Signals

Quarterly security assessment

Q2 2016

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.

In this edition, we focus on the dangers of password re-use in the wake of large data breaches of social networks, and on national priorities in the wake of the release of the Australian Government's cyber security strategy.

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.

CommonwealthBank

Cyber Security:

Trends and Observations

Key trends observed during the quarter

> Commonwealth Bank is **investing in bringing an internationally renowned research program** into cybercrime to the South East Asian region

Mass compromise of social media sites

Databases of historical (circa 2013) user credentials stolen from LinkedIn[i] (167 million accounts), MySpace[ii] (427 million accounts) and Tumblr[iii] (65.4 million accounts) have been advertised for sale[iv] on the dark web. Large-scale data breaches were also reported in Russia[v] (100m user credentials), and the Philippines[vi] (55m) this quarter. Given the widespread practice of individuals re-using credentials for multiple online services, CISOs should assume credentials belonging to a subset of their users are available on the black market. Several online service providers have chosen to force password resets for users they suspect to have recycled passwords.

CHECKLIST

- Ensure your stored user credentials are protected (see OWASP guidance[vii]).
- Educate your users never to use the same password for social media sites as they do for email accounts, banking, superannuation or other critical services.
- Commonwealth Bank offers our valued institutional customers an eLearning module on password security should you wish to deploy to your staff.

Organised crime pulls off intricate bank heist

An organised crime group has stolen US$81 million from Bangladesh Central Bank (BCB) after attacks on bank systems that use the SWIFT network for inter-bank payments. Attacks against Ecuador Bank and Tien Phong Bank (Vietnam) and an unnamed bank in Ukraine[xxxii] have since surfaced that utilised similar methods. The attacks required persistent access to BCB systems (most likely via spear-phishing and malware), bespoke malware produced to circumvent SWIFT controls, and a complex network of banking insiders, money launderers and casino junket dealers in the Philippines (and possibly China).

CHECKLIST

- Evaluate processes to ensure large or unexpected payments cannot be made without additional verification steps (such as a form of two-step authentication).
- Ensure business leaders and staff with authority to make large transactions on behalf of the company have completed security awareness training.
- The Australian Government's new Cyber Security Strategy outlines the development of voluntary cyber security 'health checks' (checklists) to assist boards and executive committees of large organisations with effective governance of security issues. In the interim, refer to the Australian Signals Directorate's 'Top 4'[viii] for a baseline of security controls.

Asia Pacific shapes as hotbed for cyber incidents

The Asia Pacific region has not traditionally been a major source of cybercrime when compared to Eastern Europe, the United States, Africa or East Asia. Increasingly, however, attacks are being sourced to countries in our region. Recent analysis by Microsoft uncovered a hacking group 'PLATINUM', which targets government, defence, telecommunications and intelligence targets in South and South East Asia. Casino junket operators in the Philippines, meanwhile, are central to attacks on several global banks (see item on the far left). This quarter, Thailand also entered the Top 10 list for source of DDoS activity for the second time in a year, while Indonesia and Singapore have both made the Top 10 lists of sources of web application and DDoS attacks. CBA's Intel sources have sourced a variety of online scams from Malaysia that had typically originated in Nigeria, and observed anecdotal evidence of East European threat actors relocating to Thailand and Vietnam (possibly to escape law enforcement or extradition troubles at home).

CHECKLIST

- Commonwealth Bank is investing in bringing an internationally renowned research program into cybercrime to the South East Asian region to provide an elevated understanding of the threat landscape in the region. Stay tuned to future editions of Signals to find out more.

By the Numbers

1.7 Billion
the number of global smartphone users now offered end-to-end encryption on their messaging app thanks to WhatsApp and Viber.

19 DDoS attacks recorded by Akamai have exceeded 100Gbps in the last quarter.[xxiv]

US$1.3 Million
Price FBI paid for a vulnerability in the Apple iPhone.[xxv]

50 Number of cyber security breaches affecting the US Federal Reserve since 2011.[xxvi]

Cyber Security:
Trends and Observations

> “analyses of the security of the law firm and its peers found **most were vulnerable to web injection** attacks”

Singapore Government restricts internet access for staff

The Singapore Government, responding to continued cyber security attacks on government technology assets, has announced it will prohibit internet access from over 100,000 staff terminals from May 2017[ix]. Staff in roles that attract targeted attack will continue to access external SMTP (email) traffic, but will only be able to browse HTTP traffic (the internet) using kiosks on a dedicated network or via BYO devices. The policy – while likely to adversely impact productivity and staff morale - will remove the risk of multiple classes of malware-based attack.

CHECKLIST

- While the measures taken by the Government of Singapore are extreme and unworkable in commercial organisations, it highlights that your staff's web browser - when launched from web-links embedded in email messages – is the most likely vector for most forms of malware-based attack.
- Offer your staff security awareness training to reduce the risk of malware infection. Commonwealth Bank has made available a set of online learning modules for our valued customers to educate their users. Talk to your relationship manager if you would like to trial these assets.

Back to the future for macro-based malware

Over the last 24 months, malware writers have flocked back to a 1990's-era style of attack – embedding malware inside the macros of Microsoft Office documents attached to phishing emails. Malware samples discovered by McAfee using this technique jumped from 5,000 per quarter in Q1 2014 to 60,000 this quarter[x]. The attack has more than likely come back into vogue due to the success of a new business model for attackers: the payload delivered in these attacks is often a form of ransomware. Ransomware is malicious software that encrypts all files on or attached to the victim's system, which can be 'unlocked' by the attackers for a fee (usually in Bitcoin, a crypto currency authorities struggle to trace). Over 50 percent of phishing emails recorded last quarter carried ransomware[xi].

CHECKLIST

- Educate your users to be wary of documents that have arrived via email that ask for macros to be enabled. There is no need to enable macros to view an Office document.
- Microsoft Office enables macros by default upon installation. Instruct system administrators to disable macros by default "without notification" (older versions) or to block macros from documents that originate from the internet (Office 2016 and Office365).
- For those users that do rely on macros in documents they need to share with others, consider some of the controls suggested by the Australian Cyber Security Centre[xii].

Panama Papers: Hacktivism? Journalism? Privacy breach?

The breach of 2.6TB of data from Panamanian law firm Mossack Fonseca smashed every conceivable record for the size and impact of a data breach. The 4.8m emails, 3m database files and 2.1m PDF documents formed the basis of a series of reports by ICIJ, a global association of journalists, who dubbed the resulting work as 'The Panama Papers'. While the precise means by which the data was exfiltrated remains unknown (and many expect it required an insider), analyses of the security of the law firm and its peers found most were vulnerable to web injection attacks[xiii] – an important reminder to the legal community of their obligation to ensure the confidentiality of client documents. An intriguing aspect of the breach is that the use of the information to produce reports in respected mainstream media outlets about potentially incriminating activities by the world's most powerful individuals largely served to minimise discussion about the theft of the data, which the law firm claimed was acquired through a cyber-attack.

CHECKLIST

- Consider use of User Access Reviews to routinely ascertain the appropriateness of staff access to various applications and data within your organisation.
- Educate your software developers about SQL Injection attacks – refer them to OWASP's cheat sheet[xiv] and send them to Commonwealth Bank's AppSec masterclass in Sydney on July 11 (see p11).

By the Numbers

28%
of global CIOs have responded to a major cyber attack in the last 2 years.[xxvii]

US$4 Million
Average cost of a data breach to an organisation.[xxviii]

US$19 Billion
The US Government's national cyber security action plan. [xxix]

The tax records of over **724,000** Americans were stolen from the Internal Revenue Service in 2015.[xxx]

The US FTC reported a **47%** spike in ID theft in 2015. [xxxi]

Deep Dive:

National Cyber Priorities in Review

Daniel Muchow
Cyber Outreach Manager

In April, the Prime Minister presented Australia's first national cyber security strategy in over six years, detailing $230m to be spent on 33 initiatives between now and 2020.

Key initiatives include:

- bringing greater clarity to Government roles and responsibilities and the creation of new senior cyber security roles, including a Minister assisting the Prime Minister for Cyber Security, a Special Adviser to the Prime Minister on Cyber Security and a Cyber Ambassador;
- more resources for CERT Australia to increase its capability and capacity;
- establishing Joint Cyber Threat Centres and an online sharing portal;
- funding grants for small business to improve their cyber security; and
- a national cyber security awareness campaign.

National priorities

Considerable national effort has been made by the United States, United Kingdom and several other developed economies to develop cyber security skills and capabilities in recent years.

An 'apples for apples' comparison of total cyber security spending is fraught with ambiguity. At least 50-60 percent of the funding announced in the Australian, UK and US cyber security strategies (represented below) is allocated to national defence and intelligence activities. This is likely to be conservative - none of the three countries break down spend on cyber security by intelligence services and rarely do any governments provide the public an insight into total spending on intelligence services and rarely do any governments provide the public an insight into total spending on intelligence services. If we are to believe leaked documents that suggest the US' total intelligence budget in 2013 exceeded US$52.6 billion, with the UK's 'Single Intelligence Account' pitched at around US$2.7 billion, we should expect the cyber component of these intelligence budgets alone would likely exceed the cyber security budget made known to the public. Intelligence spending aside, the program funding that is detailed in national strategies tells an equally compelling story about each country's priorities.

> "Adjusted for the relative size of the two economies, **the UK is spending 3x more than Australia** on cyber security"

Security Spending

	United States	United Kingdom	Australia
GDP per capita[1]	$55,800	$41,200	$65,400
Internet users/percentage of population[2]	276.6m (86.8%)	57.3m (89.9%)	20.2m (89.6%)
Proposed Government spend on cyber security in next year[3]	US$19bn	US$673m	US$73.13m
Government cyber security spend per capita[4]	**US$59.12**	**US$10.50**	**US$3.21**
Like-for-like comparison	6 x more than the UK/18 x more than Australia	3 x more than Australia.	**Spending twice as much on new desktop computers for the ADF/DoD over the same period.**

[1]PPP, US$, 2015 estimate (Source: CIA World Factbook)

[2]Source CIA World Factbook

[3]In US$, exchange rates as of 15/06, based on annualised spend (UK, AUS)

[4]In US$, Based on projected 2015 populations, Source: CIA World Factbook

Deep Dive:

National Cyber Priorities in Review

> Meeting its objectives requires **implementation to be driven at a senior level**, via well-funded, adaptive programs

Skills Development

The UK has invested a far greater share of its cyber security spending on skills programs, even if the US spends more in total. The Australian Government's allocation of $3.5m over four years – at $875k per year – is likely to support the funding of a program office, suggesting the government expects the private sector to foot the bill for training the next generation of cyber security professionals.

Threat Intelligence Sharing

The Australian Government was more bullish, however, on programs of work to expand threat intelligence sharing with the private sector. While again dwarfed by the scale of spend in the UK and the US (whose threat intelligence sharing networks are well established), the prioritisation of funding for these activities in the Australian Cyber Security Strategy acknowledges the critical role the private sector will play in securing the digital economy.

Securing Government Networks

The United States is spending a great deal more than its peers – even on a like-for-like basis - on programs of work to protect government networks and systems. For every dollar invested by the Australian Government to secure agency networks, the US is spending $2,833. This investment is motivated in part by pressure brought to bear on the US Government in the wake of data breaches affecting critical US government systems (such as those in the Office of Personnel Management).

What next?

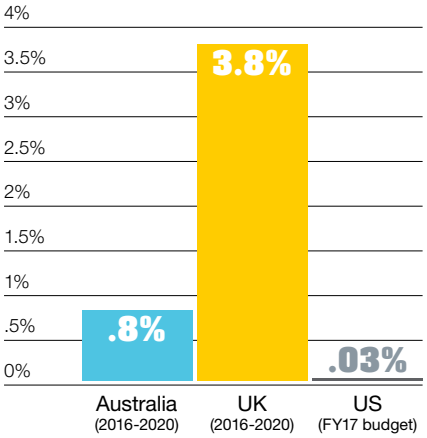
The launch of Australia's long-awaited strategy, along with the commitment of resources and accountabilities, was an important and promising step.

Meeting its objectives requires implementation to be driven at a senior level, via well-funded, adaptive programs, and with progress evaluated regularly and in a public fashion.

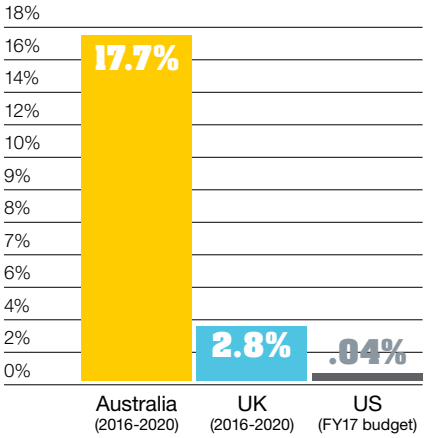
Implementation of these initiatives will also require industry stakeholders to continue to be actively engaged in the process. We expect the Government will soon be reaching out with more details on this implementation of in the months ahead.

% of Cyber Security Budget:

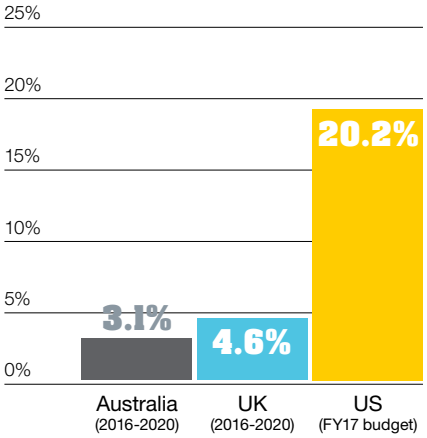
Education & Skills



Threat Intelligence Sharing with Private Sector



Improving Government Posture



Deep Dive:

Reset passwords

How attacks on social media expose your staff

Kevin Cleary
Cyber Intelligence Researcher

> “1 in 6 employees **used their work address** to sign up to social networks”

How many of your staff or customers use the same password for your services as they might for their social media accounts?

That’s an important question in the context of some unprecedented data breaches in recent months. Over 370 million credentials stolen from attacks on social networks LinkedIn, MySpace and Tumblr in 2012 and 2013 have been made available for sale on the internet at trivial prices. “Credentials” in this context include data such as usernames, passwords, password hashes and associated email address data.

The impact of data breaches of that scale doesn’t just affect the affected social networks. It impacts everyone. Recent academic studies cite that on average, people re-use a password for at least three different web services[xv], and show that close to half of online passwords are over five years old.

So would your staff or customers likely be affected? To get a sense of the impact, our team ran matches of the breached data against the email addresses of our staff. Commonwealth Bank, which group-wide employs over 50,000 staff in a broad range of roles across the country, is a very sizeable sample of the Australian population.

We found that 1 in 6 of our employees had used their work email address to sign up to these social networks. It’s highly likely that a similar ratio would apply in your organisation.

Our intelligence partners have recorded an increase in phishing attacks on users in Europe whose account details were obtained from the breach data. Attackers have developed automated tools (bots) which cycle through the compromised credentials in an attempt to gain unauthorised access to user accounts with other digital services.

Several providers of web services have publicly announced that they will force credential resets for users they suspect to have been affected by the breach:

- Reddit, a popular online bulletin board, reset the credentials of 100,000 accounts within two weeks of data being available for sale,
- GitHub, an online repository of source code, detected attempts to use the breach data to compromise its user accounts on June 14, and has subsequently forced password resets for affected accounts.[xvi]
- Remote desktop app vendors LogMeIn[xvii] and Citrix[xviii] have each forced password resets for users they suspect to be included in the breached data set. Remote access tool provider TeamViewer has also blamed these breaches of social networks for the compromise of a “significant” number of its users.

Our team is now looking to analyse whether use of work email addresses to sign up to trivial web services makes a staff member more vulnerable to targeted phishing attacks. Stay tuned to Signals for this analysis.

Price List: Recent Data Breaches

Service	Bitcoin	AUD (as at 8/6/2016)
167 Million LinkedIn accounts	2	$1,548.42
40 Million Fling.com accounts	0.5828	$451.21
50 Million Tumblr.com accounts	0.4255	$329.43
360 Million MySpace.com	6	$4,645.25

Source: Troy Hunt

CHECKLIST

- Ensure your stored user credentials are protected (see ‘OWASP guidance’[xix]).
- Consider checking your exposure to these breaches using services such as ‘have I been pwned?’
- Consider regular cycles of user password resets – being mindful of the limitations of this strategy as described by Microsoft Research[xx] and GCHQ[xxi]. Microsoft now suggests using a blacklist of commonly used passwords[xxii] and offers a handy cheat sheet for Microsoft system administrators[xxiii].
- Educate your users never to use the same password for social media sites as they do for email accounts, banking, superannuation or other critical services. Commonwealth Bank offers our valued institutional customers an eLearning module on password security should you wish to deploy to your staff.

You are invited to attend a

Security Assurance Masterclass

Brought to you by Commonwealth Bank's Digital Protection Group

sec.edu – a partnership between Commonwealth Bank and the University of New South Wales, welcomes our peers in the InfoSec community to attend a cyber security masterclass.

The masterclass will feature UNSW lecturers Brendan Hopper and Fionnbharr Davies providing the opening lectures to their renowned UNSW course on software and system assurance.

The COMP9447 course, from which this content is derived, is an advanced course that focuses on identifying, exploiting and rectifying security vulnerabilities in operating systems and critical software such as browsers.

The masterclass provides an introduction to:

- Reverse Engineering for Software Security Assurance
- Finding vulnerabilities in C and C++ code
- Identifying and classifying vulnerabilities using automated fuzz testing
- Developing reliable exploits for identified vulnerabilities for common classes of bugs

Best suited to: Assurance/penetration testing teams and security architects.

The Security Assurance Masterclass will be filmed as a Massive Open Online Course

Digital Protection Group

Wednesday July 6,
from 9.30am
Colonial Theatre,
201 Sussex St, Sydney

RSVP:
http://secedumasterclass.eventbrite.com
(password is COMP9447)

Regulatory & Legal

New laws and legal precedents relevant to security strategy

Morgan Stanley fined US$1m over data leak

Morgan Stanley has been fined US$1m[xxxiii] by the US Securities and Exchange Commission (SEC) for failing to "adopt written policies and procedures reasonably designed to protect customer information" after a staff member downloaded confidential customer data to his home server, which was subsequently hacked by a third party, resulting in the sale of the data online. The SEC argued that the bank "didn't audit or test" its authorisation procedures, nor did it monitor employee access to portals that contained sensitive data.

CHECKLIST

- Revise your staff end user computing policies to ensure they meet regulatory standards around protection of end user data.
- Consider use of User Access Reviews to routinely ascertain the appropriateness of staff access to various applications and data within your organisation.

UK surveillance bill almost law

The United Kingdom's House of Commons has passed the' 'Investigatory Powers Bill', which (assuming it is passed after being introduced before the House of Lords at the end of the year) will codify the surveillance practices of UK intelligence services and law enforcement. The bill provides powers of both bulk collections of internet and smartphone data and compels domestic service providers to retain communications metadata for one year and to have mechanisms in place to remove any encryption applied to this data. The bill allows for use of this information by intelligence agencies and law enforcement without need of a warrant, and equally allows for these agencies to 'hack' the systems of targeted systems in the UK and abroad. The bill introduces new forms of oversight for these activities, and some limited protections for politicians, journalists, doctors and lawyers. Privacy advocates have labelled the bill the 'Snooper's Charter'.

CHECKLIST

- Assume that many other nation states are engaging in the same activities (without the UK's commitment to transparency). The Australian Strategic Policy Institute estimates that at least 30 nation-states have developed offensive cyber capabilities.[xxxiv]
- Seek legal advice on your potential obligations to UK intelligence services if offering products and services within the United Kingdom.

NATO names cyber a theatre of war

Members of the North Atlantic Treaty Organisation – a military alliance that protects US interests in Western Europe – have agreed to designate cyber security as an official operational domain of warfare, creating a legal basis upon which a large scale cyber security attack against a NATO member could provoke a military response. The US Government made the same determination in 2011.

> "The bill allows for use of this information by **intelligence agencies and law enforcement** without need of a warrant"

G7 nations agree to norms in cyberspace

Leaders from Canada, France, Germany, Italy, Japan, United Kingdom and United States (collectively the 'G7' of industrialised democracies) have agreed to set of harmonised norms in cyberspace. The norms, which broadly align with the Australian Government's position, reaffirm commitment to internet openness and to a multi-stakeholder approach to internet governance. The short statement opposes "access to or transfer of source code as a condition of market access" for software suppliers, but recognises the "legitimate interest of governments in assessing the security of these products."

CHECKLIST

- To date, agreed norms of behavior in cyberspace have been meaningful between allies but there is little agreement with nation-states such as China and Russia on similar terms.
- The Australian Strategic Policy Institute has engaged experts in the private sector (including from Commonwealth Bank) in a study to determine norms in cyberspace that promote the interests of Australian industry. Stay tuned for an analysis of the results in the next edition of Signals.
- Like governments – large organisations concerned about cyber security also have a legitimate interest in assessing the security of software and systems prior to deployment. The CBA Cyber Outreach team participates in a private forum for discussion of Application Security and Assurance issues. Please ask your relationship manager if your organisation would like to participate.

Better Practice

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

Guide to Cybersecurity Event Recovery

The US National Institute of Standards and Technology has released a draft guide[xxxvi] to developing a playbook for responding to and recovering from cyber security incidents. [NB: Talk to your relationship manager if you would like to participate in a private session to learn from CBA's preparation of a Cyber Security Incident Playbook.]

Secure your password storage

The OWASP 'Password Storage Cheat Sheet'[viii] provides some particularly pertinent advice in the wake of social network mega-breaches.

Prevent ransomware Infections

CERT US has produced a list of seven preventative measures to protect an organisation from infections with ransomware.[xxxvii]

Check your RDP connections

CERT Australia has released a guide to locking down Windows Remote Desktop Protocol (RDP) connections[xxxviii], many of which have been targeted by threat actors employing ransomware.

Disable or limit macros

The Australian Cyber Security Centre has published an excellent set of advice on setting policies around use of macros in Microsoft Office documents.[xiv]

Clean installs only, please

Security firm Duo Labs has completed an analysis of security vulnerabilities left in the software shipped by OEMs (original equipment manufacturers) in new PCs[xxxix].

Plan to phase out rich media plug-ins

Owing to security concerns, web browsers are gradually ending support for rich media plugins such as Flash, Java and Silverlight in favour of HTML5. Most browsers will end support by the end of 2016.

Horizon Scan

Upcoming events of interest

2016 July 6

Sydney

Security Assurance Masterclass

sec.edu – a partnership between Commonwealth Bank and UNSW – delivers a masterclass on system and software assurance. This masterclass assumes competency in assurance activities (such as penetration testing). Cyber security professionals that attend this event can also register for a stream of further talks on July 13-15. Talk to your relationship manager if you would like your security architects or red teams to attend.

2016 July 11

Sydney

Application Security Masterclass

sec.edu – a partnership between Commonwealth Bank and UNSW – delivers a masterclass on application security. This masterclass will teach your software development teams how to identify and prioritise remediation of security flaws in code; what tools can aid the writing of more secure code and how to audit source code. Talk to your relationship manager if you'd like your software development leads to attend (free of charge).

2016 Sept (tba)

Sydney

CommBank Cyber Alliance session: Executive Reporting and Dashboards

By popular demand, CommBank's Outreach team will again share 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 attend.

2016 Oct 18-20

Sydney

Australian Information Security Association National Conference

Annual Conference for local industry group (NB: registration fees apply)

Footnotes

i: https://blog.linkedin.com/2016/05/18/protecting-our-members
ii: https://myspace.com/pages/blog
iii: https://staff.tumblr.com/post/144263069415/we-recently-learned-that-a-third-party-had
iv: http://arstechnica.com/security/2016/05/cluster-of-megabreaches-compromise-a-whopping-642-million-passwords/
v: https://threatpost.com/100m-russian-facebook-credentials-for-sale/118483/
vi: http://blog.trendmicro.com/trendlabs-security-intelligence/55m-registered-voters-risk-philippine-commission-elections-hacked/
vii: https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet
viii: http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm
ix: http://www.straitstimes.com/singapore/singapore-public-servants-computers-to-have-no-internet-access-from-may-next-year
x: http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-may-2016.pdf (Page 48)
xi: http://news.softpedia.com/news/phishing-emails-increase-789-percent-ransomware-is-their-favorite-payload-504750.shtml
xii: http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
xiii: http://risky.biz/RB407
xiv: https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
xv: https://cups.cs.cmu.edu/soups/2005/2005posters/11-gaw.pdf
xvi: https://github.com/blog/2190-github-security-update-reused-password-attack
xvii: https://blog.logmeininc.com/password-reuse-issue-affecting-logmein-users
xviii: http://status.gotomypc.com/incidents/s2k8h1xhzn4k
xix: https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet
xx: http://research.microsoft.com/pubs/227130/WhatsaSysadminToDo.pdf
xxi: https://www.cesg.gov.uk/content/files/document_files/Password_guidance_-_simplifying_your_approach_back_cover.pdf
xxii: https://blogs.technet.microsoft.com/enterprisemobility/2016/05/24/another-117m-leaked-usernames-and-passwords-new-best-practices-azuread-and-msa-can-help/
xxiii: http://research.microsoft.com/pubs/265143/Microsoft_Password_Guidance.pdf
xxiv: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q1-2016-state-of-the-internet-security-report.pdf
xxv: http://arstechnica.com/tech-policy/2016/04/fbi-paid-at-least-1-3m-for-zero-day-to-get-into-san-bernardino-iphone/
xxvi: http://www.reuters.com/article/us-usa-fed-cyber-idUSKCN0YN4AM
xxvii: http://www.hnkpmgciosurvey.com/press-release/
xxviii: http://www.darkreading.com/risk/average-cost-of-data-breaches-rises-past-$4-million-ponemon-says/d/d-id/1325921
xxix: https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
xxx: http://qz.com/628761/the-irs-is-using-a-system-that-was-hacked-to-protect-victims-of-a-hack-and-it-was-just-hacked/
xxxi: http://krebsonsecurity.com/2016/01/ftc-tax-fraud-behind-47-spike-in-id-theft/
xxxii: https://www.kyivpost.com/article/content/ukraine-politics/hackers-steal-10-million-from-a-ukrainian-bank-through-swift-loophole-417202.html)
xxxiii: https://www.sec.gov/news/pressrelease/2016-112.html
xxxiv: http://www.aspistrategist.org.au/rationale-offensive-cyber-capabilities/
xxxv: http://www.mofa.go.jp/files/000160279.pdf
xxxvi: http://csrc.nist.gov/publications/drafts/800-184/sp800_184_draft.pdf
xxxvii: https://www.us-cert.gov/ncas/alerts/TA16-091A
xxxviii: https://www.communications.gov.au/what-we-do/internet/stay-smart-online/alert-service/criminals-target-small-businesses-poor-server-security
xxxix: https://duo.com/blog/out-of-box-exploitation-a-security-analysis-of-oem-updaters

You are invited to attend an

Application Security Masterclass

Digital Protection Group

Brought to you by Commonwealth Bank's Digital Protection Group

Many of Australia's top software development teams have embraced Continuous Delivery models to push out a greater frequency of releases in a reliable way. But Continuous Delivery can present challenges to security assurance. The time required for 'point-in-time' penetration testing, for example, might span multiple development sprints, so the testing either delays the project, or there is no assurance around the final code committed to production.

In this masterclass, we will provide software developers a view of how using free open source tools and spending 30 minutes a day, they can remove a third of the bugs in their code before submitting it for testing – dramatically reducing the amount of time required for testing and helping to ensure they hit their release dates. We also take a provide advice on how to prioritise which bugs are the most critical to remediate.

The session will feature a presentation by UNSW lecturer Brendan Hopper on how to audit source code.

The masterclass provides an introduction to:

- How to identify and prioritise remediation of security flaws in your code before handing it over for testing
- What tools can aid the writing of more secure code
- How to audit source code

We'll also be announcing an exciting new research project we've sponsored at the University of New South Wales.

Best suited to: Software development teams

Monday July 11, 10am-1pm
Colonial Theatre,
201 Sussex St, Sydney

RSVP:
http://appsecmasterclass.eventbrite.com
(password is ASMC1)

CommonwealthBank