(Please click here if you are having trouble viewing this email)

Don't be a Kevin…

Call us crazy, but we find the political changes in Canberra an interesting corollary to the information security industry. Although the change occurred quickly, the telltale signs have been there for a while. This point was also made in an interesting article about "Change Blindness: Can You See the Changes in Your Industry?" (BNET Australia). It's premise is that organisations often can't or won't see fundamental change happening around them to react quickly enough before it's too late.

What does all of this have to do with information security? We sometimes hear comments like "We've never put much focus on sensitive data in the past and nothing's happened... why should we worry about it now? ... Isn't it all just "Fear, Uncertainty and Doubt" or a costly insurance policy?"

From our view – **for many organisations the world has changed** and the facts are too obvious to dismiss;

1. **It's now way 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. For example, stolen or lost laptops are the largest single source of data breaches – do you know if there's sensitive information on your laptops?

2. **People are now motivated to take your sensitive data**. Your sensitive data can be 'monetised' very easily these days. Australia's credit card theft exceeds $150 million (6/09), and there's a clear financial reason why "identity theft" is the fastest growing crime in the world.

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.

Fight against change blindness. A **data-focused approach** to security may be tough to get your arms around, but the clear external facts show the likelihood of a breach is considerably greater than you may have realised.

We'd suggest you 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.

The greatest security risk today?

The press is 'running hot' about facebook and the range of social media security issues these days. We also see surveys touting the perils of social media and web 2.0 technologies as "the greatest security risk company's face today."

The “old school” approach would be to block access in an attempt to ‘enforce the perimeter’... we’d like to believe that we live and embrace the “new school” of information security, where it’s about facilitating business growth and innovation – with open eyes.

We also find it strange that most presentations we’ve seen on this topic look strikingly similar to those we saw 15 years ago when that “strange new World Wide Web thing” was new – and yet the web continues to transform virtually every aspect of our lives.

The only practical response to social media is to embrace the opportunities it offers, and proactively manage the risk. Why?

1. **Social media is pervasive**. For example, Fred Cavazza created an impressive ‘landscape’ of social media that highlights the pervasive and extensive nature of social media.
2. **The momentum is unstoppable**. With more than 400,000,000 active users (Feb 2010), if facebook were considered a country, it would be the 3rd most populous in the world (between India and the US).

It’s here to stay and the worst thing you could do is hope it’s a passing fad. We’d suggest embracing it for all that it can offer. For example, some interesting thoughts on how to embrace social media are presented by some close friends at 7Summits Agency. At a minimum, employing some of the ‘basics’ shouldn’t require significant cost or effort – for example, CSO Online provided some good tips on how you could write a Social Media Security Policy.

Departing thoughts…

How important are your wireless nodes? For some reason, we still see some organisations securing their wireless networks with WEP encryption. WEP (Wired Equivalent Privacy) is not only outdated, but can be compromised in a few minutes with readily available tools. If you transmit credit card data using WEP, you’ll soon be non-compliant with Payment Card Industry regulations.

In fact, we’d also suggest you consider how well you have deployed any updated wireless encryption (WPA/WPA2) technologies. Password strength is one vital consideration. For example, if you’d like to see how easy it might be to ‘listen in’ to easily obtain unauthorised access, just drop us a note (here) and we can help you understand if you’re at risk.

Thank you for taking the time to read this quarter’s newsletter, and don’t hesitate to send us a note with any comments or observations – we value your input.

Kind Regards,

TrustedImpact

We help enterprises 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.