Second quarter update
June 2015

Last quarter we saw the American Health Insurance industry lose tens of millions of sensitive health records. This quarter, the US Federal Government kept a similar pace with the massive OPM Breach – now estimated to have lost personal data for over 18 million (and counting) current, former and prospective federal employees. That size is just a bit more than 75% of Australia's entire population...

But don't think we're out of the firing line, this quarter the Australia Federal Police announced there were more than 3,500 breaches in April, and "threats are expected to increase". It's worthwhile noting that that statistic is "reported" breaches – one wonders how big the "unreported" breaches might be in a country without mandatory reporting.

Hot off the presses: The Security Team of 2020

This quarter, we were delighted to release the findings of our 'security team of 2020' leadership series study.

This effort began late last year when we interviewed 30 thought-leaders from the Australian technology, security and risk industries to gain their insight into the key trends they were facing as we head to the year 2020. In particular, we were keen to explore how these trends would influence the skills and roles needed to build the 'effective' Security Team of 2020.

While we're never short of an opinion, we thought there was considerable value to capture a collective perspective from a large group of practitioners across the industry and listen to what they faced from their unique perspectives. Participants were sourced from a diverse range of large to small; commercial and government, and local to international organisations.

Overall, we listened and learned that the industry faces a genuine "leadership" challenge, rather than a "technical" challenge. In particular, five overall conclusions could be synthesised from our in-depth discussions, which were

1. There are significant **changes** which are **rapidly reshaping** the information security **industry**.
2. How one succeeds in the role of "**Chief Information Security Officer**" (or equivalent) is **also changing**.
3. For the security team to be effective in 2020, the **composition of skills and roles must change**, and must become **more engaged with their businesses**.
4. Overall '**demand**' for security personnel **will outstrip 'supply'**, however, what is **more important is** the **mix** and composition of **skills** for the successful Security Team of 2020,
5. If businesses wait until 2020, it will be too late. **Businesses must start today** to keep ahead of these trends and change the composition of skills to meet these challenges.

We provide some thoughts on the "way forward" and would be very happy to talk with you about the implications of this industry insight to your organisation. An electronic version of this report is located here. But if you'd like the printed booklet, don't hesitate to drop us an email and we'll put one in the post or drop it by at your convenience.

Strategic testing and holistic vulnerability management

We're fortunate to be able to conduct lots of technical security tests for a large number of diverse organisations. We find a broad range of approaches, for example; some organisations view a "penetration test" as a tick box exercise where a project manager files the report neatly away; sometimes we retest an environment just to see the same vulnerabilities pop up over and over; in some circumstances we hear "let's push that test out another six months - we're still dealing with the issues you found from the last test"; and sometimes when a cost crunch comes, an organisation can pull back the frequency of testing "across the board".

Therefore, we thought it would be of value to raise the issue of 'strategic testing'. In other words, are all systems the same, or can one apply a structured "80/20" approach to systems in terms of priority (for example, a rating based on the external exposure of the system, the sensitivity of data within in the system, the number of records associated with the sensitive data, etc.)?

Considerable value can be gained by working closely and collaboratively with an organisation (like us) to gain clarity on these priorities so that the testing effort and/or frequency can be better aligned to the risk these systems face. Additionally, the real value is in resolving the vulnerability - not just highlighting them. A more holistic "partnering approach" to overall vulnerability management (vulnerability identification through to resolution and ongoing monitoring) might be the answer to reducing your testing cost, but more important, increasing the value of the effort. It's not just about the test, but about minimising your risk. If you'd like to explore this simple, but powerful concept further, just drop us a note here.

By the numbers…

Each quarter we trip across 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. This quarter we found these interesting:

- 51% of consumers are extremely or very concerned that companies aren't protecting their data
- 82% of consumers have changed their shopping / internet habits due to cyber security fears
- 65% would avoid healthcare providers that experienced a data breach
- US$3 Trillion – The aggregate economic impact that cyberattacks have by slowing the pace of technology and business innovation per McKinsey and the World Economic Forum.
- IT Governance generously compiles a list of cyber-attacks / data breaches each month – this quarter you can see the list for April (here), May (here) and June (here).

Quotes of the Quarter

From "Lloyds chief names 'most serious' risk to businesses" published in Corporate Risk & Insurance on 9 April:

"Cyber Risk poses the most serious threat to businesses and national economies, and it's an issue that's not going to go away" (Inga Beale, CEO Lloyds)

From "How cyber attacks became more profitable than the drug trade" published in Fortune on 1 May:

"One large healthcare company in a major metropolitan area managed a network of more than 30,000 healthcare professionals and had only two employees dedicated to information security. Those in tune with the business of IT security know this is outrageously understaffed, but unfortunately this situation is also common."

Thank you for investing the time to read this quarter's newsletter. Please feel free 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