Third quarter update September 2013

Spring's finally upon us. Canberra's busy with a bit of 'spring cleaning' as a new party takes over. We've even done a bit of our own spring cleaning and released an updated website this quarter. Check it out (here)… we're always trying to listen and learn, so we'd welcome any thoughts or ideas.

Don't forget the low skilled masses…

This quarter's seen a flood of revelations about just how deeply embedded Big Brother is into our digital lives. If we believe everything we've read this quarter, there are digital back doors in everything from our telephones to our electric toothbrushes (son of Stuxnet perhaps?). Indeed, the power the NSA (et al) have exercised is disconcerting - particularly with an apparent lack of significant 'checks and balances' to protect against abuse.

While an interesting topic, it can also be distracting. Putting the important issue of civil liberties aside for a moment, this quarter saw some important statistics to remind us that the 'scavenger' threat is real and growing. That is, groups or individuals seeking to monetise your data or exploit systems to their benefit. In particular:

1) **There's LOTS of people looking in your (internet) windows**. Cisco now thinks that in three years almost half the world's population will be on the internet. That's almost 3.5 billion users and 19 billion devices. If only a tiny fraction (eg 1%) wanted to break into that "window" and have a look around for something of value, it's a group larger than the entire population of the country. For the less-technical audience, that's not simply your company web storefront, but ALL your company's connections… even printers (remember 3 steps to total compromise – why Googles 86,000 indexed printers should have your IT team jumping?).

2) **There's LOTS of rocks lying close by to break into your (internet) windows**. CNBC wrote (You ain't seen nothing yet) about 'cyber-crime as a service' and the incredible ease for anyone to become a hacker with free, available, simple, automated tools. Need a little training to go along with those free tools? The latest RSA fraud report has an interesting section on 'Cybercrime U' – real, money-back guaranteed courses from avoiding detection to mule herding… most for around 2,500 Rubles (~$83 AUD)!

3) **The desire to break into your (internet) windows is rapidly rising**. IntelliHub highlights the seriousness of the global unemployment crisis. You remember the old saying, necessity is the mother of invention? In today's interconnected world, one doesn't need a whole lot of 'invention' if you find yourself unemployed, hungry, with access to cheap, simple tools and you live somewhere hard to get to by local law enforcement.

Or the sophisticated few…

Christopher Joye once again published some powerful insight on 'nation-state' threat facing the Australian Government. The 205% increase in the number of cyber attacks requiring 'heightened response' is alarming, but we suspect it's only a glimpse and is probably even higher.

We're not privy to the calculations, but it would reasonably only include the specific Government agencies being monitored. Remember the contractor that compromised the building plans of ASIO from last quarter's update?

This quarter it might be valuable to consider this situation from the opposite direction. In particular, if YOU are a supplier to a Government Agency, have you considered this threat? If you were asked how you protect their sensitive data, could you provide a reasonable response? Give us a call if that's a hard question to answer.

The common thread is threat

The specific threats you face are unique. They depend on your industry, business structure and should consider information or systems that can be exploited, compromised or monetized.

For example, a utility we know has a large external, contractor workforce; lots of quiet office/depot locations, and were reducing that workforce – they asked us to help assess the technical vulnerabilities from this practical threat – practical thinking.

In contrast, we know a government agency that had performed a number of "Penetration Tests" in a shotgun approach, but found it difficult to understand why it was so easy to access some highly sensitive data.

The message? Consider where you're spending your security dollars and try to align them to the practical threats and risks your organisation faces.

Big Data = Big Target?

Big data continues to be a hot topic this quarter. It should. It has great potential for innovative organisations. But with federal privacy laws coming into place March, next year (drop us a note if you'd like to discuss the practical side of that topic), it may be worthwhile posing a few simple questions to make sure your big data isn't a big target. For many organisations big data often means:

1) Lots of customers – Are ALL the customers of the company now in one convenient, single source? Hackers like this kind of 'bang for buck'.

2) Lots of information – Is EVERYTHING about the customer linked? Does the sum of the parts now mean you've got all 'identity data' in one place (eg, address, birth date, etc)? For example, can someone now give the bank everything they needed to gain access to your customer's bank account?

3) Lots of access – Does EVERYONE have access to it? Some organisations do a good job locking down their core production / internet systems. They're often relaxed when it's an 'internal / support' system like a data warehouse… easily copied, extracted, accessed, manipulated… that's what it's built for, right?

If your big data effort sounds a bit like the examples above, consider whether your protection is commensurate. Don't be a target for "SSNDOB" (Data Broker Giants Hacked by ID Theft Service).

KISS: Keep it simple…

It's easy to confuse in our industry and hard to keep it simple. The other day we read a pretty good, simple list of security fundamentals. Not only did we think it was elegant in its simplicity, it's typically what many security programs aren't doing. We hope it sparks some constructive thought.

Looking for the 'navy seals of security'!

If great clients, interesting work, exceptional pay, and a flexible work environment sound appealing, 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 practical business problems.

Thanks for investing the time to catch up with us. Also, feel free to pass this along to anyone who might find this of interest (or they can subscribe here).

Kind Regards,

TrustedImpact

Protecting Digital

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