Welcome to the third quarter with Trusted**Impact**. Although it's been a cold winter in Australia, we continue to see the industry 'running hot.'

This quarter, we thought we'd reflect on several of our recent "battles from deep in the trenches" working closely with a range of clients, and highlight some of the more systemic, deeper issues that may be at play and provide you with some ideas to learn from.

Lessons from the front line…

Unfortunately we've seen a marked increase in security-related incidences this quarter. The motivation(s) behind these incidents were highly varied and ranged from sophisticated to unsophisticated attacks. In one instance, we found an advanced point-and-click program that could be used by low-skilled hackers to conduct a phishing attack on a local bank. Automated tools like the one uncovered is a living example how the global 'hack from home' industry is increasing the risk of compromise – anytime, anywhere (in this case, Austria to Egypt).

In our Q1 update (here), we stressed the strategic shift to "**consider the distinct possibility that 'the bad guys' may already have access to, or be inside of your organisation**". Both the rate and pace of security incidents are on the rise, and the effort to respond to an incident (or even worse, a publicly announced data breach) is not something you'd want to do as a "on the job training" exercise. As a recent McKinsey's whitepaper reinforced, "a poor response can be far more damaging than the attack itself."

Consider undertaking a cross-functional exercise to understand who might need to be involved with one or more of these events. In the event of a breach, a diverse set of actors must be closely coordinated (operations, IT, legal, public relations, etc.) to minimise the negative impact of a breach or avoid the scrutiny of regulatory bodies that are keen to be seen as addressing the public's interest in these highly publicised events.

If online is important to your business

If your online presence is important to your customers or a key part of your business model, consider the simple reality that you're now a target. Factually and statistically speaking, if YOU haven't tested your online 'footprint' for technical vulnerabilities we can guarantee you that SOMEONE ELSE HAS.

One incident was the result of not fixing a well-known exploitable vulnerability. Another was the result of out-dated, vulnerable software that wasn't patched.

Testing the 'footprint' is a good first step, but it needs to become a tightly integrated part of the broader approach to building and maintaining IT systems (SDLC). Consider whether your organisation uses a common SDLC, or more important, whether security is explicitly woven into the fabric of that SDLC? If nothing else, be vigilant to ensure critical vulnerabilities are closed off before the project is completed.

Repeat… don't outsource your reputation (previous whitepaper here)

Third parties were involved in a majority of last quarters' incidents. In one situation, the third party IT Company made several configuration errors that caused the client to be a sitting duck. At the time, it wasn't unreasonable to assume that this organisation would have configured the network correctly.

Like many things in life, if it's important (like your health), you'd typically get an independent opinion from someone with experience. The same holds for your important systems or data, and it's especially relevant if that data is also maintained by a disinterested third party or residing somewhere "in the cloud".

Consider which third parties may be custodian of key systems or who gather, store or process sensitive information. Think about identifying and segregating those who may hold your reputation at risk and assess whether they can adequately protect your reputation in the face of today's security threats.

Also, consider getting an experienced, independent party to assess the third parties who may be the custodians of your reputation.

In most situations, outsourced organisations earn their living by meeting defined Service Level Agreement (SLA's) measures at the lowest possible cost. It's a simple truth. If you're working in the third party, you'll be seeking a new employer if you suggest it needs to increase cost beyond what's explicitly defined in the contract. It's also extremely rare to find security-related measures as part of outsourced SLA's.

At the very least, even though it may be a conflict of interest, ask the third party to provide you with a self-assessment of their security capability – just don't take it for granted or without consideration. Drop us an email here if you'd like help in determining what questions to ask.

Watching for tell-tale signs

Finally, in the majority of incidences this quarter, the organisations were notified about the incident from someone outside of the organisation. Would you know if your systems had been breached?

Consider configuring your systems to monitor three simple tell-tale signs of a potential issue. Some of the basic items would likely include:

1. Monitoring **outbound traffic -** exception reporting for large volumes or anomalies
2. Knowing if changes were made to key program files on your internet infrastructure
3. Identifying and monitoring anomalies such as a large number of failed log-in attempts

Security: an activity – not an organisation!

In the last decade the CIO's job description changed from needing to be a deep technology expert to needing to be an advisor and facilitator of innovation. The exact same shift is occurring in information security.

Security must evolve to be activity that's ingrained into the everyday operations of the entire organisation. Not merely a standalone organisation. The security team role must now facilitate business-driven and risk-based decisions for the entire organisation to consciously choose, rather than be the group that either assumes responsibility for data protection or defines the "rules" of what can or cannot be done by the rest of the business. The new mission for security is not to say 'no' but rather 'how'.

We're looking for 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.

———

Many thanks for reading this quarters' update. We'd welcome your thoughts – 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.