Just when you think the political environment can't get stranger, it does. Just a week ago Donald Trump threatens to 'totally destroy' North Korea and mocked his leader as 'Rocket Man', we now have the highly intellectual retort calling Trump a 'mentally deranged U.S. Dotard'. ...Dotard... it kind of reminds us of what we might have said on the grade 6 playground in a fit of frustration and anger blurting out something that seemed to sound good at the time. That was OK in grade six, but now we're playing with thermonuclear weapons. Heaven help us.

Fortunately, the business environment seems to have disconnected itself from the political rhetoric, and continues to look positive with "low inflation and global expansion continued"! In our security space this quarter, we got a true taste of what global interconnectivity means when Petya and Wannacry ransomware rippled across the globe on a scale that we hadn't previously experienced. More on that in a bit.

"Don't forget to change your name, date of birth, home address and social security number, regularly".

That had to be one of the better tweets (by @SarahJamieLewis) when Equifax announced their massive 143 million record breach. If you lose someone's credit card, it can be cancelled and reissued. Lose someone's personal details (and biometrics) and we find that it's not so easy to cancel and reissue those!

With major data breaches happening in the last several years, several things can be assured:

1. Share price will be hit (albeit, to be fair it often recovers). Equifax (EFX) was trading at around $140 per share and dipped as low as $93 per share thanks to the breach. That's about US$5.5 BILLION or ~1/3rd.
2. It's a Board and CEO problem and thus, action must be decisive. Equifax moved quickly to 'retire' their CIO and CSO within a few weeks of the breach. Now the CEO has stepped down too!
3. Intolerance at a political level. "Lawmakers demand accounting"
4. Potential litigation. Equifax faces largest class-action lawsuit in US History.

While it's still early days and lots of details are still emerging on the scale of the breach, the view is Equifax officially has no excuse... "*Capping a week of incompetence, failures, and general shady behaviour in responding to its massive data breach, Equifax has confirmed that attackers entered its system in mid-May through a web-application vulnerability that had a patch available in March*".

Hindsight is 20/20, but one clear lesson can be learned: don't underestimate the need to 'respond' and 'recover' (NIST) as a fundamental strategy of your cybersecurity program. Not paperwork, but an exercised program across the leadership of your organisation. The eCensus debacle was a good local example, and Alastair MacGibbon eloquently noted that it's not just about writing procedures: "*While the ABS and IBM had a library of incident management documents to guide them through the events of 9 August, they were impractical, poorly tested and none outlined a comprehensive cyber incident response or communications plan that could be effectively implemented*".

Have you engaged experts to help in the event of an incident? It'll be hard to go to the purchasing department and ask them to undertake an RFP for communications, PR, legal, or forensic assistance after the horse has bolted. A little planning can go a long way, and if you need help we have lots of experience – just ask. As we've said for a long time: getting hacked or having a data breach is inevitable... becoming a headline doesn't have to be.

Cyber Scale: The impact of 50 billion interconnected devices

This quarter we felt the impact of our global, internet-connected world when two major ransomware attacks spread like wildfire. So much so, that insurers are scrambling to put a price on cyber catastrophes. Let's remember that the main 'root cause' of this issue was unpatched software, or an ineffective disaster recovery capability. Those two things are about as fundamental and basic as you can get when it comes to cyber 'hygiene'. We also understand that convincing the Board to allocate precious budget dollars to something that is not grounded in cost savings or innovation is very hard.

Fortunately, these 'basics' were quantified this quarter to help you in those discussions. Maersk estimates that 'NonPetya' will cost it US$300 million in lost revenue; FedEx also reported an estimated US$300 million loss. Mondolez (who owns the brand Cadbury), the world's second-largest confectionary company, reported a 5% drop in quarterly sales, blaming half of that dip to the ransomware attack. And Reckitt Benckiser, an international consumer goods giant, announced the assault may take a £$100 million bite out of the company's revenue.

Locally, we were frightened to read that "ransomware forced 1 in 5 Australian SMB's to stop business (to immediately deal with the issue or because they lost access to critical files needed to keep operational). The fundamentals – it can be basic, boring and not always easy to do – but worth getting it right. If you need help gaining visibility of your exposure, or to help define a practical approach to reduce this risk, drop us a note here.

The biggest threat is inside your organisation

We were honoured to participate in a cybersecurity executive briefing for Victorian Government leaders last week. One of the strongest recurring themes was the risk associated with unaware or vulnerable employees. For example, we conduct lots of 'phishing exercises' for our clients. These are short, sharp analytical assessments designed to capture measurable statistics behind this risk, and more important, the effectiveness of awareness programs. A recent test for a government department found 30%, not only clicking on a nefarious link, but providing us with their username and password. What's even worse, is that when the IT team sent a broadcast email to 'not click' the rate of clicking increased. Do you know your organisation's 'click rate risk'?

This recurring theme is one reason why we thought it would be a good topic to compile an impressive panel of experts in our involvement with Cyber-in-Business 2017 (#CIB17). The organisers of CIB17 are on the top of their game, and we're delighted to be involved because we also think that cyber is a business problem – not just a technology issue. It's on 26 October – we'd love to see you there, and you can register here. Why is employee risk an issue? 75% of large organisations suffered staff-related security breaches with 50% of the worst breaches causes by human error! Some simple and practical thoughts to consider are in this short but useful blog.

Still looking for the best of the best

We're looking for well-connected professionals with 10+ years of experience - technical guru's and creative thinkers who can solve real business problems. Drop us a note or your CV (here) for a confidential chat.

Significant Salient Statistics...

This quarter's statistics come from Thycotic's 'State of Cybersecurity Metrics Annual Report', which found:

- 1 in 3 companies invest in cybersecurity without any way to measure its value.
- 4 out of 5 companies fail to include business stakeholders in cybersecurity investment decisions.
- 4 out 5 companies don't know where their sensitive data is located, and how to secure it.

Thank you 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