Welcome to the second quarter of 2016. All of our clients are extremely busy and there's a lot of business growth and energy across nearly every sector in Australia. That's a positive sign for this quarter, despite the impending elections in both Australia and the US.

This quarter experienced the largest leak of confidential data in history. 11.5 million confidential documents from the Panamanian company Mossack Fonseca (aka "the Panama Papers") was apparently "100 times more data than... WikiLeaks". We expected to read of a highly sophisticated technical exploit used to steal this highly confidential data... but alas, no, just 'staggeringly out of date software' again, as we typically find when conducting technical security tests. The message? Persevere with that boring patching of your systems – it pays off.

Australia's Cyber Security Strategy sees daylight!

In July last year, we were fortunate to participate in a noteworthy event that brought together some of Australia's most influential business leaders with the (then) Prime Minister. However the change in the country's political leadership meant the strategy was thrown into the air for months and there was little clarity on when or if it would be released.

The tension finally broke in April, and we were again fortunate to participate in a similar round table and the formal release of the Cyber Security Strategy at the Australian Technology Park. While the strategy didn't change dramatically from the initial round table, the additional granularity and definition behind the strategy's actions and outcomes was well worth the delay. It's also debatable whether the A$230 Million (some good analysis here) earmarked for the Australian strategy is actually worthy when compared to similar budgets such as the UK's £3.2 Billion, or the United States' US$24.8 Billion. However, as Tobias Feakin aptly pointed out (here), "The Australian government hasn't invested in this area since 2009, so it's well overdue".

The value of your data?

A report worthy of highlighting came out this quarter from Dell SecureWorks. Titled "Customer service is the motto. Hackers are now extending their services hours, guaranteeing their work, and expanding their offerings to keep customers coming back", the report goes into significant detail to demonstrate how vibrant the underground market is, with respect to monetising data. For example, in Australia it found credentials for your local bank account (ANZ) earned $3,800 to $4,750 depending on the amount in the account.

We were also frightened to read in that report that "Corporate Email Accounts" were getting $500 per mailbox. Why so scary? We help clients with tailored 'phishing campaigns' in order to provide analytical insight into this "click risk" for them, and also maintain a statistical database of results from which to provide a practical and relative perspective. With over 600 emails as a statistical population, on average, one quarter (25%) of employees click on a nefarious link (think risk of things like crypto-locker or malware). However, even worse, nearly as many (23%) actually provided us with their active company username and password.

Executives are typically motivated by factual stats and it's a great way to 'baseline' the effectiveness of an employee awareness campaign. Do you know your number? Drop us a note (here) if you want help getting it.

Cybersecurity "the biggest risk", says SEC Chair

This quarter saw Bangladesh's central bank lose $81 million that was funnelled through the Society for Worldwide Interbank Financial Telecommunication network (aka SWIFT). Several weeks later, more details emerged about similar attacks in Vietnam and Ecuador. As a result, Mary Jo White (Chair of the US Securities and Exchange Commission) released warnings that "represent the SEC's strongest warning to date of the threat posed by hackers".

While we suspect there may be a fair amount of sophisticated approaches taken in these attacks (at least to monetise them), it's worthy to highlight that the initial evidence in the Bangladeshi situation found that it was vulnerable "because it did not have a firewall and used second-hand, $10 switches to network computers connected to SWIFT". Really?

Well, maybe not too surprising if we tell you the true story of one of our assignments from a few years ago. A client needed a conference room where one of our Senior Principals were conducting security testing, and kindly asked him if he could relocate to an empty cubical to hold an external meeting. As he sat down in the cubical, he noticed a printed A4 page with word 'SWIFT' at the top. He asked if the client wanted the paper, and was told 'nah, just keep it there – it's no big deal'... Not only did that one piece of paper have step by step instructions on how to make a SWIFT transfer, but it also had the valid username and password... which, by the way, was the SAME password he used to obtain 'privileged access' to that organisation's IT environment. ... It shouldn't be that easy.

Billions gained from Business Email Compromise (BEC)

Literally every week for the past several months, we've heard real stories from senior executives across a range of different companies in Australia about how close they came to transferring funds at the (fraudulent) request from (someone posing as) their CEO or CFO. So we weren't surprised then when we saw the US FBI release a Public Service Announcement update this month that US$3.1 Billion of losses have been registered with the FBI in the last 18 months alone in relation to a "Business E-mail Compromise" scam! That's a "B" as in BILLION!

The Announcement has sound advice, worthy of considering and implementing in your organisation. At first blush, you may wonder who'd fall for something like that. Apparently, some sound organisations like Ubiquity Networks who lost US$46.7 Million, or XOOM Corporation, who lost US$30.8 Million, or The Scoular Company, who lost US$17.2 Million. FACC, an Austrian Aerospace manufacturer announced in May that it lost €50 Million, and then proceeded to fire both its CFO and CEO. These scams are extremely well researched, but with numbers like these, clearly worth the investment for the bad guys. Speak to your executives so you don't fall into the above category.

Still looking for the best

If diverse clients and projects, impressive peers, challenging work, unequalled pay, and a flexibility workstyle sound interesting, drop us a note or your CV (here) for a chat. We're looking for proven consultants who are security pro's with 10+ years of experience - technical guru's and creative thinkers who can solve real business problems.

Salient, Stunning Stats...

Each quarter we see a wealth of statistics published from diverse sources. When used sparingly and in the right context, statistics can often improve a discussion with senior executives or those less exposed to the industry.

- 66% of consumers would be VERY LIKELY (20%) or SOMEWHAT LIKELY (46%) to leave/switch from doing business (or cancel a membership) with an organisation if they were hacked. (n=2400, Centrify)
- 146 days (nearly 5 months) – the median time of a data breach between the compromise of an organisation to the discovery of the data breach. Mandiant M-Trends 2016.

Thank you for investing the time to read this quarter's newsletter. Please to pass this along to anyone you think would find it useful (or they can subscribe here).

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