

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



2010 has started with a bang. We're seeing lots of activity from innovative companies taking this opportunity to "accelerate out of the tight turns" of the previous 18 month economic situation (a sporting analogy difficult for us to miss as we drafted this overlooking the Melbourne Grand Prix!).

In particular, we are seeing two key business trends that you may want to consider for your organisation. The first is enabling market growth and improved customer self service, while the second is an increased emphasis on proactive information security.

The power to make or break innovation and growth

We're seeing a large number of innovative clients extending their capabilities beyond their enterprise with a range of approaches such as tighter integration with partners, open collaboration, and closer interaction with customers. But without the right approach to information security, this innovation and growth could be easily stifled, or put the organisation at considerable risk without the right perspective. For example:

Partners and Outsourcing: Do you have the right contractual measures, metrics or controls in place to manage the risk of your customer's data landing in the wrong hands – but with your organisation's reputation at risk? ["Have you outsourced your reputation to someone who doesn't care"](#) tries to provide some ideas on how to facilitate a stronger, more effective partnership.

M&A: The economy has also provided a range of opportunities for acquisitions. From our experience, accounting, venture capital, consulting, and legal experts can be good at assessing the profitability and potential synergies of a merger or acquisition. Yet little, if any, attention is paid to the security posture of the organisation under scrutiny – often with disastrous results. [Click here](#) if you'd like to get some ideas on things to consider in this situation.

Internet Self-Service: For some clients, growth has been facilitated by offering a greater level of 'self-service' and ability to transact services via their internet channel. As an enterprise moves closer to performing core business processes with its customers, the "risk landscape" may have shifted dramatically. Particularly, because this typically means that previously "internal-only, back-end," systems are now accessible via the internet. A quick [Vulnerability Assessment](#) can be a simple 'litmus test' to determine if there are more systemic issues to consider.

Proactive Security

We felt the recent article(s) about [Medicare](#) employees allegedly accessing inappropriate records was a 'good news story' since it demonstrated that Medicare has a level of proactive monitoring in place to minimise the loss of its sensitive data. ... this raises a question that many enterprises would likely find challenging to answer.

There are two key elements to the issue – the first is having a solid handle on the organisation's 'sensitive data'. Implementing an effective data-focused strategy can be hard, but it's a necessity since there are now viable market's to "monetise" your organisation's sensitive information.

The second element is a proactive 'monitoring and reporting strategy' in order to find the right 'balance' between cost and value when protecting your data from the "lift and shift" concern one of our best clients worries about.

Departing Notes...

Public Sector? Are you or someone you know in the public sector? Late last year, the Victorian Auditor General's office released a [report](#) that found *"The confidentiality of personal information... used by the public sector... can be, and has been easily compromised. ... the lack of effective oversight and coordination of information security practices strongly indicate that this phenomenon is widespread,"*

This was unfortunately corroborated this month by the [Western Australian Auditor General](#) that found *"agencies lacked comprehensive management, technical and physical controls over their laptops and portable storage devices to minimise the risk of them being lost or stolen and of sensitive information being accessed"*. Send us a [note](#) if you'd like to discuss the implications of this report on your organisation.

APRA regulated? Are you or someone you know supervised by the Australian Prudential Regulation Authority (APRA)? On February 1st, they released a new "Prudential Practice Guide" on the "Management of security risk in information and information technology" to *"target areas where APRA's ongoing supervisory activities continue to identify weaknesses"*. Send us a [note](#) if you'd like to discuss the implications of this guide ([PPG 234](#)) on your organisation.

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,



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.

Please feel free to forward this to any friends or colleagues who may find it useful.