This quarter's seen a number of 'far away' global issues manifest themselves onto our local shores. For example, the conflict in the Ukraine became much more 'local' when we sadly lost 27 Australians in the MH17 incident; we've gained concern for a much more traditional virus than we're used to thinking about (Ebola in West Africa), and local police raids against Islamic State terrorist threats all remind us that we live in a closely connected global village.

Historically, the 'tyranny of distance' meant that Australia often found itself out of the 'mainstream' of many global concerns and threats. These events remind us that it is no longer the case, and that we can't rely on historical perspectives in today's world. This is particularly true now that we live in the Digital Age, which knows no traditional physical limitations such as distance, country boarders, or time zones.

The (Digital) "Neighbourhood" got bigger…

This quarter Internet World Stats now count over 2.8 BILLION users on the Internet. That's a really BIG population of people who ALL have access to your internet-facing systems, every minute, of every day. For example, they all have access to your website, your remote access to internal systems, your new mobile APP that may track your customers and connect to back end systems, or even your personal cloud. And if only 1 person out of 100 people was motivated to exploit those systems, that's 28 million people… or a malicious group BIGGER than Australia's entire population. Just because we can't physically see them, doesn't mean that they're not there.

Therefore, today's internet-facing systems must be built and maintained with a higher degree of security in mind then ever before. Applying the "traditional tyranny of distance thinking" (as described above) is no longer valid. Security needs to be 'by design' and not simply an afterthought. For organisations undertaking systems transformation or even just dipping their toes into the Digital Age with a new customer web-site, now is the time to do this. If you'd like to explore what building security in from the start means to your organisation, drop us a note (here). It doesn't have to be onerous or expensive. In fact, it can even save you money and effort.

We like working with those 'who get it'

We're always thrilled to work with organisations that 'get it' when it comes to security. Recently Ian Gibson, the CIO of SuperChoice (an organisation for which Trusted**Impact** is proud to be its chosen security partner) was interviewed about his views on 'cyber resilience'. It's a good proactive perspective worthy of viewing here.

Speaking of resiliency…

A few years ago the head of the US FBI announced that "there are only two types of companies: those that have been hacked and those that will be". The practical reality of that statement gained additional traction this quarter when the commander of the US Cyber Command spoke about shifting from prevention to resiliency:

"*Most organizations… put their resources and focus on stopping people from penetrating their systems… we have got to not only focus on stopping people… but … to operate and remediate at the same time. That's resiliency*"

We are also finding that similar thinking is emerging among some of the forward-thinking business and technology leaders that we have been working with. Drop us a note (here) if you'd like to discuss the subtle, but very important implications of 'resiliency' and what it likely means to your security strategy, resourcing and skills.

Cyber now a 'fiduciary responsibility' of the Board?

We've all heard a lot about the Target breach from last year. But this quarter there has been a very important development: a lawsuit asserting that Target's Board of Directors breached their fiduciary duty. The lawsuit claims "the board should have recognized and acted on certain risks associated with the company's business… [and it] breached its fiduciary duties to the company by ignoring the warning signs..." The gist of the article is that "while a board cannot be expected to foresee every potential disaster that might befall the company, it can in fulfilling its

oversight function, ensure that management has adequately taken account of those events that are foreseeable". Does your business rely upon information to operate effectively? Is a cyber-attack or data breach foreseeable? Is the Board or management team applying their fiduciary duty of care?

One simple way to apply duty of care

One way your organisation (and Board) can demonstrate its fulfilling its fiduciary responsibility (as highlighted by the lawsuit above) is to develop and exercise a meaningful business-driven 'incident response' plan using practical security-based scenario's. These scenarios can't just be IT-centric. When a breach occurs it requires cross-functional teamwork (e.g., business operations, legal, risk, public relations, senior management, etc.), all working closely together to mitigate the negative BUSINESS impact. You shouldn't be ironing out the wrinkles when it's real.

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 (and often including external stakeholders). Drop us a note here if you'd like to discuss our hands-on experience in this area.

Metawhat? Metadata retention insight

Sometimes we all find ourselves in an unfortunate situation where you may be asked to describe something that isn't very clear or well understood. We're confident that this unfortunate interview with Attorney-General, George Brandis will haunt him for a long time. But on a more practical side, we thought the Sophos article (here) provided good insight to understand what might be learned from one man who volunteered one week of his metadata simply from his mobile phone.

Hold the press (and patch quickly!)…

Just as we were about to publish, we've learned of the "Shell Shock / Bash Bug" technical security vulnerability affecting UNIX / Linux based operating systems (good description here). While many traditional systems are less affected, the consequence to the "Internet of Things" can be extensive. While details are still emerging, it's rated a 10 out of 10 (CVE details here), and US financial regulators are stressing that "the pervasive use…and the potential…to be automated presents a material risk."

It shouldn't be ignored if you're chartered with the protection of your organisation's information or its systems. Just give us a call, or drop us a note if we can help you understand the risk your organisation faces with this issue.

Please update our address in your records

Our Melbourne office relocated last quarter and is settling in well at 9/22 Albert Road, South Melbourne. Please update your records and stop by if you find yourself in the neighbourhood!

———

Thanks for investing the time to catch up with us. Also, don't hesitate to pass this along to anyone who might find this of interest (or subscribe them 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