First quarter update
March 2014

This quarter is clearly the 'quarter of confusion'. The global and local economic outlook is varied with conflicting statistics abound. 96% of Crimean's vote to become part of Russia but the West rejects the vote as illegal. And a humorous cartoon poses, which aircraft is better to elude detection? A 65 foot long military stealth fighter, or a 209 foot long commercial airliner? Thus, one message seems clear: in a state of confusion, it's often best to keep focus and get on with business.

Is anyone outside of the industry worried about Privacy?

Newly enacted privacy laws took effect this month. The industry's still waiting to see if Canberra will jump into action or merely sit on the sidelines and watch. Only time will tell, but there doesn't seem to be a lack of opportunity for the AOIC to show its new teeth. For example, the criticality of private data is no more evident than in the Asylum seeker breach, where lives may be at risk because of the breach. Albeit, the recent ruling of a meagre $10,200 fine for Telstra's exposure implies the AOIC is still trying to grow its baby teeth. Particularly since that fine represents 0.000096% percent of Telstra's 2013's earnings.

Is XP's 'end of life', cybercrime's 'beginning of life'?

It's a whole new world of opportunity for cyber criminals when Microsoft stops supporting Windows XP on April 8th. In the last 5 years alone, there've been 336 published security vulnerabilities in Win XP, and 95% of those were HIGH severity issues. This might lead one to think the end of XP is a good thing for security, but keep in mind that 30% of the world's desktops run XP and 80% of large organisations run XP. So, while Microsoft may be ending its support and regular vulnerability fixes in a matter of weeks, it will be months, if not years, before XP leaves the industry. What this means is a huge number of vulnerable, and now unsupported, computers in operation (and possibly holding your information) for a long time to come!

Those big numbers imply that malware will find a fresh new home, botnets will become larger and stronger for potential "Denial of Service" attacks, and large corporate and government organisations will face a much greater security challenge until the systems are upgraded. For example, now the period of time between the release of a security patch and when it's upgraded goes from a "Day 1" risk to a "Day Infinity" risk. The issue is important and deserves due consideration. The Australian Signals Directorate's latest cyber intrusion mitigation's strategies succinctly notes: "Avoid Windows XP".

Target saw the writing on the wall too…

Last quarter we learned of the credit and debit card breach at Target in the US. This quarter we see some real examples of the impact. Sales transaction counts were down 5.5% - a steeper decline then when the US was in the midst of the Global Financial Crisis in 2008. Two banking Associations estimate it cost more than $200 million for banks to reissue cards, and the company's Chief Information Officer fell on her sword. Perhaps that's because Target purportedly knew of the issue and ignored warnings? The risk is real, ignoring it won't make it go away.

Changing behaviour

In the 1990's Business Process Reengineering (BPR) was a hot management topic. But over time, BPR thought-leaders quickly realised that changing workflows and business processes was the easy part. People had to also change what they did and how they did it – that was the hard part. Changing behaviour is one of those 'touchy feely' subjects which is about influencing someone's beliefs, attitudes and motivations.

Information security faces the same challenge in today's world. It's not just about placing posters around the company. If any organisation is really going to improve its risk posture, it'll have to address the fundamental issues of employee awareness and cultural change. However, the two disciplines are unique and require different skillsets.

This point was reinforced by several surveys we saw this quarter. One found that a one-quarter of workers do not think data security is their responsibility. Another revealed that senior managers are the biggest offenders of putting their companies at risk of a data breach. And yet another more found 63% sent sensitive work documents from a personal email address and 71% were under the impression that the company approved of that practice. It's clear that an investment made towards raising awareness and behaviour change is prudent.

"A habit is a choice that we deliberately make at some point, and then stop thinking about, but continue doing, often every day." (Charles Duhigg). That's why we've partnered with a change management firm to build a powerful program that addresses the core issues of information security in conjunction with behaviour change. Drop us a note (here), if you'd like to learn more about this exciting new initiative.

Same objective - different business unit: TrustedImpact - People

In the last six years, we've been fortunate to have performed hundreds of successful projects. The majority of our clients know us as a firm that provides them with insight-based projects that provide them with a clear outcome or deliverable for a simple fixed cost. Our formal quality and review processes ensure that different perspectives are considered and projects leverage experienced professionals with complementary, yet different, strengths.

However, we've found that some clients want to engage with us differently. Sometimes they want to have an experienced security expert to operate as part of their team. They want to manage the effort on a contract basis and it's typically about augmenting their team with unique skills. In addition, individual contractors often operate in isolation. We're working on the specifics of this new business unit, but look to create a tightly connected 'community' of like-minded security experts who can also see broader industry opportunities that it provides. If you're keen to be involved or want to learn more, just drop us a note (here).

Making your own luck…

If you've been with us for a while, you'll know that we often try to finish the quarter's insight with something out of the ordinary. "5 Things Super Lucky People Do" grabbed our attention this quarter. The 'Luck of the Irish' is an American phrase from the 1800's. "Intolerant Americans figured the Irish people weren't smart enough to find gold, and blamed their success on being lucky rather than skilled… The truth is that seemingly lucky people are opportunists. They do things that allow them to take advantage of the world around them." We hope that it sparks some constructive thought.

Many thanks for investing the time to catch up with us.

Also, feel free to pass this along to anyone who might find this of interest (or they can subscribe 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