Trusted Impact Quarterly Update – Q1, 2013

Cyprus banks are crumbling, Korea is a hotspot for ‘nukes’ of all sorts (traditional to electronic), and ‘Apple becomes average’ this quarter. One constant in this quarter of turmoil is the growing global threat for others to benefit by compromising your systems and your data… remain vigilant!

Sabre rattling can be distracting

This quarter we’ve been overwhelmed by the amount of ‘mainstream press’ (eg, New York Times, Washington Post, etc) fuelling the emotive angle behind the cyber cold-war. For example, the US Pentagon is increasing their ‘cyber command’ a factor of more than 5 times (900 to 4900 according to the Washington Post), and not to be outdone, New Zealand also announced a ‘Super-cyber Security Alliance’ with the UK. Even Singapore amended its legislation to take preemptive action against cyber-attacks – one of many countries that have done so in the last two years.

Without a doubt, one of the most thorough reports was published this quarter portraying the details of one of China’s cyber espionage units. If you like factual evidence, you’ll enjoy yourself with this report from Mandiant. However, as a balanced contrast James Andrew Lewis published a Washington Post article about the ‘Five myths about Chinese hackers’ that puts a number of key aspects into perspective. We noted his comment:

> *“The problem isn’t that the Chinese are so skilled; it’s that U.S. companies are so inept…”*

To be fair, it’s not just US companies that are ‘inept’, it’s a global and local issue – particularly for many medium or small companies. For example, the recent local ‘ransomware’ stories (good compilation of Australian stories here by SC Magazine) highlight that naiveté amongst smaller organisations is still is very prevalent. Having “a good antivirus program” against potential compromise is not only imprudent, it verges on silly.

So What? Unless you’re directly playing in that space, we think it’s pretty important not to get too distracted by this information – interesting as it may be. If a Government truly wants to gain access to your organisation’s data, it will likely have the skills, time and required investment to do so – either technically or through more traditional social engineering methods.

It’s the great masses of less sophisticated threat sources (ie, economic-driven, crime-driven, hactivist-driven, malicious-driven) that need vigilance to perform the boring things like patching your systems, and getting independent reviews of your system configurations or performing security testing. It’s also time that you start taking a data perspective – simple first steps are; what data is valuable (why would someone be motivated to take it), where does it reside (think about the stuff that’s outside of the typical ‘IT production systems’), and consider different ‘threat vectors’ (motivations such as exploitation of IT resources through to ‘hacktavists’). Drop us a note here if you’d like to discuss how we’ve helped other organisations with these challenges

Pain’s inevitable – suffering’s optional (don’t let your organisation suffer)

We heard this phrase as a way to describe long distance running (thanks Andreas!). It also works well for an information security breach. For example, it’s now virtually inevitable that you’ll have a security or data breach of some sort. However, becoming “the victim” (and suffering)doesn’t have to be.

Traditional Crisis Management or Business Continuity scenarios don’t usually cater for technical incidents that involve the loss of sensitive data. Conversely, traditional technical incident approaches typically focus on system recovery and restoring an IT capability.

Not ‘pre-considering’ the broader organisational can have serious repercussions. As McKinsey & Co. noted, “a poor response can be far more damaging than the attack itself”.

A typical plan contains three distinct phases such as Assessment, Response and Closure. Each phase is typically managed by a tailored team of company personnel including subject matter experts and representatives of different areas of the business. The seniority of the participants typically varies by each phase.

Organisations that have developed a thoughtful data breach plan and who use practical scenarios to test the plan have a much improved chance to reduce the consequences of a data breach incident. “Suffering is optional…” drop us a note here if you’d like to discuss our experience in this area.

So What? Consider undertaking an exercise to align the different organisational departments in the event of a data breach (ie HR, Legal, PR, Operations, IT, Exec, etc). It’s not typical that all the affected parties would generally need to work tightly together and you don’t want to be working through the details when the event is real. Define the interfaces, overall process, and perform a ‘dry run’ to work through disconnections.

Principals in the press

We’re very proud to have a couple of our Principal Consultants hit the press in a range of venues this quarter. Ron Speed was quoted the February 14-20th edition of the Business Review Weekly (The ‘F’ Work and its chilling effect”). The article covers the issues of Fraud and Ron highlights “*as more businesses become electronically connected with employees, customers and suppliers, so, too, has the potential for fraud grown… they need to know where their critical data is, they must protect that data and they need to interrogate that data to monitor any irregular transactions or behaviours*”

Also in the press this quarter was Darren Arnott, the author behind several articles that receive exposure at CSO magazine (3 steps to total compromise – why Google’s 86,000 indexed printers should have your IT team jumping”) and further published in Epoch Times. Darren highlighted the serious impact of having exposed ‘system management interfaces’ to the internet. Why worry about having a printer indexed? If you’d like to know more about that topic and how vulnerable you may be to those issues, just drop us a note here and we’ll give you a call.

Tweet with us

We’re now cranking away on Twitter. We’d love to connect – join us here.

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.

Thanks for investing the time to catch up with us. 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,

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.