It's the second quarter of the year (calendar), and (for many based in Australia) it's hard to believe another fiscal year is quickly coming to a close! Unfortunately, we experienced a local casualty of the Digital Age this month. Australian founded and headquartered, PageUp is still assessing the damage of a data breach. More on that below.

New rules in customer information...

The global rules around customer information changed this quarter... as of May, we saw the European Union's General Data Protection Regulation - better known as GDPR – take affect and now most businesses have had to rethink their approaches to data security. Although it's a European Union regulation, it impacts anyone who does business with European citizens, including companies with websites that are available in Europe. In other words: almost everybody. We found a pretty good "top 10" list of GDPR information here, and a good infographic here if you're trying to understand or explain the implications of GDPR for your organisation.

(the right) Lessons Learned...

This quarter we (unsurprisingly) learned that the City of Atlanta, Georgia fell victim of 'ransomware'. We found it odd that the article focused almost entirely on the ethical trade-off between paying a $50,000 ransom amount, rather than spending what ended up being $2,667,328 for incident response assistance and crisis communications services, etc (if you don't have a calculator, that's 53 times the ransom amount!). The article appears to suggest that it was actually okay to spend over 50X the ransom amount on 'post incident' recovery, because "we should never pay ransom", that it would only 'encourage them', or we must never 'give in' to such heinous threats. If the article wasn't in a reputable magazine like Wired, one might have thought it was written by the 'crisis communications' firm hired by the City of Atlanta.

Hmmm... we try to reflect upon key events of the quarter to learn the important 'so what' issues for you and your organisation... the REAL lesson from this incident is not about whether you should or should not pay a ransom, it's about reducing or removing the risk that ransomware with lock up your data! For example, this would have been achieved by a) training staff not to click on nefarious links, b) limiting your exposure to the internet (sources indicate that there may have been external exposures such as RDP or SMB), c) 'patching' your systems with the latest security updates, and d) simply having a well exercised Disaster Recovery plan whereby one could restore an infected machine with little to no loss to data... if you remove the risk, the response to the crisis becomes irrelevant!

So, if you think you face similar challenges, we have considerable experience identifying open vulnerabilities, our 'SecurityThinking' culture change program reduces that risky 'click' behaviour, and we've helped c-suites work through 'cyber crisis workshops' to improve the executive team's ability to respond and recover (in the calm of an exercise, rather than the panic of a disaster). It's worth the investment. Just drop us a note to explore it further.

Lingering pain of a breach...

This quarter the US Securities and Exchange Commission (SEC) fined the company previously called "Yahoo" (now "Altaba") US$35 Million to settle charges around the massive 2014 data breach that exposed about 3 Billion user accounts. The fallout from the Yahoo data breaches continues to illustrate how cyberattacks thrust companies into the competing roles of crime victim, regulatory target, and civil litigant. The fine is significant, less because of the size, but because it makes the first time the SEC has ever gone after a company for failing to disclose a cyber security breach to the stock market. It's a trend that is likely to continue with future breaches – perhaps in Australia too.

This event gave us the opportunity to reflect and summarise the tangible 'fallout' that's happened since the original breach. It adds up over time! On September 22, 2016, Yahoo disclosed the breach in a press release. The following day, Yahoo's stock dropped 3%, or ~US$1.3 Billion in market capitalisation (albeit, share prices recover over time). We mused whether any "Billions" style hedge funds were shorting that stock.... but back to the real cash outflows:

- Initially, US$16 Million was spent in incident related expenses ($5 Million for forensics, $11 Million for legal fees), the company "flatly stated" that it didn't have cybersecurity liability insurance (a lesson there).
- Then Verizon, who was acquiring Yahoo at the time, agreed to a reduced purchase less $US350 Million off of the original offer.
- In time, the company settled a class action lawsuit for $80 Million.
- This quarter, the SEC fined it US$35 Million

In total, that makes US$481 Million (A$655 Million) in hard cash outlay – so far. In addition, there's even more from a personal perspective that we shouldn't forget. Marissa Mayer, CEO forfeited a US$2 Million cash bonus, and an "annual equity grant" estimated at US$12 Million a year. The CIO, Alex Stamos was shown the door, and the General Counsel, Ron Bell, resigned (link). The major lessons?

1. The cost of prevention often will be much less than the cost of response and recovery.
2. Cybersecurity insurance is a worthwhile investment – just read the small print.
3. Do "cyber" due diligence in an acquisition – it's not just about cost savings or merger integration any more, as we described in 'did you buy an information security breach'?

Local road kill on the information superhighway

We'd be remiss if we didn't highlight the local fallout of a significant breach this quarter. PageUp, an Australian-founded and headquartered "Software as a Service" (SaaS) business is still coming to grips with the size and scale of its data breach. Thanks to GDPR requirements, they had a small 72 hour window to alert the British Information Commissioner's Office. Alistair MacGibbon kindly noted that he felt PageUp was 'victimised' by the onerous disclosure timeframes and had demonstrated a commendable level of transparency. Litigation and 'class action' are words that have been mentioned and we've seen emails where some of their ASX 200 clients have been contacting job applicants with information on how to reduce their exposure. While the company was considering a public listing, those plans are likely to be put on hold.

How do we learn from this? Cloud applications and SaaS businesses face a range of technical and configuration issues (how many times do we need to read about breaches due to "open Amazon S3 Buckets" before we do something?). For another example, a recent client opened a directory of their SaaS application to a traveling developer (and forgot to close it) – it was running outdated software (which was a beacon to the internet) – and they used a poor password (making it easy to crack). To make matters worse, forensics were challenging because no one ever considered monitoring or saving logs which could assist with the visibility of what happened. We suspect PageUp may be somewhat similar, and if that sounds like you, do yourself a huge favour and go to the 'Centre for Internet Security'. They have benchmarks for both Amazon and Azure that provide excruciating detail on how to secure your cloud. If the benchmarks look daunting, drop us a note and we'd be delighted to help.

———

Thank you being part of our community and taking the time to read our quarterly update. If you'd like to send this to others who might enjoy it, please pass it along 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