Signals

Quarterly security assessment

Q4 2015

CommonwealthBank

Ben Heyes
Chief Information Security and Trust Officer, Commonwealth Bank

Signals aims to empower business executives with unique insights into the cyber threat environment and advice on the strategies and controls necessary to ensure a robust defence.

This advisory was prepared by our security analysts for business leaders that trust Commonwealth Bank as their preferred supplier of financial services.

It reflects the calibre of guidance I provide executives and boards in my role as Chief Information Security and Trust Officer of Commonwealth Bank.

We hope and anticipate the report will filter out the noise from media reporting of cyber security events and provide context and confidence for your security strategy.

Cyber Security:

Trends and Observations

Key trends observed during the quarter

> Adjust risk calculations to account for **heightened nation-state activity**

Ransomware on the rise

Ransomware is a form of attack in which access to files or applications on a devices is typically disabled after a malware infection, and the user is presented demands for payment in order to 'unlock' the files. The Australian Cyber Security Centre notes that 72% of surveyed Australian organisations experienced a ransomware incident in 2015, up from 17% in 2014. The malware is most often delivered via a phishing campaign.

CHECKLIST

- Consider a rolling program of phishing simulation to test the susceptibility and raise awareness of staff to phishing attacks.
- Enforce IT policies that place sensible limits on user access to shared drives they do not require regular access to.
- If infected with ransomware, report the incident to ACORN (the Australian Cybercrime Online Reporting Network).

State-sponsored attacks continue

Government agencies and technology providers continue to be subject to attacks attributed to the work of State-sponsored attackers. Attacks that impacted Australia's Bureau of Meteorology[i] in the lead-up to the Paris climate talks and the compromise of network security devices from US firms Juniper and Fortinet count among the attacks assumed to be perpetrated or sponsored by nation-state actors. While attribution for cyber incidents is fraught with difficulty, the volume of this activity has grown to the point that analysts are confident they can fingerprint a nation-state attacker according to the techniques, tools and procedures used – to the extent that social networks Facebook[ii] and Twitter[iii] now offer warnings to users they suspect of being compromised by these actors.

CHECKLIST

- Adjust risk calculations to account for heightened nation-state activity.
- Consider whether your organisation holds any data on employees of government agencies, military contractors, technology companies or other industries of interest to nation-state aligned actors.

Cyber security skills and innovation on national agenda

Efforts by the Australian Government to build an innovation ecosystem around cyber security has borne fruit even before the Government's review is released. Newly-minted Prime Minister Malcolm Turnbull has announced a $30 million investment in a cyber security 'growth centre' in Canberra. Commonwealth Bank has further announced a $1.6 million skills partnership with UNSW, which aims to address the lack of skilled graduates available to industry and lack of qualified teachers to provide training across Australia's universities. It will result in the creation of five new courses at UNSW and a courseware licensed for distribution under Creative Commons and freely accessible to a broader number of students as a MOOC (online course).

CHECKLIST

- Communicate with your technology staff the opportunity to refresh security knowledge by registering for the free **MOOCs (massive open online courses)**[iv] developed by UNSW and funded by CBA under the sec.edu program.

By the Numbers

There are

21 million

mobile SIM cards active in Australia

72%

of surveyed Australian organisations experienced a ransomware incident in 2015.[xvii]

Cyber Security:
Trends and Observations

Hotel chains compromised

Most of the world's largest hotel chains suffered large data breaches in 2015 in circumstances which suggest a targeted campaign by well-resourced actors. Starwood Hotels[v] (incl. Sheraton, W, Westin) and Hilton Hotels[vi][viii] (incl. Hilton, Waldorf, Doubletree, Hampton Inn) separately announced data breaches in November 2015 for the period between November 2014 and July 2015. In late December, Hyatt Hotels disclosed[viii] that 250 of its facilities had been hacked between August and December 2015. All the hotels reported malware infections via similar attack vectors – their physical point of sale and reservation systems[iv] at gift shops, event booking desks etc. The Starwood and Hyatt breaches resulted in the theft of an undisclosed number of complete sets of customer credit card information. Starwood noted that fraudulent transactions followed its breach. The breaches followed similar events at luxury resorts operated by Trump Hotel Collections in mid-2014.[x]

CHECKLIST

- Consider subscribing to threat intelligence sharing networks that can provide early warnings when your peers are targeted.
- Seek access to a threat intelligence function to assess your organisation's exposure to data breaches at third parties. (Example: Are your executives' personal or financial details exposed in these hotel breaches?)
- Study Hyatt Hotels' response in the aftermath of its breach as a strong case study in terms of providing clear, detailed communications that aimed to alleviate customer concerns.
- Ensure your cyber security strategy considers traditional aspects of physical security. For example, are your point of sale devices always within sight of a manager? Are your frontline staff empowered to challenge an unscheduled visit from your retail systems supplier or service technicians?

Data breaches hit home

Breaches of the customer databases of VTech and Sanrio (Hello Kitty) have exposed to parents across the globe the implications that a pervasively-connected world has for their children's privacy. The hacking of toy manufacturer VTech demonstrated that 11 million customer details - including names, mail and email addresses, encrypted passwords, security questions and answers, IP addresses, download history and the contents of chat logs (including children's photos and videos) – were easy pickings to unsophisticated attackers. The Sanrio (Hello Kitty) breach exposed the full names, birth dates, email addresses, encrypted passwords and password reset questions and answers of 3.3 million of the company's customers.

CHECKLIST

- Assess the potential security risks associated with connecting your products or assets to the public internet and invest in controls accordingly.
- Factor into your 'Internet of Things' strategy the potential for devices you connect to the internet being visible to search engines such as Shodan.io.

> "Most of the **world's largest hotel chains** suffered large data breaches"

By the Numbers

The cost to Target from its 2013 data breach has tallied

US$290 million

(AU$400 million)

to date after it agreed to pay **US$39.4 million (AU$55 million)**[xv] to settle a class action suit filed against it by US banks and **US$67 million ($93 million)** to Visa.[xiv]

UK telco TalkTalk estimates the cost of its October breach at

£35 million (AU$70m)

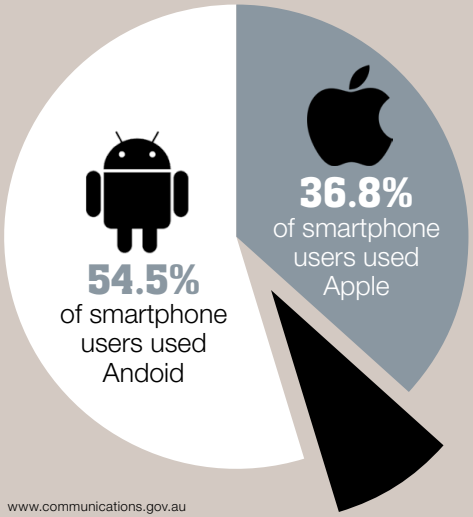
Some 157,000 customer details were exposed

Over

200 billion

apps have been downloaded from mobile app stores since 2008

As of September 2015...



www.communications.gov.au

Over

100 million

customer records were stolen as part of a multi-year hacking, fraud and money laundering scheme uncovered by US authorities. [xviii]

Deep Dive:

Closing the Cyber Skills Gap

Introducing ***sec.edu***

Brett Winterford
Information Security Analyst

An adequately sized and appropriately skilled cyber security workforce is critical to advancing Australia's digital economy and meeting current and future cyber security challenges.

Today, there is a large deficit between demand for skilled professionals required to secure and protect Australia's digital assets and the supply of adequately trained and experienced professionals.

The US Bureau of Labor Statistics predicts that the rate of annual growth for hiring of information security analysts is in the order of 36.5 per cent out to as far as 2022. The UK Government's National Audit Office reports that without significant intervention in exercises that attract and train the next generation of cyber security workers, demand will outstrip supply for the next 20 years. Buoyed by these official figures, providers of cyber security training have boldly claimed that the world is one million candidates short of cyber security talent.

In late 2015, we asked online employment marketplace SEEK to dig up some numbers on whether Australia is in a similar predicament, and the results were telling:

- SEEK IT Insights found that advertised roles in cyber security grew an incredible 60.6 percent in the last 12 months.
- Security roles were classified as the hardest to fill within the Information and Communication Technology (ITC) sector, according to the SEEK analysis.
- Security roles are on average the third highest paying role in IT ($122,741 average advertised salary – see chart).

Deep Dive:
Closing the Cyber Skills Gap

> “This licensing format permits the **democratising of access** to security education across the nation”

sec.edu

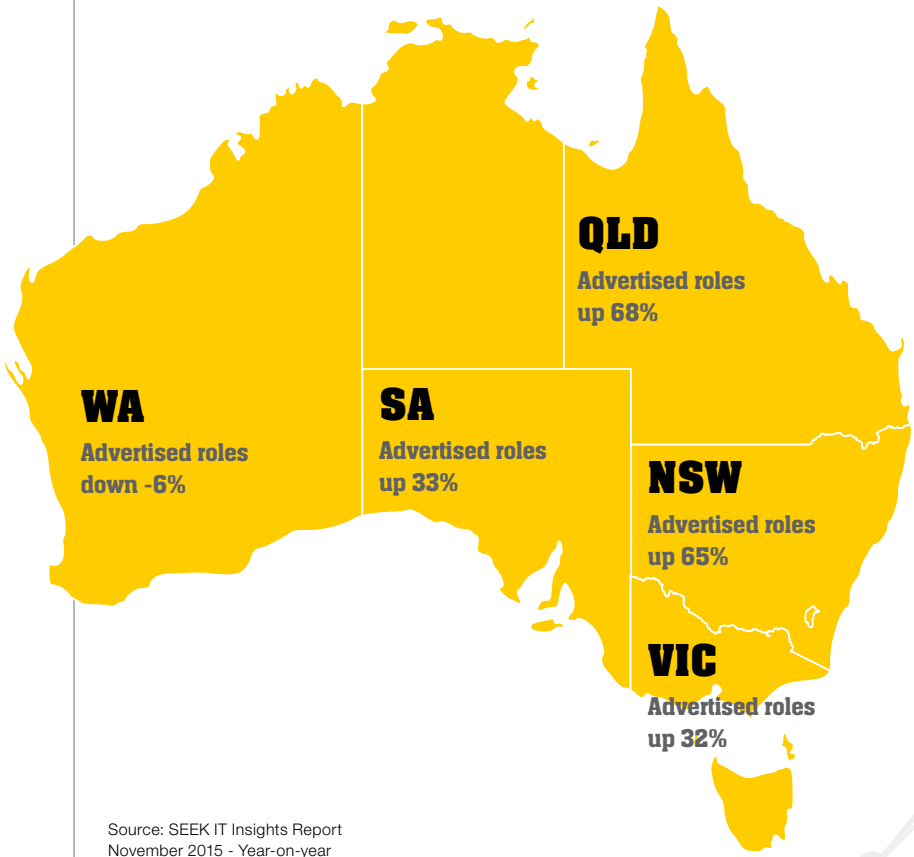
Commonwealth Bank – recognising the investment its customers have made in digital technologies – saw a responsibility to show leadership on this issue.

In December 2015, Commonwealth Bank announced a $1.6 million, five-year investment in a new centre of cyber expertise at the University of New South Wales in Kensington, Sydney under a program called ‘sec.edu’. This will deliver a new training facility, teaching expertise and a complete undergraduate curriculum for students that wish to take advantage of the growth in cyber security roles.

Critically, UNSW has agreed to distribute the resulting courseware under Creative Commons Licensing as a Massive Open Online Course.[xi] This licensing format permits the democratising of access to security education across the nation. Nothing would prevent other Australian universities re-using the material to uplift the quality of their own cyber security programs.

Already, over 4300 students have signed up to take the first free ‘Security Engineering’ course online.

State by State
Where is the demand?



Source: SEEK IT Insights Report November 2015 - Year-on-year growth in ‘security’ roles, October 2014 to October 2015

Top Australian computer science universities (global rankings)

13. University of Melbourne
26. Australian National University, Canberra
35. University of NSW
36. Sydney University
49. University of Queensland

Source: QS University Rankings 2015[xii]

Top cyber security teams from Australian Universities - 2015

1. UNSW (1)
2. UNSW (2)
3. UNSW (3)
4. UNSW (4)
5. Monash University
6. UTS - University of Technology, Sydney
7. Murdoch University
8. University of Sydney
9. Edith Cowan University (1)
10. Edith Cowan University (2)

Source: Cyber Security Challenge, 2015[xiii]

Regulatory & Legal

New laws and legal precedents relevant to security strategy

Mandatory Data Breach Notification Laws drafted

In December 2015, Australia's Attorney General released an exposure draft of legislation that would amend the Privacy Act to require an organisation to notify the privacy regulator – the Australian Information Commissioner – and affected individuals if the organisation experienced a 'serious data breach'. The draft legislation is available for comment until March 4, 2016, but can't be passed into law until at least 12 months after industry consultation (mid-2017 at the earliest).

CHECKLIST

- Ask your privacy team or legal counsel to review the draft legislation.
- Contact your Commonwealth Bank relationship manager if you would like to improve your understanding of what constitutes a 'serious breach' under the legislation - Commonwealth Bank's Privacy and Digital Trust team is willing to make themselves available to interested clients in early 2016.

US cyber security information sharing bill signed into law

US President Obama has signed into law a mechanism by which private organisations are offered indemnity from privacy, antitrust, freedom of information laws and regulatory action if they volunteer to share threat intelligence/cyber security information to the DHS. It was included in a 2000+ page Omnibus Appropriations bill negotiated in private between the major parties and stripped of several user privacy amendments. Guidelines for sharing threat indicators (including privacy aspects of this sharing) will instead be determined by the US Attorney General and DHS over the coming months.

CHECKLIST

- Expect the Australian Government's Cyber Security Review to consider a cyber threat information sharing mechanism.
- Commonwealth Bank will offer key clients a briefing on the outcomes of the review once its findings are made public in February 2016.
- Consider the 'reasonable expectations' of your customers and stakeholders as a higher yardstick than the privacy considerations required by law.

New Zealand launches new cyber security policy

The New Zealand Government has updated its cyber security policy, proposing the establishing of a national Computer Emergency Response Team (CERT) that offers a two-way exchange of cyber threat intelligence between private organisations and government agencies, the biannual conducting of cyber preparedness exercises that includes private industry and heightened cyber hygiene in both business and consumer communities via a nationally-coordinated awareness campaign (Smart Connect).

Legislators at odds over encryption crackdown

Legislators in several countries have called for tighter regulation on the use of privacy-enhancing encryption in consumer messaging services in the wake of terrorism events in Paris, Beirut and other cities. Pressure is being applied to technology companies such as Apple and Facebook-owned WhatsApp to cease offering end-to-end encryption or to provide intelligence services key escrow (backdoor access). Apple in particular is reluctant to remove privacy protections from its services – similar demands compelled BlackBerry to pull out of the Pakistan market as of January 1, 2016[xix]. The insertion of backdoors has been rejected by Governments in the Netherlands[xx] and France[xxi] on the basis that they introduce a potential point of compromise for malicious actors.

CHECKLIST

- Continue to use end-to-end encryption to secure your services where appropriate.

UK proposes new surveillance bill

The United Kingdom has proposed new legislation that compels telcos and providers of digital services to monitor and store user data for a minimum of 12 months. The Investigatory Powers bill formalises permission for UK intelligence services to forcibly gain access to user machines (globally) for surveillance purposes and compels all private organisations operating within the UK to provide mechanisms for bulk surveillance by intelligence services, even if it requires the breaking or use of weaker security protections (such as encryption) required to secure the integrity of user services. The laws have been vehemently opposed by both global technology companies and domestic UK telcos.

CHECKLIST

- Seek legal advice on your potential obligations to UK intelligence services if offering products and services within the United Kingdom.

Better Practice

The latest advice your technology team should consider when setting security policies:

Protect yourself when travelling to international events

The Australian Signals Directorate has released its **latest security guidance** for senior political or business representatives attending international or high-profile events, which includes tips on dangers of USB drives, webmail and public WiFi.

Learn how to identify and triage ransomware

Researchers from antivirus vendor SophosLabs have released **samples and supporting data for variants of ransomware** for analysis by your security team.

No crypto? No excuses!

Not-for-profit **'Let's encrypt'** [xxii] has launched a free, automated SSL certificate service in beta. The automation features require experience with Unix/scripting. Certificates valid for three months (hence requirement for automation). Check with your cloud provider as to whether they can offer the same free service.

Set reminders for expiring security certificates

A simple, free service – **'Certificate Monitor'** – now provides administrators an automated reminder when security certificates on their web properties are soon to expire.

Horizon Scan

Upcoming events of interest

2016 Feb 03 — **Sydney**

CommBank Cyber Alliance session, Executive Reporting and Dashboards

CommBank is sharing with peers and key customers a view of how to best communicate cyber security issues to the board. Contact your relationship manager if you would like to access this material.

2016 Apr 12-14 — **Canberra**

Australian Cyber Security Centre annual conference

The Australian Government's annual information security event.

2016 May 23-27 — **Gold Coast**

AusCERT2016 Conference

Australia's largest and oldest information security conference

Footnotes

i: http://www.abc.net.au/news/2015-12-02/china-blamed-for-cyber-attack-on-bureau-of-meteorology/6993278

ii: http://arstechnica.com/security/2015/11/iranian-military-spear-phish-of-state-department-employees-detected-first-by-facebook/

iii: http://motherboard.vice.com/read/twitter-told-a-bunch-of-users-they-may-be-targets-of-a-state-sponsored-attack

iv: https://www.openlearning.com/SECEDU

v: http://www.wsj.com/articles/starwood-reports-payment-information-data-breach-1448033469

vi: http://krebsonsecurity.com/2015/11/hilton-acknowledges-credit-card-breach/

vii: http://news.hiltonworldwide.com/index.cfm/misc/guestupdate/frequently-asked-questions

viii: http://www.hyatt.com/protectingourcustomers/

ix: http://www.computing.co.uk/ctg/news/2436988/questions-raised-over-hilton-worldwide-point-of-sale-hack

x: http://krebsonsecurity.com/2015/10/trump-hotel-collection-confirms-card-breach/

xi: https://www.openlearning.com/courses/sec

xii: http://www.topuniversities.com/university-rankings/university-subject-rankings/2015/computer-science-information-systems#sorting=rank+region=+country=+faculty=+stars=false+search=

xiii: https://scoreboard2015.cyberchallenge.com.au/

xiv: https://twitter.com/CommsAu/status/678810894814437376/photo/1

xv: http://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203

xvi: http://www.bbc.com/news/uk-34784980

xvii: https://www.acsc.gov.au/publications/ACSC_CERT_Cyber_Security_Survey_2015.pdf

xviii: http://www.justice.gov/opa/pr/attorney-general-and-manhattan-us-attorney-announce-charges-stemming-massive-network

xix: http://blogs.blackberry.com/2015/11/why-blackberry-is-exiting-pakistan/

xx: http://www.bbc.co.uk/news/technology-35251429

xxi: http://www.theregister.co.uk/2016/01/15/france_backdoor_law/

xxii: https://letsencrypt.org/