Thanks for taking the time to read this quarter's newsletter. And we thought the press was running hot last quarter! Major breaches are happening daily – even entire companies have gone under as a result of malicious internet activity (distribute.it).

Security an "unsolvable problem"?

The media's bombarded us with a deluge of unfortunate events. So much so, that we've heard a few clients lament "is it all becoming way too hard"? We think it's a matter of perspective, risk and balance. For example, a couple of points to consider:

1) **Put it in perspective**: Anyone can get anything from anybody with intent, resources and time. The Stuxnet virus is a sophisticated weapon of war, not a reason why it's "all too hard" and neglect the fundamentals of a basic security program. As one of our technical guru's wrote "It's always the silly things that allow me full access to a network. Sensitive information in directories on a website, configuration files with passwords embedded, devices with default or no passwords, open file shares, and on it goes…". There are complex threats in certain circumstances, but that's no excuse to ignore the basics…
2) **The world has changed**: At the start of the "IBM era" (50's – 70's), data became electronic and fundamental to core business processes. In the "Microsoft era" (70's – 90's) data was mass produced and distributed to every nook and cranny of the business. In the "Google era" (now) we've built doorways to the internet. NOW, that initial electronic data is accessible to 5 Billion internet users… that's one BIG number – it means that if there's a "one in a million chance" someone's interested in your data, there are 5,000 chances someone's interested in your data! Assess your internet exposure.
3) **Your data now has value – protect it** (Credit Cards to email addresses). Banks learned to protect this asset a long time ago – that's why they have hundreds of security professionals. Can some of your data be monetized? Inventive criminals find creative ways to take it.
4) **Apply a "20/80 Rule"**: Some people ponder the possible, while forgetting the basics. It's human nature – the "possibilities" are interesting to consider – the basics are boring and often mundane. Take patching your software… never-ending and tedious, but the 1st and 2nd MOST IMPORTANT "Strategies to Mitigate Targeted Cyber Intrusions" (Defence Signals Directorate). An ounce of security thoughtfully applied is worth a ton of security pondered.

Lessons from the Sownage

When our Managing Director was asked for boardroom commentary on the Sony Playstation breach, little did we think it would be the first of more than 20 breaches against the company.

The volunteers at 'attrition.org' have done an impressive job of chronicling the unfortunate progression (here), and while the old adage 'any publicity is good publicity' may be true, we're not sure the www.hassonybeenhackedthisweek.com is the kind of publicity any organisation would like to have available on the internet. While there's certainly lots to be learned these events, we think some of the key take away's include:

1. **Boring but basic – patch your software**. When was the last time you checked for the latest version of your critical software application(s)? The initial Sony breach was purported to be from missing firewalls and "outdated versions of the Apache Web server" (here). **Does someone in your organisation have the specific accountability to manage this risk?**

2. **Don't just "pay lip service"** – It's touted Sony's vulnerabilities were known for some time (Latest Hack Shows Sony Didn't Plug Holes). The statement from one of the notorious groups causing a lot of havoc is sobering…

   "Our goal here is not to come across as master hackers… SonyPictures.com was owned by a very simple SQL injection, one of the most primitive and common vulnerabilities, as we should all know by now… Why do you put such faith in a company that allows itself to become open to these simple attacks?

   What's worse is that every bit of data we took wasn't encrypted… over 1,000,000 passwords of its customers in plaintext… This is disgraceful and insecure: they were asking for it."

Many organisations can make big strides by just ensuring they're doing the basics (sometimes forgotten in the hype of the latest news). Drop us a note (here) if you'd like to see our simple 'maturity model' we use to highlight gaps.

Australian credentials testing mobile applications

Like the early dot-com days when web-developers threw up internet 'store fronts' as fast as they could, there's also been Apple or Android "APPS" developed to help companies innovate in this exciting space. This is slightly contrasted with CSO Online's "scooped" pictures of the soon to be released iPhone contender "The security-approved smartphone" …

Seriously though, if your organisation has/is developing an APP in this space, you may want to consider a Security Test. We know of NO other company in Australia (OTHER THAN OURSELVES) with the proven credentials and experience testing in this space. If the Government advises against sending data offshore, you may also want to keep your confidential testing onshore too. Drop us a note (here) if you'd like to learn of our unique intellectual property, approach and credentials testing in the iPhone, iPad, Smartphone, Android space.

Please don't hesitate to send us a note with any comments or observations from the above – we'd like to hear from you.

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 its **guaranteed** – we will deliver, full stop.