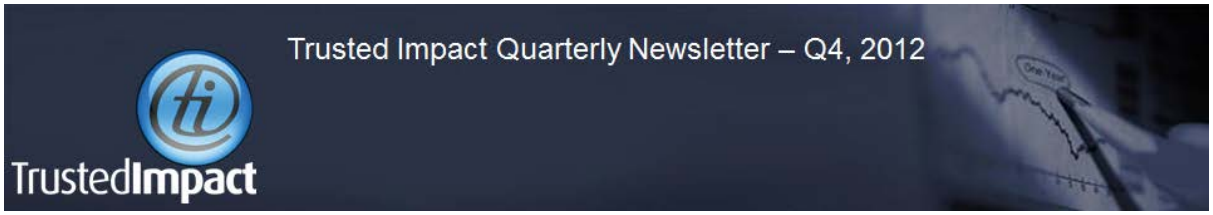

As another year comes speeding to the end, we'd like to thank you for being a friend, colleague, or valued client (or all the above!). But before we get too far into this quarter's summary, we would first like to wish you a spectacular, safe and secure New Year!

Common themes from the hacker road kill of 2012

We're in a privileged position where our singular focus in information security enables us to be exposed to a breadth of activity across small internet-based start-ups to large iconic Australian establishments. When one's focus is very narrow but spans across multiple industries, it enables us to see recurring patterns and consistent themes that most organisations singularly can't see.

For example, the other day the Macquarie University breach illustrated some consistent themes across a range of security incidents that we've been directly exposed to or that arise over and over again. We thought it might be useful to reflect on this experience and highlight some of the basics that seem to be missing. These include:

1) **Over reliance on third parties to protect the organisations' reputation**. In the previous breach/article a comment was "… *the site has only been operational for few weeks, and that it had engaged a third party to host and maintain it on the University's behalf*".

   In a different, but similar incident a comment was "*well… as a Gold Partner, you'd think they knew what they were doing*". Let's be very clear about what gold partner means: it means they sell lots of licences and are good at implementing the product. It does NOT mean they have any experience securing it from security threats. That point was further reinforced when Darren Arnott – one of our top Principals was quoted in the "Click Frenzy" ZDNet article here.

2) **Not knowing if there are new or changed files on your webserver**. In the Macquarie breach (hotlink above); the comment was "*the hackers also uploaded a [file]… to allow anyone… to interrogate the database at will*". Would your organisation know if it had new or changed files placed on its webservers?

3) **Exposed 'Administrative Panels'**. If only we had a dollar for every exposed administrative panel that we see from our testing experience… A good quote from the hacker in the Macquarie breach was "*When your Administration panel is accessible publicly, what do you think will happen? … anyone could have done it. It just took some investigating. Don't dub me as an elite hacker, because I simply am not*". Just drop us a note (here) if you'd like to explore alternative approaches.

4) **Out-dated / vulnerable software.** The Defence Signals Directorate maintains an excellent list of ways to mitigate against targeted cyber intrusions. Two of the top four strategies involve patching software. Automated programs trawl the internet every minute of every day to identify vulnerable software. We also see it over and over again in many of our "Penetration Tests." It's not very exciting and can be difficult to do, but maintaining up-to-date security is a no brainer if you want to protect your systems from intrusion.

The changing strategy of security – lessons from 2012

We helped several organisations with their security strategy during 2012. We thought it might be useful to highlight some of the key themes to provide you with some considerations during the upcoming year.

1) **Evolving to business-driven security model**. Just as the CIO's role has changed over time from needing to be a 'technology expert' to needing to be an 'innovation advisor and facilitator' to the business; so too is the shift occurring with information security.

   The security team must now facilitate business-driven and risk-based decisions to be understood by and chosen by 'the business' and rather than be an organisation that has responsibility for data protection or defines the rules of what can or cannot be done by frontline business units.

   The new mission for the security team is not to say 'no', but rather 'how'.

2. **Gaining a clearer focus on "data" or "information"**. The traditional 'perimeter' approach to protection is neither effective, nor prudent. Organisations that are custodians of its customer's valuable and sensitive information, must gain a greater clarity on what data is sensitive, focus on the key applications that process and store it, and protect the flow of this information inside and outside of the organisation. It's difficult for some organisations to segregate sensitive data from the traditional data flows – but the old 'homogenous' approach to data requires excessive investment and is practically flawed.

   This also extends beyond the enterprise to partners, customers, third parties and even "the cloud". Today, business innovation means open collaboration, direct interaction with customers, tighter integration with partners, and incorporating external talent and resources. Organisations cannot unconsciously outsource the protection of their reputation to external organisations that may not have the capability or maturity to protect it. Our extensive 'cloud security' experience might also assist – just give us a call.

3. **Developing incident response capability**. The skills, tools, expertise needed to detect, resolve and mitigate the impact of an inevitable data breach are unique and also require cross-functional coordination.

   Today, it's almost guaranteed that an organisation's systems will either be compromised and/or that its sensitive data will be breached at some point. When a breach occurs it requires cross-functional teamwork (e.g., business operations, legal, risk, public relations, senior management, etc.) to mitigate the negative impact. Drop us a note (here), if you'd like to talk about some practical 'cyber war gaming' (also reinforced by a recent McKinsey whitepaper).

4. **Maturing the organisation's security culture**. Business innovation demands sharing intellectual property, sensitive information, systems and infrastructure. When sensitive data is exchanged with third parties its confidentiality, integrity and availability is paramount.

   Decisions must reside with the people who perform these roles as a part of their daily jobs, rather than superficially controlled from a centralised team (often located deep in IT). This isn't merely about putting up posters or running training programs, but involves the very difficult challenge to change the ingrained culture of the organisation to consider and protect customer or sensitive data as an unconscious part of the daily routine. Drop us a note if you'd like to explore how to begin the initial steps of this challenging task.

Why be concerned? Privacy gets serious in 2013...

The Federal Government made some of the biggest changes to the Privacy Act at the end of this year. Now, civil penalties for serious breaches can be applied to BOTH Government agencies and private sector organisations.

Also in late breaking news this month, the Victorian Government announced it will create a new privacy and data protection office, combining both the State's Privacy Commissioner and Commissioner for Law Enforcement Data Security. This is an important move which will seriously strengthen the State's data security oversight.

Come tweet with us

We've seriously cranked up our commitment and ongoing activity on Twitter. We'd love to connect – join us here.

———

Thank you for reading our last quarterly update for 2012. We'd welcome your view so don't hesitate to send us a note with any comments. Best wishes for an exciting and prosperous 2013!

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.