Welcome to the second quarter with Trusted**Impact**. Our aim's to distil the key issues from last quarter and keep it short, relevant and focused on important business issues pertinent to you and your organisation.

When the cloud goes dark

There is and will continue to be a lot of "hype" around Cloud Computing. There's little doubt the cloud is a great concept with great potential for many. However, this month's Wired Magazine highlights a practical reality. In short, the "[US] *Feds Tell Megaupload Users to Forget About Their Data*… and say they may shut down cloud-storage services without having to assist innocent customers in retrieving data lost in the process." While one might question the legitimacy of the New Zealand-based 'MegaUpload" service, low cost cloud options can be appealing to many business users. Legal and jurisdictional issues such as this example, bankruptcy, or commercial litigation are realistic, real-world risks (among others).

Another trend is becoming clear - we see many IT Departments risk of being 'disintermediated' in a few years. Business users can go directly to cloud providers without engaging with those 'difficult IT people with all their cumbersome security requirements'. The ease of engaging cloud providers directly by business users may overcome the traditional risk-based questions asked used by IT Departments to protect the organisation's data.

Awareness and insight is the key… therefore, you may want to consider a short, yet comprehensive program to understand these risks. Trusted**Impact**'s Ron Speed is the ONLY Cloud Security Alliance (CSA) Certified Instructor in the region, and Trusted**Impact** has partnered with the IT Training Company, to offer the Certificate of Cloud Security Knowledge (CCSK) training to promote the use of best practice security in Cloud Computing – click here for the latest training calendar.

Oh… and did you hear the new definition of C.L.O.U.D.? ("Can't Locate Our User Data")

"Only 15 minutes to teach an 11-year-old to carry out an SQL injection attack"?

That's a quote from a Forbes article "Now Anyone Can Hack A Website Thanks to Clever, Free Programs." Today, hacking is a viable 'work from home' choice in a world where global unemployment is rife. As a 'business'; hacking's start-up costs are low. Free, automated, easy-to-use tools are readily available, and your data can be pretty easily monetized. For example, do you think those poorly worded phishing emails are silly? Last year they returned an average of US$4,500 PER ATTACK to their creators [click for RSA stats]. In many second and third world countries, that's a very impressive annual salary.

As further noted in one of our recent whitepaper's, "*…it's very difficult to coordinate across countries and geographies with diverse laws, legal frameworks and policing bodies. If an online criminal operates from offshore, the chances of being caught or stopped become even less.*" While it's great news to see some progress with the recent international 'sting', we suspect it's only a 'drop in the bucket'.

From a related but different angle, yesterday's IT developer simply delivered web-based applications that; a) worked, at b) the lowest cost possible. It's simple economics: deliver agreed design and functionality for the lowest cost. Security was very rarely a consideration, and we can statistically demonstrate that fact from a baseline of hundreds of technical security tests conducted across large to small organisations.

The lesson? If you've never tested your internet-facing systems, you should. In fact, someone may already be doing it without your knowledge. It's now a fundamental duty-of-care consideration for senior managers. And if you haven't tested them recently, consider testing them again – in the last six months of 2011, ONE new software vulnerability was uncovered every TWO hours of EVERY day. Drop us a note here if you'd like to learn more about testing your systems.

Has your rush to innovate opened your internal systems to hackers?

Mobile websites and "apps" are being built at a frantic pace to allow customers to transact anywhere - anytime. Your new mobile website or company app is just like your traditional website; providing a new 'doorway' to your systems and customer databases.

ALL of our tests in this area have uncovered significant security vulnerabilities. The ticketing start-up Eventbrite learned the hard way when a bug in the iPad application didn't protect credit card data. Can you really afford NOT to test your mobile website or app? Drop us a note if you'd like to discuss our proprietary framework for testing mobile apps, or download our 'impact offering' here.

Keeping focus on the basics…

As your business evolves, it's easy to lose sight on the basic things that unravel many security programs. It's also easy to be distracted by interesting and emotive "Flame, Duqo, and Stuxnet" cyber-warfare stories. Your executive group needs to understand that with enough motivation, money and perseverance anyone can gain access to your data. But too often, it's the simple 'no brainers' that can open an organisation to immeasurable and reckless risk. For example, one of our consultants 'pwned' a company's international wire transfer system because of the simple re-use of passwords (LinkedIn's breach helped to reinforce that on an individual level?!).

We try to help our clients focus on the stuff the matters. Of course this means technical testing, but we also make sure other elements of a security approach are considered; such as operational security processes, incident management and detection capabilities, business continuity and disaster recovery, staff awareness and security culture and 3rd party / vendor management (to name a few). Keeping a focus on doing the basics well can be tedious, but have you ever seen a winning team that didn't do the basics like it was second nature?

Because many struggle with a holistic view, we've developed a few different "Health Check" approaches that apply simple but customised frameworks to prioritise the most urgent security issues, and gain the best return from their efforts. Drop us a note here if you'd like to see some of these frameworks or discuss these approaches.

14 lessons about getting what you want in life

One of our consultant's tripped across a good blog (here) with some of Benjamin Franklin's best quotes – just to change things up a bit we thought it might add a little inspiration with some "one liner's to live by", such as; "**Well done is better than well said**", or "**Never confuse motion with action**"... and, "**when you're finished changing, you're finished**". We hope the above link is a small, but worthy diversion to your hectic day.

Need help delivering the business perspective of security?

Senior executives are busy. They have business problems to solve and results to deliver. The "business perspective of security" can often be difficult to communicate to them effectively. We really like having those kinds of discussions – if an independent view, levering broad, fact-based, real-world experience from people who've lived those roles, would be helpful - just drop us a note here.

———

Many thanks for reading our quarterly update. We'd welcome any feedback – don't hesitate to send us a note with comments or observations. Also, feel free to pass this along to any colleagues (or they can subscribe here).

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.