Welcome to our first quarterly newsletter 2011. We appreciate you taking the time to read it and hope it provides you with some interesting thoughts in return.

The media's been running hot with high profile security incidents this quarter! Of particular interest to many clients is the unfortunate lack of clarity around the RSA security breach. We've heard lots of questions about trying to understand the practical implications on a company-by company basis. To assist, the folks at Securosis wrote a pretty good summary of the key issues (here), in case you hadn't already seen it. Some additional perspectives we hope is of interest include:

Perforating the "perimeter"

You're likely to have heard of Open Group's Jericho Forum comment a few years back that stated:

*"The **explosion in business collaboration and commerce on the Web** means that **today's traditional approaches to securing a network boundary are at best flawed,** and at worst ineffective."*

This became even more relevant with the recent release of Apple's innovative "Personal Hotspot" functionality that provides "three times" the opportunity to bypass the traditional business perimeter.

This is just one more example where a "data-focused" security strategy is inevitable for any organisation that collects sensitive information. The world has changed and it's time for the old security paradigm to change with it. The facts are too plain to dismiss;

1. **It's too easy to "accidentally" lose sensitive data** that can harm your reputation and business. Without a specific focus on protecting 'sensitive data', it readily proliferates outside your traditional office walls or secure network perimeter.

2. **People are motivated to take your sensitive data**. Your sensitive data is 'monetised' very easily these days.

3. **Traditional business processes rarely segregate the sensitive data**. This often means that sensitive information is scattered across the entire organisation – you can only protect or monitor what you are aware of.

A **data-focused approach** to security may be tough to get your arms around, but the facts demonstrate the likelihood of a breach is greater than you may have realised. Consider at least the first step – what data is sensitive, and where does it reside – then you can make practical steps towards minimising the likelihood of its loss... and its related business impact. Drop us a quick email (here) if you'd like to better understand the implications to your organisation.

Are you still relevant to the business?

We think security professionals should ask themselves that question every quarter. It was recently highlighted when we helped a client understand the implications of using iPads for its Board and senior executives. This audience is often the most demanding (in terms of dictating use, openness, flexibility and functionality), they're also likely to be less experienced understanding the risks they may face. The "new model" of enabling the business with 'eyes open' involves simply articulating the

trade-offs to find a balance between an open flexibility and a secure, but unusable device. Give us a call if you'd like to see or discuss the framework for assessing the trade-offs and options.

The undoing of corporate IT infrastructures?

A few short years ago (2003), there was discussion that PDA's would be the next major "threat vector" to Corporate infrastructures. Recently the smartphone/tablet "App Stores" were touted in a similar fashion.

Fortunately the PDA threat was overstated, but it's likely that the App Store threat is not. There's little doubt these devices will play an important role in business innovation. Some of our friends at CVP Customer Value Performance are about to release a Pulse Report ™ that identifies the take up of mobile applications for sales innovation in banking (contact us here if you'd like more information when available). They kindly asked us to provide some insight on the security issues…

We're all about facilitating business innovate and growth, but with 'eyes open.' Some of the 'simple basics' for consideration as you may be pondering your own company's approach to this exploding market opportunity include:

- Smartphones/Tablets are much more likely to be lost or stolen – consider an architecture that ensures no transactional or sensitive information is stored on a device.
- Public WIFI is great, but it's easy to intercept, steal and modify the transmission of data if unencrypted. One of our clients configured their devices to disallow WIFI and use the company's VPN and infrastructure to achieve at least a minimum level of filtering.
- Understanding the technical interactions between the various "layers" of hardware, operating systems, and an application is complex, but important if the application is going to be used for anything with sensitive information.
- Consider ways for users to verify your application is installed from a trusted source, and finally,
- Since ongoing issues will arise, assess reliable methods for updating the application and notifying users if security updates are required.

Don't hesitate to send us a note with any comments or observations – we'd value your thoughts.

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.