Welcome to Trusted Impact's quarterly newsletter for the third quarter in 2010. We appreciate you taking the time to read it and hope it provides you with some value in return.

Who would have thought?

Time and again history has been proven a poor predictor of the future. This quarter we've seen plenty of examples – whether it's the hung Parliament in Canberra or a second try at a AFL Grand Final... who would have thought?

As a close analogy, it's easy for executives to use a similar historical approach when it comes to information security (haven't had a breach before, why worry about it now?). Unfortunately, the statistics show that in information security, the landscape of business and associated threats have fundamentally changed in the past few years. Let's look at some hard facts:

- Just last week, the size of the 'digital universe' reached more than one "*zettabyte". (that's one billion, terabytes!?)*. IDC and EMC collaborated to develop some very interesting information (here) that illustrates the exponential growth of the "digital universe'. What portion of that one zettabyte could be considered highly sensitive, or monetised by criminals? Even if it's a minute fraction, it's still a very large number.

- That information, combined with five billion 'internet-connected devices', and the very high internet adoption rate (+70% for Australia), demonstrates that electronic information either IS, or VERY SOON WILL BE a fundamental part of Australian business success. The information age is now squarely upon us and your business landscape has changed – the facts are irrefutable and should be considered for planning.

- Unfortunately evidence suggests more (simple things) can be done. Sophos found that 81% of corporate endpoints failed basic security tests: They either lacked Microsoft security patches, client firewalls were disabled, or endpoint security software updates were missed!

With the median cost of US$3.8 million per annum for a data breach (estimated from detailed analysis of 45 breached organisations), it's really hard to understand why organisations consider the past as any reliable indicator of information security risk.

Whether it is a simple 'Health Check' or Vulnerability Assessment, it's time to apply a duty of care to protect your reputation (and balance sheet) from the likelihood of a severe data breach.

More enlightening social media statistics…

As we discussed in our last newsletter, the momentum of social media continues to grow. We received a considerable amount of '*thanks for the interesting information*', so thought we'd highlight a thought provoking video which poses the question "Is Social Media a Fad... or The Biggest Shift Since The Industrial Revolution?" It reinforces the reality of social media as an unstoppable trend that will also change the overall landscape of business. It's here to stay and the worst thing you could do is

hope it's a passing fad. At a minimum, employing some of the 'basics' doesn't require significant cost or effort – here are some good tips on how you can write a Social Media Security Policy. Also, a simple, but elegant policy was found at the Australian Broadcasting Corporation (many thanks to our friend Karina for highlighting). Simply put... an ounce of prevention is worth a pound of cure!

Rethink how you handle sensitive data...

There have been some interesting articles that highlight a number of 'new threat vectors' that (at least according to the news), surprises many businesses. For example, 'nearly every digital copier built since 2002 contains a hard drive... that stores an image of every document copied, scanned or emailed by the machine' (Digital Photocopiers Loaded With Secrets).

This issue hit close to home when one of our team stood in line to get their shiny new iPhone 4 during its new release in Australia. It seems that to expedite the purchase and activation process, queued customers were kindly asked to provide a credit card and photo ID so that photocopies could be made (or leave the queue because they could not be processed). The store personnel were well intentioned and our team member was assured all paper copies would be disposed properly... But it really makes one wonder whether Albert Gonzales and his mates "residing in or near Russia" might find access to that copier hard drive of interest?

On a different but related note, the proliferation of 'smart mobiles' over the last few years is also a new concern worthy of some thoughtful consideration. An unfortunate situation (located here – thank you for pointing it out Alex), highlights the simple fact that all hard drives – whether they be in computers, laptops, "tablets", or now SMART PHONES, do not actually erase data.

While it can be argued that the likelihood of someone reconstructing your CEO's iPhone hard drive may be low, the potential impact to the organisation could be high for many organisations, depending on what its senior executive are texting and emailing to each others' smart phones. We've seen some well defined processes on how to destroy data on computer hard drives, but infrequently find any relevance to these other 'hard drives'. Consider extending the hard drive destruction policy to other relevant threats. It's not too hard or costly if you're thinking about where sensitive data may reside. If you'd like to discuss the first step of a 'data-focused security strategy' we've got direct experience with Australia's leading organisations – just drop us a note here.

Thanks again for reading this quarter's newsletter. Please don't hesitate to send us a note with any comments or observations – we value your input.

Kind Regards,

TrustedImpact

Helping you understand, prioritise, and secure sensitive information.

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
and its **guaranteed** – we will deliver, full stop.