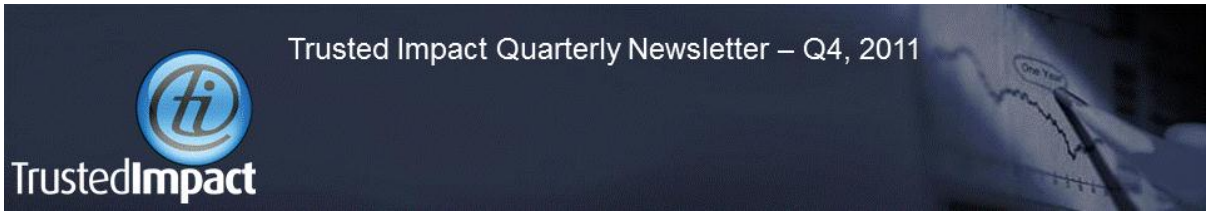


As the year quickly comes to a close, we'd like to thank you for being a friend, colleague, or valued client (or all the above!). We appreciate the opportunity to send you our thoughts and perspectives.

## Does your organisation suffer from 'inattentional blindness'?

A short, but interesting video of inattentional blindness is here. It's the "*failure to see visible and otherwise important things when one is focused on something else.*" When we saw a similar video, we wondered whether organisations might also have inattentional blindness when it comes to information security due to their necessary focus to achieve consistent quarterly results.

Although we're clearly biased, one might also suggest our singular focus in information security provides us with a perspective that some organisations might not see – in particular, the reality and increasing risk that an organisation's data can be easily monetized by individuals with little concern for your reputation, your customers sensitive data, or the cost you'd incur if you fell victim like Sony did earlier this year.

So if your organisation sees the internet as an important channel to your customers, or if you collect sensitive customer data, "WE SEE THE GORILLA" and want YOU to see it too (refer to previous video for that comment to make sense)!

Even data you may consider to be 'low value' can have a big impact. For example, the Epsilon breach highlighted the cost of a stolen email address. The simple cost of merely notifying 60 million customer's would have a tangible operational cost and impact on an organisation's bottom line. As a popular 'cloud service' this breach also highlights the risk of **THE CLOUD** without considering the value of data stored in it.

And before you think your organisation is too small to be on the radar, you may want to review a good article about the "5 reasons cybersecurity matters to small business" just published by zdnet.

## Cybercrime now $100 billion larger than the global black market for marijuana, cocaine and heroin?

Let that statistic sink in a bit... That's a very big number ON TOP of what most people would typically recognise as a very significant global problem. (Symantec report here). Cybersecurity received a fair amount of attention from different perspectives throughout the year.

For example, McKinsey & Co. (here) stressed that cybersecurity must be addressed at the most senior levels as a business issue (a shared philosophy that separates Trusted Impact from many in the industry). Their 'critical questions' are a good starting point.

This year also saw the US Government declaring cyber threats as an 'act of war' and Barack Obama declared it as "one of the most serious economic and national security challenges we face as a nation". The U.S. Securities and Exchange Commission also announced disclosure guidance regarding cybersecurity risks and incidents. And in Europe, the European Commission seeks to impose "massive data breach fines".

We're interested to see similar local concerns raised by State and Federal Government (see WA Auditor General report). Julia Gillard's recent "ministerial reshuffle" is believed to 'give sharper teeth to an upcoming cyber security white paper'. Perhaps Malcolm Turnbull or David Smorgan can provide some local insight as well (thanks to the new Stratfor breach).

The key messages?

1) Cybersecurity – it's big, it's real, and it's prudent for your organisation to consider what it means.
2) Regulatory bodies from all directions are recognising the importance of information security and are likely to ask you to demonstrate your security posture at some point in time in the near future

But resist the temptation to 'just lock everything down,' as this drives up compliance costs and restricts business growth. A better strategy is to find ways to **securely open** your systems and information for legitimate business while still 'keeping the bad guys out'. Of course, what may be the right answer for one company may not be right for another. If you'd like to discuss what might be the right fit for your organisation, just drop us a note here.

## Bricks and mortar thinking doesn't work in the internet age

Innovative organisations are leveraging the internet and its electronic "channels" (internet, smartphones, etc.) to gain strategic advantage (as a market innovator), drive cost savings (via lower overall transaction costs) and increase revenues (with greater market penetration).

But as traditional customer channels shift from outlet-based or call centre-based transactions to internet-based, online transactions, there's a major shift in RISK. Some of the key differences include;

- **Anonymity**: "On the internet, nobody knows you're a dog". Identity theft is the fastest growing crime in the world today, and is nurtured by the impersonal interaction that's an inherent part of the internet. Organisations need to be conscious of this shift to ensure appropriate "trust models" are established to protect important customer transactions while not overburdening the customer's ease of transaction.
- **5 billion customers on your doorstep - every minute of every hour of every day:** It's estimated there's over 5 billion internet users world-wide. The sheer magnitude of that number means that even if only 0.1% is keen to exploit your web footprint, that's TWO times the population of Australia! Online channels do not follow traditional rules - malicious activity happens anytime, anywhere and there's no customer service rep to manage things in the middle.
- **The automated nature of IT**. Malicious activity has become automated. This means the diversity, volume, speed and business impact of malicious activity is exponentially greater than traditional customer channels. But the challenge is to find ways to monitor exceptions or anomalies, rather than placing additional constraints on a customer's ability to transact with the organisation.

You may want to consider an electronic channel Threat Risk Assessment to gain insight on the impact this shift may mean to your organisation. Drop us a note (here) if you'd like to learn more.

## ...and don't forget the simple stuff...

Don't forget that MOST data breaches are NOT complex cyber threats. For example, Science Applications International Corp (SAIC) recently lost lots of sensitive data when computer backup tapes were stolen from a contractor's car.

We know an Australian IT company that maintains very sensitive data on behalf of their clients. It was announced to one of its customers that its data backup regime was performed well because an employee took home backup tapes each night to protect against the unlikely event of a system failure... sound slightly familiar?

While it's fair to note that Australia is less litigious than the U.S., SAIC now faces a **$4.9 Billion lawsuit**. In 2006, the US Department of Veterans Affairs lost one laptop and quickly settled a similar lawsuit for $20 Million (later recovered and determined to have not been accessed – one VERY expensive laptop)!!

## We're looking for the best of the best

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 professionals with 10+ years of experience - technical guru's and creative thinkers who can solve real business problems.

Thank you 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. Also, please feel free to pass this along to any colleagues (or they can subscribe here).

Kind Regards and Happy New Year,

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.