Trusted Impact Quarterly Newsletter – Q1, 2012

Welcome to the first quarter of 2012 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.

The strategy of security – big shifts and new trends

These days, you'd almost have to live under a rock not to see the unceasing flow of information security-related news. So much in fact that it's almost becoming difficult to separate the 'wheat from the chaff' (the old metaphor about separating items of value from those of little or no value). In addition, the broader implications of day-to-day information security events can often be lost in the 'noise' surrounding one's job and your organisation's business priorities.

That's one of the reasons why we enjoy having a singular focus in information security. Not only do we see trends and themes with a focused perspective, but the 'collective insight' gained from a diverse range of clients who are large, small, new, and old provides us with a unique vantage point and perspective.

An important shift in the industry has emerged in the last few quarters. In particular, the need to consider the distinct possibility that 'the bad guys' may already have access to or be inside your organisation.

The 'first wave' of security was about building technology walls around the organisation to keep bad things out of the organisation. The 'second wave,' evangelised by the Jericho Forum, said the "perimeter was dead" and recognised the need to separate valuable / monetizable / sensitive data so that there is less to have to protect, but also facilitate innovation and partnering.

While many organisations are still getting their heads around the 'second wave', recent data suggests the "third wave" may be upon us – which is the real possibility that for some organisations, they may have already been compromised. Therefore, it becomes important to have the skills, tools and ability to detect and remove malicious activity on the inside.

Why? Too many stories have (and continue to) surface where technology vendors who were frequently the 'trusted protectors of the gates' are admitting their 'perimeter products' have been compromised for some time. So, ironically, while they intended to bolster an organisations' defences, they may have inadvertently become "Trojan horses". Examples include:

- RSA's "SecurID" tokens – the preverbal "keys to the kingdom for high value IT systems around the globe" were compromised last year (more here).
- Symantec recently admitted the source code for its antivirus software, its 'remote control software' (pcAnywhere), and its well-known 'Norton Utiliites' programs were compromised.
- Verisign, the "company in charge of delivering people safety to more than half the world's websites" (according to Reuters) was hacked repeatedly in 2010 and could not pin down what data was stolen.

In short – the technology used to 'lock' the corporate data, isn't useful if everyone has the keys. Even then, it's tough to keep up with the changing world. This was reinforced by the US Director of the FBI who believes:

> *"…there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."*

While we're not purporting the sky is falling, there are some important implications to an organisation's approach to security…

The implications of this shift?

We think security should be about managing to an acceptable level of risk, and how the organisation invests it scarce resources towards security is always open for debate. What we're highlighting is the likelihood of this risk is likely greater than anticipated, and the tools, skills and capability are very different too.

It's traditionally not been an area of investment for organisations outside of large financial institutions. But as sensitive data becomes easier to monetize, it is prudent to consider how to address a risk that has become greater likelihood, rather than a mere possibility.

A 'defensive' approach is still valid. It's just that it's not the entire picture, nor is it prudent to ignore, in today's fast changing environment. Three simple questions to consider include:

1. Would you know if you had a breach, or would you be prepared if you read about it in the news? Telstra's recent data breach was purportedly first published in a user forum.
2. Has the organisation identified the diverse groups that need to be coordinated to proactively respond to an issue (eg, Customer Service, IT, Legal, Public Relations, etc.)? You don't have lots of time after the 'horse has bolted from the barn'. Sony's still paying the price of waiting too long to notify customers of its major breach last year.
3. Does your organisation have the architecture, tools or skills to assess (and understand) anomalies in data flows going outside the organisation (not just those coming inside?).

Drop us a note (here) if you'd like us to help you understand what this may mean for your organisation.

Our strategic partnership to create 'meteorologists for the cloud'

If you were a farmer, you'd probably know the value of a meteorologist and appreciate the impact weather had on your business and livelihood. When it comes to cloud computing, we'd think a similar analogy applies – not all 'cloud's' are the same and it's important to know how (computing) clouds differ to your business and livelihood.

As such, we're thrilled to announce that we've entered into a strategic partnership with one of Australia's leading data centre and cloud infrastructure training organisations, The IT Training Company, to offer the Certificate of Cloud Security Knowledge (CCSK) training. The IT Training Company is partnered with the Cloud Security Alliance, a global not-for-profit organisation with a mission to promote the use of best practice security in Cloud Computing.

Ron Speed, Principal Consultant with Trusted**Impact** – the only certified CSA Instructor in Australia and New Zealand – will be delivering the certification training program with The IT Training Company in various locations in the upcoming weeks.

The relevant risks of the Cloud are vastly different for each organisation – certification will provide you with both a practical foundation of security and risk issues in the cloud, plus the formal industry recognition to do so.

Schedules are almost finalised – if you'd like to learn more just click here and we'll send details in a few days.

Why the New Digital Frontier needs new thinking

The brave new (digital) world is upon us – organisations and customers intensely connected anywhere, anytime. Ubiquitous mobile devices and feature rich online services enabled by fast accelerating Internet speeds. Rewards for organisations able to innovate online are major. For some, it's simply a matter of survival.

But executives leading the charge to the 'New Digital Frontier' must think and act differently. Traditional 'bricks and mortar' thinking simply doesn't apply. Our RECENTLY RELEASED WHITEPAPER presents the facts for a non-technical audience to understand why organisations must think differently and heed Darwin's challenge to "adapt or die".

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

Kind Regards,

Trusted**Impact**

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.