie that "**top business executives do not fully appreciate the complexity and danger of threats they are now facing from evolving cyber security risks**". Even McKinsey just published "why senior leaders are the front line against cyberattacks".

These types of messages are striking a chord with many of our clients because the reality is that the first and last lines of defence against a data breach are not policy-based or technology, but embodied in the mindset of 'SecurityThinking." A new program and partnership about changing the organisation's behaviour and culture. Drop us a note here if you'd like to learn more.

How NOT to handle a crisis – eBay lessons learned

This quarter we saw eBay lose 145 million sensitive customer records. You'd think that an internet-centric organisation might have conducted some level of "cyber-incident" planning to work through what might be needed in this scenario. Apparently not, as it's been noted as one of the shining examples of how NOT to handle a crisis.

However, probably the best story is the personal account of one of our Principals who tried to delete their account as a result of the breach. When he tried to remove it, his account immediately became suspended and he had to 'appeal' the suspension with a member of the "Trust & Safety team". When he sent them a follow up email to request removal, he was notified that he had to scan (jpeg or pdf) and email eBay both; an identity document such as a driver's license or passport, and one address proof document such as a credit card statement or bank statement. Let's recap: the company that lost 145 million account details now requests someone to send them considerably more sensitive information via an open email just so they can remove their account??

Do you think eBay saw the irony in that request? Probably not, as it was also noted by ZDNet that "the company told the Australian Law Reform Commission that reputation damage was enough of an incentive to protect customer data, and that statutory action against privacy breaches was unnecessary".

This quarter Javelin Research found that about 1 out of 3 consumers would "discontinue or reduce their patronage post-breach" following a breach. However, not allowing someone to cancel their accounts shouldn't really qualify… if you'd like to understand how to undertake a cyber-threat planning exercise, just drop us a note (here).

Pass federal privacy, then disband the enforcers?

Woefully overdue federal privacy legislation took effect last quarter. Then we learned that this quarter, budget cuts will disband the Office of the Australian Information Commissioner (OAIC). Did anyone else connect those dots?

The Privacy Act finally gave the OAIC 'teeth' to enforce the obvious – which was the need to hold organisations accountable to protect your and my private data from loss and exploitation. Something that has been in place in many western countries including the UK and US. In an era where data and privacy breaches are happening weekly, this legislation was sensible. Now it seems we're disbanding the 'police' before they got a chance to enforce that law.

At least Victoria is making positive strides, with new legislation that combines the powers to drive reforms in both information security and privacy principles. Drop us a note here if you'd like to understand the practical implications that these changes may have to your organisation.

Is flexibility the answer?

How is your team placed to manage the range of threats that many organisations face in today's digital age? We've found that sometimes maintaining a permanent team with the skill depth required to proactively manage cyber security can be challenging, time consuming and expensive. With the introduction of our new business unit, Trusted**Impact** People, we've introduced a flexible contracting model which gives our clients access to high calibre niche security contractors who can augment your team on a flexible basis. Drop us a note (here) if you'd like to explore how this approach might give you the flexibility you need.

Mergers & Acquisitions – due diligence in the digital age

A few years ago we spoke with several investment bankers about the impact that cyber-risk had on an acquisition's or merger's valuation. We found that most due diligence teams (typically experts from finance, accounting, consulting, and legal firms) were good at assessing profitability and synergies of a merger or acquisition. Yet little, if any attention was paid to the security posture of the organisation under scrutiny.

We've been fortunate to have assisted several organisations consider these type of issues, and were pleased to hear that the well-known private equity firm KKR, has introduced a 'cyber risk score' to its assessment of companies in its portfolio.

Don't watch your cloud blow away

With a little marketing creativity, anyone can portray themselves as a solid cloud company. Indeed, the attraction of outsourcing a difficult headache to someone else is always appealing. But this quarter we saw another real example that helps bring "likelihood and consequence" into practical experience:

"*Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in a [sic] irreversible position both financially and in terms of on going credibility"*

It seems the company was using a sound 'cloud platform' (Amazon Web Service), but lost control of its 'control panel' as discussed here. **Key lesson #1**: do not expose important "control panels" to the internet, or at least without very strong controls behind it. We see this happen way too often from the hundreds of 'penetration tests' we conduct. **Key lesson #2:** Don't forget to think about not only what's going into the cloud (value of the data), but also assess whether the cloud company has the skills and resources to protect your data's availability, integrity and perhaps confidentiality. If you'd like help to understand the major issues, just drop us a note here.

Movin' on up

Please update your address books. Next quarter, our Melbourne office will be relocating to 9/22 Albert Road, South Melbourne. All other contact details remain the same. Come visit us if you're in the neighbourhood!

Thanks for investing the time to catch up with us. Also, don't hesitate 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