This quarter, the debate as to whether the Russians did, or did not, influence the US election continues to rage. So much so, that other countries such as the UK, France and Germany also believe the same may have occurred in those countries.

Irrespective, we're still left with the result of the US election and are in the first 100 days of President Donald Trump's reign. Many would have bet heavily that he wouldn't have made it anywhere close to the presidency, but that's now history and each day's presidential tweet seems to bring another unbelievable position...

Is the 'Internet of Things' spying on us?

The growth and dramatic impact of internet-connected devices continues to be estimated at astounding levels, such as shown in the roundup of forecasts located here. The myriad of charts and numbers in that link all show one thing: we live in a connected world and it will only continue to accelerate.

Last quarter we saw how millions of internet-connected devices can be harnessed by a virus to create the 'botnet that broke the internet'. However, this quarter we were reminded of another risk of internet connected devices, when we read that the U.S. FTC settled a case against a manufacturer of 'smart TV's' who was using 11 million televisions to secretly collect, and sell, data about customer locations, demographics and viewing habits. If you were lucky, you may have also missed how an APP-controlled vibrator was collecting and collating data in Canada. The television manufacturer was fined $2.2 million, while the sex toy maker agreed to pay a total of C$4 million.

What are the lessons learned? We've seen numerous organisations building APPs (and other connected devices) to support their innovative digital strategies. Consciously consider the potential privacy implications and have the APP security tested to ensure that sensitive or private information isn't being captured (for often well-intended purposes). And by the way, it's not just a theoretical issue. About a year ago we helped one Australian organisation understand how it was unknowingly capturing a considerable amount of private information about its customers.

Mandatory notification laws are here

After several aborted attempts over the last several years, Australia's mandatory data breach notification scheme quietly received royal assent approval this February. It's anticipated the new laws will take effect in February 2018. The formal explanatory memorandum can be found here. However, a good summary of guidance is here.

Are Australian companies ready? Would you know if you had a data breach? Statistics would likely say it's doubtful. For example, according to a Trustwave Report, only 41% of breachers were detected by the victims themselves, and of those, the time between intrusion and detection was nearly a half of a year (168 days). There's also a good, growing list of 'pwned' (compromised) websites and user credentials here.

But the excuse of not being aware of a breach is being tested vigorously in other parts of the world. In the US, the Federal Trade Commission made a ruling in February as a glimpse of what's to come that "sends a clear and sobering signal to business owners: You must make significant, demonstrable efforts to protect yourself from data breaches or face the consequences"

There are tangible benefits of having a swift response too. A Ponemon Institute study found that the cost associated with a data breach is US$1.2 million less if the 'mean time to contain' is below 30 days versus greater than 30 days.

Do you have a plan for notifying your customers if they're effected by a data breach? Drop us a note if you'd like to discuss ways to improve your ability to identify, detect, recover or respond to minimise the business impact.

The (tangible) value of Cyber Due Diligence

In the M&A space, dealmakers learned the value of cyber due diligence. Experts from accounting, venture capital, consulting, and law firms can be very good at assessing the profitability and potential synergies of a merger or acquisition. Yet little, if any, attention is paid to the security posture of the organisation under scrutiny – often with disastrous results. For example, when Yahoo realised it lost data for more than one billion accounts last year shares of the internet pioneer fell more than 6 percent. This quarter Verizon, who is acquiring Yahoo formally agreed to reduce the purchase price by $350 million.

Cyber risk rankings…

This quarter, we saw numerous statistics pointing toward cyber as a significant risk, worthy of proactively managing as part of your business. If your Senior Management or Board are wondering how real the risk is, it might be worthwhile quoting a few recent sources like:

- Cyber attacks are tied for third highest risk in Australia in 2017 by the World Economic Forum,
- This ranking was echoed by Allianz, who rated cyber incidents as the third most important corporate peril, above fire, natural catastrophes, and even macroeconomic developments,
- James Clapper, whose term as Director of the US National Intelligence ended in January, ranked the cyber threat as the number one global threat the US faces – ahead of traditional terrorism.

Cost of a breach defined: lost customers, revenue, and opportunity

Cisco released their Annual Cybersecurity Report in January. It (unsurprisingly) found that more than half of organisations faced public scrutiny after a breach. More specifically however, 22% lost customers, 29% lost revenue and 23% lost business opportunities. A large number of each category (~40%) had impacts greater than twenty percent!! The statistics can be confusing, but the simple message is that it pays to invest in an adequate level of security. What would a 20% loss of your customer base, or yearly revenue target equate to?

Cyber "incentive's misaligned"

Cybersecurity isn't simply about technology, but involves people, process elements, AND the alignment of incentives across the organisation. This quarter, Mcafee released an interesting survey that highlighted three levels of "misaligned incentives" - all putting our 'defenders' at a disadvantage. For example, it found that a majority of organisations said they had a cybersecurity strategy. But while many senior executives believed this strategy was fully implemented across the organisation, only 30% of those responsible to implement it, agreed. Cybersecurity is a 'LEADERSHIP' challenge and requires business leadership to manage (as further highlighted in our recent Public HealthSector Assessment Case Study, and Security Team of 2020 report).

Microwaves that turn into Cameras, and jailbreaking… your tractor??

On a lighter note to finish this quarter's update we noted a couple of interesting items.

When discussing the possible wiretapping of Trump Towers, Kellyanne Conway describes the many ways to surveil an individual... you know, like those "Microwaves that turn into Cameras, etcetera"...

In another strange twist, apparently American farmers are also hacking their John Deere tractors with Ukranian firmware. "*Tractor hacking is growing increasingly popular because John Deere and other manufacturers have made it impossible to perform "unauthorised" repair on farm equipment, which farmers see as an attack on their sovereignty and quite possibly an existential threat to their livelihood if their tractor breaks at an inopportune time.*"

Many thanks for taking the time to catch up with us, and being part of our community. Please pass this along to someone who might find it useful (or they can subscribe directly 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