Trusted Impact Quarterly Update – Q2, 2013

As cold winter temperatures descend on Australia, the information security industry continues to run red hot.

This quarter Big Brother was ‘outed’ and now the rest of the world’s population knows what many industry professionals already knew – that most first world governments have been capturing everything from telephone calls to Facebook status updates. One recent article calculated that the GCHQ (Britain’s spy agency), is capturing 21 petabytes each day (that’s 21 with 15 zero’s), or just under 250 Gigabytes - every second, of every minute, of every hour, every day. Now that’s ‘BIG data’!

The long-term political implications of this ‘privacy versus secrecy’ debate are unclear, so we thought we’d keep focused on sending you thoughts and considerations that will help your organisation face the practical information security risks you face today. While nation-state cyber-risks sit on one end of the spectrum, try not to forget the other end – large scale practical threats that most organisations face on a daily basis simply trying to maintain the confidentiality, integrity and availability of their organisation’s sensitive information.

A breach is inevitable – becoming a headline doesn’t have to be

Early this quarter, the world experienced an awful terrorist bombing during the Boston Marathon. A Boston-based organisation that one of our Principals’ worked with wrote an excellent, practical article about the connection between a smooth emergency response and proactive crisis planning (note the good list of questions in the article). Boston’s response was indeed impressive – thanks to a little foresight and planning.

In parallel, statistics show that your organisation has even greater chances of experiencing a data breach. While a few organisations have considered the technical aspects of how to recover from an incident, fewer have considered how to manage the business implications of a data breach – particularly if the breach became public.

One other related data point is that in the near future, Australia will face mandatory data breach notification laws.

The writing on the wall from these disparate items is simple. A data breach is statistically inevitable – mandatory notification will be required soon – you really need to plan how your organisation would respond to a data breach. A poor response can often be worse than the actual breach itself.

We’ve been fortunate to help several organisations define and clarify their data breach crisis management approaches. Key considerations not only include the technical aspect, but to be effective, it must be interwoven into the organisation’s existing crisis management processes and involve disparate groups that historically haven’t worked together in this context. Drop us a note here if you’d like to learn more.

I didn’t do it…

QUESTION: What do stolen blueprints for the new ASIO headquarters building, a $4.9 Billion lawsuit in the US, and local (confidential) Australian retail organisation’s network compromise, all have in common?

ANSWER: *3rd party business partners were the source of the compromise or breach*.

And whose reputation or financial statement took the hit for the loss (we’ll let you answer that one)? In rare cases, there may be grounds to recover financial losses, but the broad topic of information security is woefully silent in the vast majority of partner or supplier contracts.

Success in today’s interconnected world means you MUST collaborate and exchange sensitive data with a diverse range of business partners. Partners can be resellers of your products or outsourcers for call centres or your IT. They can also be performing Business Process Outsourcing in areas such as Human Resources or Payroll, and can be Professional Service firms such as lawyers and accountants.

These business partnerships are a business necessity, but to assume that the responsibility to protect against a data breach and the resulting fallout of a breach resides with the third party is both naïve and dangerous.

Sifting through the company's Accounts Payables ledger for an exhaustive list of third parties can be an overwhelming first step. However, we think the 20:80 rule is a more practical approach to consider – in other words, what 20% of your third parties relate to 80% of the risk that your organisation faces?

We recently published a simple one page framework [here] that provides some high level guidance on an approach your organisation should consider. Each company is different, but it's very likely that you have a few key business partners that are the source of a considerable level of risk to your brand and reputation. We'd be thrilled to talk to you about putting together a proactive, practical program that can start to mitigate this fast growing risk – just drop us a note here if you'd like us to give you a call.

Don't forget the basics

It's easy to be distracted by the interesting stories of cyber-warfare in the new digitally connected era [an exceptional wired magazine article here]. But try not to forget it's not just about countries and large companies - 67% of breaches happen in companies with less than 100 employees and that 78% used methods requiring low or very low skills (Verizon).

Leadership in the digitally connected age

The other day we were asked "what's the ONE thing a Board member or CEO can do to improve security in their organisation"? While we could draft a long list, we frequently run into glaring examples where leaders simply forgot to LEAD BY EXAMPLE…

For example, we cringed when the publicly-listed company CEO had their personal assistant bypass the advice of the CIO and place all of their documents into Dropbox for access to a number of his devices (a good idea, poorly executed). Or the other example where the Sales GM demanded that the company's website never be taken down to update the software against security vulnerabilities (yes, they also had the ability to hot swap the site).

Leadership in the digitally connected age requires education and awareness – often at the most senior levels. If you'd like to discuss how we might be able to assist with this challenge, just drop us a note here.

Tweet with us

Keep an eye on key industry events as they happen. Nothing is faster than twitter – join us here.

Looking for the best of the best!

If great clients, interesting work, exceptional pay, and a flexible work environment sound appealing, drop us a note or your CV (here) for a confidential chat. We're looking for well-connected professionals with 10+ years of experience - technical guru's and creative thinkers who can solve practical business problems.

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

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 it's **guaranteed** – we will deliver, full stop.