



Welcome to Trusted Impact's quarterly newsletter for the fourth quarter of 2010. We appreciate you taking the time to read it and hope it provides you with some interesting perspectives in return.

It's been a busy year, which was highlighted well by SC Magazine's recent article "[Stuxnet to Gonzalez to Snoop: The year in lists](#)". We won't steal their thunder – it's a good read if you've got a spare moment.

However, it would be tough to write a newsletter this quarter that didn't mention the significance of all the events surrounding WikiLeaks. There's been considerable press and no lack of polarised opinion, so we won't try to add to the confusion. Instead, we thought we'd offer a couple of 'lessons learned,' (thus far) from our point of view that may be relevant to you or your organisation.

WikiLeaks lesson #1 – “reputational loss” is tangible.

Confidence and trust are hard to gain, but easy to lose.

We often hear how information security (even a basic level) can be too hard to justify because of the “intangible nature” of protecting an organisation's reputation. However, “[in just a matter of hours, \[Julian Assange\] robbed shareholders of as much as \\$4 billion](#)” and plunged the Bank of America's share price to a 52-week low after it was rumoured that WikiLeaks might have detrimental information it was going to divulge.

Although we'd suggest our definition of 'sensitive information' is often different than much that's been published on WikiLeaks (e.g., opinionated observations versus specific customer data that may cause harm if lost and misused), it measurably demonstrates the potential impact of lost shareholder confidence.

Though often difficult to quantify, the reputational loss of this order-of-magnitude is difficult to ignore, and the investment needed to protect against the risk of lost sensitive information shouldn't be arbitrarily brushed aside just because it might not strictly align with traditional business case metrics.

WikiLeaks Lesson #2 – it's all about the data!

Your organisation's data is likely to be its most proprietary asset. Competitors can copy processes and buy the same equipment, but it's your data that is unique, and now, very valuable. Most organisations have never had to think about what data might be sensitive and where it may reside.

WikiLeaks highlights a simple fact that the likelihood of a data breach may be considerably greater than you may have realised. It's highlighted that:

1. **It's 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 motivated to take your sensitive data.** Your sensitive data can be "monetized" very easily these days. Australia's credit card theft exceeds \$150 million (6/09), and there's a simple financial reason why "identity theft" is the fastest growing crime in the world.
3. **Traditional business processes rarely segregate 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.

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. Drop us a note ([here](#)) if you'd like to understand how we've helped several organisations start on this journey.

We suspect that WikiLeaks and a range of the fundamental issues that it confronts will be with us for many years to come. It's elicited raging debates on both sides of the argument, so to finish our perspective on the topic, we thought it might be helpful to try to keep one's sense of humour with the following "oldie but goodie", [YouTube parody](#).

Thanks to you, it's been an outstanding year at Trusted Impact. We're fortunate to have had the opportunity to help some great organisations and even greater individuals inside those organisations during 2010. We hope you have a safe New Year and trust that 2011 will exceed all of your expectations.

Please don't hesitate to [send us a note](#) with any comments or observations – we'd value your thoughts.

Kind Regards,



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.