It's summertime in the Southern hemisphere and the holiday season is just around the corner. The end of the year is often a good time for reflection, so hopefully this quarter's update will provide you with some ideas on how to make 2014 even better.

Most important, we'd like to thank you for being a friend, colleague, or valued client (or all the above!), and hope that you have an inspiring holiday season filled with family, friends and fellowship!

A very ~~merry~~ digital Christmas

The Australian National Retail Association just released figures showing six months of consecutive retail gains leading to Christmas. Cyber-Monday shopping results saw sales rocketing 'at a torrid pace' over last year, and mobile devices accounted for nearly one-third of that traffic. Exceptional statistics to support the great power of the 'Digital Age."

But as Voltaire (and others) said, 'with great power comes great responsibility'… well, at least in our words, the great power of the digital age should be met with the great responsibility to ensure your organisation's digital strategy considers information security.

Witchery (aka Country Road) just learned this lesson when its mobile APP was found to let customers view and EDIT each other's personal information. We understand a spokesperson said "*a small problem has been identified by our third party provider and is being fixed*".

Small problem? Let's switch gears quickly. If you remotely believe the statistics that 1 in 4 Australian's would stop doing business with a retailer after a security breach, you might not consider it to be a small problem. Or similarly if you believe Harvard Business Review's "Net Promoter Score" article that the ONLY number you need to grow is about loyalty, it may not be a small problem. The previous survey also found that 16% of Australian's would tell friends and family NOT to do business with the breached company… in the Digital Age security is no longer a nuance and cost, but a differentiator and competitive advantage.

If the previous statistics are only half right, it would be a prudent business decision to take a strong front-foot approach. Last year we highlighted the value of 'cyber-incident planning' ("Lessons from the front line").

The Witchery spokesperson also said the problem was from a third-party provider… consider our old whitepaper on 'have you outsourced your reputation to someone who doesn't care", or refer to a past issue on how to better manage the risk of 3rd party providers (titled "repeat… don't outsource your reputation"), if you'd like some ideas.

Finally, don't forget that in March next year, Federal Law Reform means the Commissioner can now 'seek civil penalties in the case of serious or repeated breaches of privacy'. With the Law Reform, organisations maintain responsibility for outsourced activities. We'll leave it to you to connect those dots. We're planning on organising a 'panel discussion' on the issues and opportunities with Privacy Reform sometime early in the year. Drop us a note here if you'd like us to send you an invitation.

Escalating likelihoods & consequences… or, the question you hope your boss never has to answer

Has your organisation ever experienced pressure to roll-out an important IT system to meet challenging time constraints? Hard to believe, right? Nearly all organisations we know face this challenge. It generally involves assessing the trade-offs, and potential likelihoods and consequences. Often those decisions are based on past or 'traditional business' experience, and therein often lies a problem - business in the digital age is fundamentally different from doing business in a traditional 'bricks and mortar' business.

A little more than a decade ago, eBusiness was a new term and online was more of a PowerPoint slide concept than a reality. Cyber security wasn't even a term and 'speed to [the online] market' took precedence over all other criteria. But the world has changed dramatically in that short period of time.

With a singular focus in information security, we've gained a unique perspective across many industries, clients and projects. Simply put, the risk (both likelihoods and consequences) of doing business in the digital age has changed and decision-making should reflect this evolving landscape.

The US Secretary of Health and Human Services learned this painful lesson this quarter. A simple search reinforces the increased likelihoods and consequences of not considering basic security issues with important online systems. Things get uncomfortable when politicians start making comments like:

"You accepted a risk on behalf of every person that used this computer that put their personal and financial information at risk because you did not even have the most basic 'end-to-end' test on security of this system"

As a footnote, we also learned that the IT chief responsible for the Obamacare site announced he was leaving. Another practical consequence in today's digital era.

Constructive 'exposure'?

A mature information security program requires a lot of important elements to come together including; executive sponsorship, organisational commitment, financial backing and lots of hard work.

Sometimes it takes the exposure of an issue to reinvigorate an organisation's focus in security. Some happen from unfortunate events. For example, having a publicly exposed data breach that impacts an organisation's stakeholders and customers.

On the other hand, a more constructive approach came out last month when the Victorian Auditor-General's Office (VAGO) released an audit report that examined 11 public sector agencies in regards to information security. As one might imagine, the specific issues that VAGO found varied dramatically between agencies. But in the aggregate, it was clear that additional awareness, funding and management attention is necessary.

We were extremely pleased to have assisted VAGO with this audit and have high hopes that it will provide constructive exposure to reinvigorate many of the existing programs already underway at these agencies.

When size doesn't matter…

This quarter saw a lot of publicity about the risk small business face against cyber-attack. There were several mainstream articles here, here and here if you want to pass along this information to colleagues or friends who work in small organisations. A little awareness can make the difference between being a success or a statistic.

Finishing the year with a smile…

We thought you might enjoy a bit of levity to finish off the year. While there's a whole lot of truth in these warning signs, Ray Pompon put together a great list for you to consider as you build your 2014 security program. Also, don't miss the great 'animated gif' of Jim Carey illustrating that apparently the world's population spends 500,000 hours a day typing passwords and other internet security codes!?!

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