Here are a few points of interest we've been working on this quarter that may also be relevant to your business.

Test your "APP" before someone else does

Your company's Apple or Android "APP" (aka, iPhone, iPad, Smartphone, Tablet) is simply a small 'web application' or mini internet site (roughly speaking). If that APP only presents simple publicly available information, skip to the next topic. But if it interacts with your organisation's transactional, back-end systems or deals with sensitive information, give us a call. A new Imperva study found traditional web applications experience '**one automated attack every two minutes**' – even if those stats are slightly close, you can be assured someone will test your APP to exploit your back-end systems.

We understand we're the ONLY company with LOCAL experience Security Testing APP's with leading LOCAL organisations. If the Government refuses to send data offshore, you may also want to keep your confidential APP testing onshore too. And if you want someone who has 'been there / done that' so that they can hit the ground running with experience, send us an email. We'd be happy to share our unique, proprietary approach.

The simple business math of a data breach

"26% of Australians would no longer do business with a bank, a credit card company or a retailer that had a security breach resulting in their personal information potentially being stolen." *(SailPoint Market Pulse Survey 2011 – other interesting findings here)*

Let's wildly assume that only HALF of that number is correct (i.e., 13% to be wildly conservative). Simply multiply that number times your organisation's earnings before taxes. Then assume you only lose those customers for one year (and they don't tell their friends or stay away) and assume all your costs are variable – highly unlikely, but very conservative just to make the point… What does that equal for your organisation?

Usually it's a VERY big number. In one organisation we know well, that's a CONSERVATIVE **$50M+ impact** to their bottom line from a data breach. Perhaps the headline (at least for that organisation) should have been "you will lose more than $50 million straight from your bottom line if you have a data breach." Granted, we've got "voluntary notification" laws so no one in their right mind would tell anyone. You can "hope" that a breach doesn't hit the headlines… but we've found hope is not a very reliable strategy for success. Give us a call if you want to discuss strategies to protect your bottom line from an impact of this magnitude.

A sign of the times? Identity protection laws with razor teeth

This month, a bill was introduced to the US Senate which lays the foundation of a broad-reaching legislation to protect online personal information. **If your organisation is "a business entity engaging in commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more United States persons,**" the proposed bill is worth a quick read (here).

This bill (if passed into law) requires organisations to "implement a comprehensive personal data privacy and security program that includes **administrative, technical and physical safeguards** appropriate to the size and complexity of the business entity and the nature and scope of its activities".

Of particular note are the harsh penalties. Three separate parties (Federal AG, State AG and individual citizens) separately can seek civil penalties, injunctive actions and individual remedies EACH to $20 million per violation!?!

We recognise it's highly unlikely that penalties of that magnitude would be introduced in Australia. However, it does provide a comprehensive foundation for a logical 'import' of some degree to Australian shores. A stitch in time saves nine… when was the last time you thought about this type of risk or even performed a simple health check of your security posture?

Peering through the fog of the "cloud"

The Cloud's a hot topic. And because of it, there's also an onslaught of sales rhetoric and confusion when it comes to understanding the key pros and cons from a risk or security perspective.

We typically believe it's all about the type of data (and use) that is going into the cloud and thus, generally depends on each client's situation. Nonetheless, we get asked a lot of questions and we thought we would help by highlighting a few good sources of information that can help you with the issue if you are considering the cloud.

The first is from the folks at "Tier-3" who created a well written executive-level overview worthy a quick read (found here). On the other end of the scale is an extremely comprehensive framework from Europe that was created by the European Network and Information Security Agency (found here).

We're looking for the cream of the crop

Life is just too short to merely 'show up to work'. Do you ever feel that way in your current role? Do you feel like a dispensable cog in an enormous engine? Are you undervalued? Do you want to drive your security career, or have someone else drive it for you?

If great clients, impressive peers, interesting work, exceptional rewards, and extreme flexibility sound interesting to you, drop us a note or your CV (here) for a confidential chat. We're looking for well-connected consulting pro's with more than 10 years of experience. Creative problem-solvers who have experience translating security expertise to resolve practical business problems.

Thanks for taking the time read our newsletter - don't hesitate to send us a note with any comments or observations – we'd like to hear from you.

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.