Signals

Quarterly security assessment

September 2018

CommonwealthBank

Contents

Horizon Scan

Upcoming events of interest

2018 Oct 9-11

Melbourne

AISA National Conference

The Australian Information Security Association hosts its annual conference for members. **https://cyberconference.com.au/**

2018 Oct 19

Melbourne

OWASP AppSec Day

Commonwealth Bank's Digital Protection Group will again be the principal sponsor of AppSec Day, the annual application security conference organised by the Open Web Application Security Project (OWASP). AppSec Day provides a forum for software developers, testers, DevOps engineers and security professionals to improve the security of their apps. The event features talks and hands-on technical workshops. Tickets are available from **http://appsecday.io**

2018 Nov 1-2

Melbourne

iappANZ 2018 Summit

The primary forum for privacy professionals in Australia and New Zealand, iappANZ, hosts its annual summit. This year the summit will discuss the "seismic shift" underway in privacy and data protection.

2018 Nov 1-2

Wellington, NZ

KIWICON 2038

After a brief hiatus, KIWICON is back with a distinctly cyberpunk vibe. KIWICON is the principal gathering of New Zealand and Asia-Pacific's cyber security researchers, practitioners and policymakers.

Welcome

Welcome to the 13th edition of Signals, CBA's quarterly security publication, prepared specifically for our customers, clients and partners. CBA's Digital Protection Group is committed to protecting the security of our customers, and contributing to Australia's cyber security community.

We face a challenging external environment in which cyber-attacks against high profile organisations across the economy are becoming increasingly commonplace. Responding effectively requires a combination of strong internal cyber capability, the right partners and world-class technology. Getting that mix right allows CBA to better serve the millions of Australians that rely on us for their banking needs.

The Signals team has done a great job bringing together commentary on trends and emerging developments as well as analysis around some of the key messages we're hearing about from you. In this issue, we focus on new regulations in the security space and examine the latest advice to consider when setting security policies.

As part of our ongoing commitment to improving the financial wellbeing of our customers and communities, we will continue to look for more ways to bring you interesting, relevant insights. You can reach my team with any feedback or suggestions at cyber-outreach@cba.com.au

Pete Steel
Acting CISO and Chief Digital Officer

Editorial

Melanie Timbrell
Senior Manager,
Cyber Outreach

US unmasks threat actors

"We'll continue to identify and illuminate those responsible for malicious cyberattacks and intrusions, no matter who or where they are."

Such was the warning issued by FBI Director Christopher Wray on September 6 as the US Department of Justice released a 179-page criminal complaint[77] against Park Jin Hyok, a computer programmer who - for over a decade - allegedly worked for the Chosun Expo Joint Venture, an affiliate of North Korean military intelligence.

The complaint is an extensive rap sheet. The Department of Justice alleged that Park Jin Hyok was involved in the 2014 hack of Sony, the 2016 theft of $81m from Bangladesh Bank, the attempted theft of "at least $1bn" from banks in various countries, attempts to infiltrate the systems of US defence contractor Lockheed Martin, and the 2017 ransomware attack known as WannaCry 2.0 which infected more than 400,000 machines worldwide[78].

Park is the latest example of the US demonstrating its resolve when it comes to pursuing and prosecuting the perpetrators of cyber-attacks.

In March this year, the US charged nine Iranians[79] with participating in a state-sponsored hacking scheme to steal sensitive information for commercial gain from universities, private companies and US government agencies.

Even more striking was the July grand jury indictment[80] of 12 Russian intelligence officers accused of hacking the Democratic National Committee and Clinton presidential campaign.

The sanctions and indictments put a face on what is often an anonymised threat. It reminds us of the human "army" of actors who are persistent, methodical and highly skilled.

Defending our organisations against evolving threats where the rules of engagement are yet to be established requires our own deep pools of talent from which to recruit and train skilled practitioners.

> "It reminds us of the human "army" of actors who are persistent, methodical and highly skilled"

In this issue we look at the urgent need to build the talent pipeline, with interviews from recent university graduates currently training in cyber. We draw the conclusion that early engagement, a broader approach to skills investment, and widening the recruitment net are key elements in securing that future workforce.

We also take an in-depth look at ransomware as a highly destructive threat to Australian businesses. In just a few years ransomware has become a lucrative revenue stream for cybercriminals, netting billions of dollars each year. The enduring question we examine is what can be done both to defend against the possibility of attack, and in the event of compromise.

Editorial Panel

Observations made in Signals are made using the confidence matrix and estimative language used by the US CIA. Our choice of words is very deliberate and based on both data and observations we source from our own telemetry and a measured degree of confidence in external sources.

Certainty	100%
Almost Certain	93% (give or take 6%)
Probable	75% (give or take 12%)
Even	50% (give or take 10%)
Unlikely or improbable	30% (give or take 10%)
Impossible	0%

Confidence in our assessments

High Confidence – based on high quality information from which it is possible to derive a solid judgment.

Moderate Confidence – based on information from trusted or reliable sources, without the necessary data or corroboration to warrant a higher level of confidence.

Low Confidence – the information is poorly corroborated, but is otherwise logical and consistent with a source's motivations.

Trends & Observations

Key trends observed during the quarter

Heightened awareness and new regulations drive breach reports and complaints

This quarter has seen a noticeable uptick in reporting of privacy and data protection issues, both domestically and across the globe. In July, the Office of the Australian Information Commissioner (OAIC) reported an increase in data breach notifications by Australian organisations under the Notifiable Data Breach scheme. It received 242 notifications between April and June[9], which Information Commissioner Angelene Falk said reflected growing awareness by organisations of their obligations under the scheme, which took effect in February 2018. A similar impact has been felt in Europe, where the General Data Protection Regulation (GDPR) took effect in May. Data protection complaints to the UK's Information Commissioner's Office (ICO) in the first 5 weeks of the GDPR regime were more than double the number of complaints from the same period the previous year.[10]

CHECKLIST

- Make your board and senior executives aware of the growing regulatory and public focus on data protection, and the potential implications for your business of a breach.
- Consult the Office of the Australian Information Commissioner for its guidance[11] for Australian businesses on the new requirements in the EU's General Data Protection Regulation and how businesses can comply with Australian and EU privacy laws.
- Ensure your organisation is prepared to respond well to a possible data breach and meets its legal obligations by creating a thorough data breach response plan. Read our Deep Dive "Into the Breach" in the last edition of Signals[12] for our insights on implementing such a plan.

Social media giants intensify fight against platform abuse

Social media networks are intensifying efforts to prevent abuse of their platforms by malicious actors.

Following reports of Russian influence campaigns soon after the 2016 US presidential election, some platforms initially understated the potential impact of such abuse[26]. A more proactive approach to moderation has been adopted in recent months, likely reflecting the seriousness and continued persistence by malicious actors to misuse these platforms. In August Google, Facebook and Twitter all announced the removal of "inauthentic" content relating to "influence campaigns" believed to originate in Iran.[27] Facebook also uncovered a campaign linked to Russia.

Locally, Facebook has said it is working with authorities to prevent misuse of its platform ahead of the 2019 Australian federal election[28]. Facebook is also piloting expanded security tools for election campaigns.[29]

CHECKLIST

- The actors conducting these influence operations via social media do so primarily in order to shape political discourse to achieve political outcomes. This could extend to the targeting of individuals or topics of public discussion that have relevance to your business.
- Given the growing reliance on social networks for marketing purposes, it's important for organisations to continue to monitor and be aware of the reported misuse and abuse of these platforms.

Security of healthcare data under scrutiny

The journey towards digital health continues to be afflicted by security and privacy concerns. In July, the Australian Government's My Health Record (MHR) program attracted criticism[20], particularly in relation to the system's controls over users' access to records and overly broad provisions in the legislation for third-party access in addition to a more general perceived lack of confidence in the system's security.

The MHR debate coincided with a breach of health records of 1.5 million patients in Singapore, resulting from an attack that the Singaporean government described as "deliberate, targeted, [and] well-planned," including repeated attempts to access the personal information of Prime Minister Lee Hsien Loong[21].

The value of medical records on the black market – in some cases valued higher than credit card information – means cybercriminal activity will continue to drive health breaches. The health sector was also the top sector for reporting data breaches in the OAIC's most recent data breaches report[22].

CHECKLIST

- The broad and intense public reaction to the My Health Record system is a strong reminder of the importance of a proactive approach to assuring stakeholders – including end users and data subjects – about the privacy and security controls of new systems.
- Continued targeting of health data emphasises the importance of user awareness training in the health sector. Commonwealth Bank offers clients access to eLearning modules for training staff in online safety. Talk to your account manager or relationship manager for access.

By the Numbers

12
Russian intelligence officers indicted for hacking the 2016 US election[1]

8000
remote access scams against Australian businesses this year[2]

$476 million
in online (card not present) payment fraud in Australia in 2017[3]

340 million
records containing personal information exposed to public by marketing firm Exactis[4]

Trends & Observations

Attackers directly targeting online reputation

Cyber-attacks often result in reputational damage for targeted organisations, though this is more commonly a secondary impact from a public breach of sensitive data or disruption to online systems. Attackers now appear to be pursuing a more direct route to exploiting organisations' sensitivity to brand damage.

In August, attackers extorted private companies by threatening to flood online review sites and search engine results with negative reviews (most likely by using bots).[23] In a more personally targeted campaign, cybercriminals also netted USD $500,000 from a "sextortion" scheme in which victims received an extortion email claiming their webcam had been hacked to film them while watching pornography[24]. To convince the victim of the veracity of this claim, the email included one of the victim's previous passwords, likely sourced from a previous data breach.

Extortion is a key tool for cyber criminals, as evidenced by schemes like these and the prevalence of ransomware campaigns. The FBI's Internet Crime Complaint Center received about 15,000 extortion-related complaints last year alone[25].

CHECKLIST

- Regularly monitor your social media channels and public-facing sites for evidence of unusual or anomalous behaviour.
- Educate your staff about extortion attempts and, more broadly, email-based scams. Commonwealth Bank offers clients access to eLearning modules for training staff on how to stay safe online. Talk to your account manager or relationship manager for access.
- If affected by ransomware or a similar extortion-based attack, consider seeking assistance from the Australian Cyber Security Centre via 1300 CYBER1.

Multi-factor authentication in focus

In previous editions of Signals, we have highlighted the ability of cybercriminals to compromise online accounts by obtaining login credentials through phishing or purchasing stolen credentials online.

To mitigate this risk, digital services are increasingly looking to multi-factor authentication (MFA) or two-factor authentication (2FA), which require users to provide a further "factor" of authentication in addition to their username and password (such as a unique code).

In August, following a series of account compromises, Instagram announced support for third-party multi-factor authentication apps[13]. Microsoft also mandated MFA for admin users of its Azure cloud service[14]. However, the use of SMS-based MFA (where a user receives their unique code via SMS text message) has come under scrutiny.

After a serious data breach in August despite having 2FA enabled, popular internet forum Reddit concluded that "SMS-based authentication is not nearly as secure as we would hope"[15]. Commentators increasingly observe attackers deploying "SIM swaps" and phone porting to circumvent SMS-based 2FA.[16]

CHECKLIST

- Review the Australian Cyber Security Centre's guide on Multi-Factor Authentication[17]. The guide describes the importance of MFA and outlines different MFA methods.
- For your most critical accounts, consider deploying hard tokens or security keys. Google reports that it has had no account compromises since requiring all its employees to use physical tokens in early 2017.[18]
- The Q1 2018 edition of Signals includes a deep dive "Proven defences for pocket change", which describes the value of password managers and MFA, and how to enable the latter for various popular online services[19].

Authorities warn IoT devices being used for malicious activity

Researchers have for some time warned of likely security risks from the growing number of internet-connected devices deployed with sub-standard security protections. Various signs indicate these risks are materialising.

Malware samples targeting Internet of Things (IoT) devices collected by Kaspersky Lab have increased three-fold in the first half as compared with the whole of 2017.[30]

The Mirai family of malware has proven most popular, and cracking Telnet passwords remains the most popular attack, Kaspersky said.

In August the FBI warned that cyber actors were "actively" searching for vulnerable Internet of Things (IoT) devices – especially in developed nations – through which they can route traffic and disguise the source of their malicious activities .

Reflecting this assessment, security researchers in September documented the rapidly growing Hakai IoT botnet - first spotted in June and which has since burgeoned through targeting vulnerabilities in well-known router brands[32]. The passing of the US' first IOT security bill in August by the California legislature[33] and recent investments[34] by ventures and start-ups in IoT security – notably by prominent Israeli firm Cellebrite[35] – are positive signs that momentum is also building in response to the IOT threat.

CHECKLIST

- Authorities recommend regularly rebooting network devices, as this can potentially disrupt any malware on the device.
- The FBI offers a range of good advice to protect IoT devices, including changing default usernames and passwords, ensuring devices are patched, and ensuring firewalls are configured to block traffic from unauthorised IP addresses.[36]

By the Numbers

US$12.5 billion
in global Business Email Compromise losses over 4.5 years[5]

242
data breach notifications in Australia between April-June 2018[6]

59%
of reportable data breaches are malicious or criminal attacks[7]

15 million
credit card numbers stolen in US alone by cybercrime group FIN7[8]

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Deep Dive:

Defending your business against ransomware

John Hare
Executive Manager, Cyber Outreach

In a constantly evolving cyber threat landscape, ransomware remains an enduring fixture on our business customers' list of concerns. Customers are interested to know the latest advice on avoiding falling victim to a ransomware attack and how to respond and recover, should the worst happen.

This Deep Dive will investigate these issues and will also address the thorniest question of all: to pay or not to pay?

Typical stages of a ransomware infection

1. Lure

The victim is tricked into downloading a malicious 'dropper' file, often via:

a) An email attachment
b) Visiting an infected website
c) A fake software update or app

2. Dropper

The 'Dropper' is a simple, lightweight program designed to:

a) Evade detection
b) Download the ransomware 'payload' from the attacker's C2 ('Command and Control') server

3. Payload

The ransomware is a larger program that encrypts files or denies the user access to the computer

4. Demand

The objective of the malware is to extort a ransom (often payable in cryptocurrency) in return for the decryption key that will unlock the files or to restore access to the computer

What is ransomware?

Ransomware is malicious software (malware) that either:

- encrypts files; or
- blocks access to a computer or mobile device.

Ransomware demands a ransom, often to be paid in cryptocurrency, for the decryption of the files or unlocking of the device. It may be insidious, but this is malware with history: the first known attack, the so-called AIDS Trojan, took place as far back as 1989, with the malware being distributed by floppy disks the attacker claimed contained a program which analysed an individual's risk of contracting AIDS.[44]

Whilst the means of delivery may have changed over the years and the sheer scale of the problem has increased exponentially, ransomware operators still often rely on fooling users into doing the wrong thing. From a business perspective, online behaviour of staff remains the biggest vulnerability.

Preventing ransomware attacks

The Australian Cyber Security Centre (ACSC) website[83] contains information and links to a wide range of prevention measures. No single measure will provide a silver bullet. As with many cybersecurity threats, defence-in-depth is the best strategy.

However, user awareness is particularly important, given the majority of ransom attacks rely on insecure user behaviour.

Phishing remains a key mode of ransomware (and other malware) infection, and users should be trained to avoid email 'lures'. These are emails with malicious attachments or links to malicious sites.

The recipient is enticed to open the email and execute the attachment or click the link, often through a sense of urgency engendered by the phishing email (fake bills, invoices, penalty notices).

Other key prevention methods include:

- Using and regularly updating reliable anti-virus software
- Disabling macros in Microsoft Office applications, since these may be used in malicious attachments to emails to download ransomware
- Enforcing a regular security patching policy to ensure all mobile devices, laptops and desktops are using the latest versions of their operating systems and applications
- Keeping abreast of the latest cyber threats by referring to sources such as Stay Smart Online, which can also provide alerts to new and emerging threats

What to do should the worst happen

Given the prevalence of ransomware, you may wish to consider having an incident response plan that specifically contemplates this threat. Accessing back-ups will be a key part of this plan. You should identify your critical data and ensure this is backed-up off-line at a cadence that reflects how quickly your critical data

Deep Dive:

Defending your business against ransomware

> Some ransomware is designed to **scare and to attract payment**, without any intention of enabling restoration of that data

changes over time.

The cost of frequent back-ups may necessitate a difficult discussion as to how much irretrievable data loss is acceptable to your business.

Europol provides a potentially valuable service through the 'No More Ransom' project.[38] This website offers decryption tools for a number of ransomware strains, provided by law enforcement agencies and commercial partners.

To pay or not to pay?

But what if you don't have back-ups and external resources can't help in restoring your critical data?

The ACSC is very clear in its advice: "Never pay a ransom demanded by ransomware. There's no guarantee paying will restore your files, and paying a ransom could make you vulnerable to further attacks. Report the infection and seek help from a cyber security expert."

However, some Australian businesses are ignoring this advice. According to research by Telstra, 47% of Australian businesses that found themselves victims of ransomware paid the ransom[39]. 86% of Australian businesses who paid a ransom were able to retrieve their data after the payment, according to Telstra.

According to research by Telstra...

47%

of Australian businesses that found themselves victims of ransomware paid the ransom[39] and

86%

of Australian businesses who paid a ransom were able to retrieve their data after the payment

This latter statistic may make paying the ransom look like a relatively attractive option over significant irretrievable data loss. But let's examine the consequences of paying a ransom in greater detail.

Breaking the law

It's important to realise payment of a cyber ransom may not be legal and as such you should seek legal advice before making a decision on what to do.

Paying a ransom is no guarantee of getting your data back

In this respect, ransomware is increasingly resembling 'real-world' extortive crime and kidnap, where acceding to a ransom demand may not secure safe and timely release, and may simply lead to a further ransom demand. The attack on Kansas Heart Hospital in May 2016 is one such example. The hospital paid a ransom demand following a ransomware attack that encrypted critical patient files. However, rather than decrypting the files, the criminals demanded another ransom, which the hospital refused to pay, determining this was no longer 'a wise manoeuvre or strategy'[40] .

Then there is the issue of the ransomware operator's intent and competence. Some ransomware is designed to scare and to attract payment, without any intention of enabling restoration of that data, or poorly-coded ransomware may make restoration impossible. The infamous worldwide WannaCry attack of May 2017 was one such case. The ransomware demanded $300 or $600 payable in Bitcoin, but accession to this demand would not have led to the restoration of data. The malware did not assign paying victims a unique bitcoin address, so had no way of automatically verifying whether the victim had paid the ransom[41].

When is ransomware not ransomware?

When it is data-destroying malware, masquerading as ransomware! The "Not-Petya" malware attack of June 2017 involved malware that presented as ransomware which closely matched a previous strain called Petya. However, victims quickly found that there was no facility to actually pay the ransom. Instead the malware not only locked users out of their devices, but also destroyed data and wiped memory in the process[47].

The USA, UK, Australia and Canada attributed the attack to Russia[48]. Earlier this year the White House said Not-Petya was originally designed to disrupt Ukrainian businesses and utilities.[49]

The malware was distributed via a weaponised update of tax preparation software commonly used in Ukraine. However, whether by design or neglect, the impacts were felt well beyond the Ukrainian target set, with several multinational companies becoming collateral damage. WPP[50], Merck & Co[51] and Maersk were just some of the household names to be affected. Maersk in particular reported between US$200 and US$300m in lost revenue as a direct result of the disruption caused by Not-Petya[52].

Not-Petya demonstrated the speed with which criminals or nation states exploit new intelligence. The EternalBlue exploit that facilitated the spread of Not-Petya had been publicly leaked by a hacker group named Shadow Brokers in April 2017[53]. That exploit was employed in the WannaCry malware four weeks later and again in Not-Petya the following month.

Deep Dive:

Defending your business against ransomware

> Crypto-jacking is the use of **malware to steal computing power**, rather than money or data, by surreptitiously mining for cryptocurrency on the victim's computer

Vulnerability to further attacks
By paying a ransom you have identified yourself as a compliant target and may increase the prospect of being attacked once again, by the same criminals or a different group.

Securing the ecosystem
Ransomware will endure as a profitable enterprise for criminals as long as victims are willing to pay the ransoms. By paying a ransom you are helping to perpetuate the problem. The Europol-sponsored initiative, 'No More Ransom' advises: "if the ransom is paid, it proves to the cybercriminals that ransomware is effective. As a result, cybercriminals will continue their activity and look for new ways to exploit systems that result in more infections and more money on their accounts".[42]

What next?

Some analysts have argued that we may have reached, or are soon to reach "peak ransomware", since many cyber criminals are turning to crypto-jacking as a profitable alternative. Crypto-jacking is the use of malware to steal computing power, rather than money or data, by surreptitiously mining for cryptocurrency on the victim's computer.

However, the fall in value of cryptocurrency may mean crypto-jacking is not as attractive as it was. It seems that ransomware will continue to be a fact of life for businesses for the foreseeable future, fuelled by the ease with which criminals can obtain the required tools and the willingness of their victims to pay up.

Meanwhile both the design of malware and the business models that support it will continue to evolve. New malware strains demonstrate ever-more advanced capabilities, including encryption algorithms some analysts believe are all but unbreakable.[43]

Against this background, it is incumbent on any responsible business to ensure it has layered defence to prevent a ransomware attack, which must include staff education. It must also have a plan to respond to a ransomware attack and ensure there are adequate back-ups of critical data. Failure to take these steps will leave the affected organisation with no good options: facing either irreversible data loss and disruption or the prospect of paying a ransom. This latter option certainly does not guarantee the return of your data, but it will certainly profit criminals and further perpetuate the ransomware threat.

Adam Fisch contributed to this Deep Dive.

What has caused the proliferation of ransomware?

The relative ease with which cybercriminals can cheaply obtain ransomware or even Ransomware-as-a-Service (RaaS) has dramatically lowered barriers to entry. Aspiring cybercriminals with limited technical know-how can now quickly and easily purchase user-friendly malware that is provided via an internet-based vendor platform.

This malware can be customised with a specific target in mind or enhanced by spam networks. RaaS also offers enticing business models with criminals paying a single fee or having a profit share agreement with the developer. The Hostman RaaS, for example, costs affiliates $49.95 for unlimited use and has an average ransom payment of $600[45].

The Dark Web contains a number of underground marketplaces for ransomware and RaaS. In this thriving market, competition is fierce and vendors seek to differentiate themselves through unique features to evade detection or increase success, or by attractive commercial arrangements such as franchising and profit sharing.

The opportunity for criminals comes at an immense cost to its victims. Home Affairs minister Peter Dutton told a conference in April 2018 that "on conservative estimates, cybercrime currently costs Australians upwards of $1 billion per year."[46]

Deep Dive:

Building the cyber talent pipeline

Melanie Timbrell
Senior Manager, Cyber Outreach

Martha McKeen
Senior Manager, Cyber Outreach

It's been 20 years since McKinsey coined the term 'war for talent'. Its enduring usage in management lexicon speaks to the aptness of the phrase in reflecting the struggle to attract and retain quality staff, with cyber security now a key battle front.

Many column inches have been dedicated to the global shortage of skilled cyber technicians and the projected widening of the gap between supply and demand.

Typically however, the factoids which tend to be quoted look at the aggregate numbers of projected unfilled vacancies across the spectrum of IT security jobs. While the magnitude of these numbers serve as a good wake-up call to signal the scale of the projected shortfall, they do not tell the full story.

The other side of the coin for organisations is the overall gap in coverage. That is, not just thinking about the number of people in seats, but also thinking at a higher level about whether the right mix of skills is present to meet the challenges of a world in which the goal posts keep shifting.

Commonwealth Bank's General Manager, Cyber Security Centre, Brendan Hopper speaking at an industry event recently likened the difference in skills required to write code as opposed to testing the security of software to the distinction between an author and a proof reader.

"As an industry we now have specialists who are dedicated, not to writing code, but to going through software and finding classes of bugs and vulnerabilities and making software more secure," Hopper said.

The reality for some organisations is that dedicated, specialised cyber resources may be neither practical nor affordable. But for those which identify the need to hire cyber specialists and have the wherewithal to do so the key question is how to ensure sufficient talent is available into the future.

Start cultivating relationships early

The risk posed by gaps in cyber security talent is not being felt in the private sector alone.

'Developing skills and expertise' formed a key part of the government's 2016 Cyber Security Strategy[54] in recognition of the shortage in trained cyber security professionals and the targeted actions required at all levels of the Australian education system to address this.

Organisations such as CBA are taking this remit seriously, looking to cultivate the right cyber mindset earlier than ever before with initiatives such as a government-backed industry alliance to bring cyber security into Australian high schools.

Through a series of challenges covering topics such as web application security and network security the thinking behind this is the earlier we start to focus on the core skills and competencies we need, the earlier we can inspire students to follow pathways that will lead to cyber security careers.

Traditionally, however, it is universities which have formed the recruiting ground for future talent and indeed many of the recent graduates we spoke to for this article ended up with their employer as a consequence of relationships formed at university.

Be flexible in your recruitment approach

Graduate programs, cadetships and internships are still in high demand among those pursuing tertiary level study in disciplines such as computer engineering, giving a sense of structure at a time during which a sense of certainty is appealing as many students transition to full-time work for the first time.

One common theme, however, was the desire to see more flexibility in the recruitment process to cater for different finishing times in the academic year.

"Spotting the talent and offering them a role 12 months before they graduate is a great strategy, but many students don't start looking until later in the year, so a certain amount of flexibility is required to get the best talent. That also includes things like flexible start dates, and mid-year entry," said CBA Enterprise Services graduate, Adam Smallhorn.

Several of the graduates also spoke about the importance of early initial engagement in providing incentives for graduates to apply. Organisations which engaged later with cut-off dates after the first tranche tended to have a smaller pool of interested applicants as some

6 Steps to attracting cyber talent

1. Engage early by connecting with a range of educational institutions at varying stages of students' schooling
2. Get involved in encouraging an interest in cyber security through activities such as sponsoring 'capture the flag' challenges, industry immersion programs and on-campus events
3. Offer flexibility in the recruitment process to cater to different start dates and backgrounds
4. Once in the organisation, offer flexibility to try different things in addition to support and mentorships to help people find the right role
5. Focus on what you can't teach – attitude and aptitude
6. Offer continuous learning opportunities and programs

Deep Dive:
Building the cyber talent pipeline

students were already committed, observed the interviewees. Many structured graduate programs are also currently not open to international students which, Smallhorn says, may be closing the door on a pool of talent which has been trained to the same standard as local students.

A move away from prescriptive online tests for selection is a key callout from Brody Noonan, Cyber Security Engineer at Bankwest, who in spite of applying for the Bankwest grad program twice and missing out, nonetheless ended up at the organisation in a technical role.

"You can always teach the tech side of a role with on-the-job experience so I would think it should be more about the person and their motivations," Noonan said.

Atlassian SecurityIntelligence Intern Clancy Rye says the barrier to entry for security can feel quite high and expressed the view that ultimately education should be a way to supplement and assist an otherwise ongoing lifestyle of "learning and tinkering".

When asked about the skills required to perform his current role, which is a mix of incident detection and response, vulnerability detection, threat intelligence and cultural uplift, Rye spoke about the attributes required over and above the technical know-how.

"Technical competence and understanding are obviously quite important, but so is common sense, the ability to think critically and keep your head under pressure.

"Being personable and able to work effectively in a team is also incredibly important, as is the drive to learn and improve."

Profile

Name: Adam Smallhorn

Current role: Graduate, Enterprise Services, CBA

Degree: Computer Engineering, UNSW (2017)

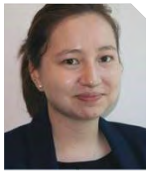
Top three things you looked for in an employer/role:

1. Flexibility and work/life balance

2. An organisation that gives back to the community and industry

3. Employees who are active and influential in the industry

Profile



Name: Jessica Mitchell

Current role: Graduate, Enterprise Services, CBA

Degree: Bachelor Science in Information Technology, UTS (2015)

Top three things you looked for in an employer/role:

1. Ability to explore options for working in different roles

2. Work / Life balance

3. Good reputation for people and culture

CBA's ecosystem partnerships

- Partnership with the University of New South Wales to create a specialisation in cyber security within UNSW's computer science degree. The program, which launched in 2015, has supported the growth of new subjects in security like web application security, digital forensics, offensive security and incident response
- The annual CommBank cyber prize awards Australia's top performing academic cyber security students at five participating universities – UNSW, University of Sydney, Edith Cowan, RMIT and Monash University
- CBA is a major sponsor of the Cyber Security Challenge Australia[56]
- CBA has partnered with the University of Sydney's Australian Computing Academy, AustCyber, Westpac, NAB, ANZ and BT Global to deliver a series of cyber security challenges for high school students. The first of a series of challenges will launch in November to Australian schools nationwide
- CBA is a Gold sponsor of the National Computer Science School and Girls' Programming Network
- CBA is a major sponsor of the Access for Women program at UNSW
- CBA in partnership with the department of Home Affairs supports the Women in Cyber Security Mentoring Experience program for up and coming female cyber security professionals

Provide opportunities to learn from the get-go

Flexibility in the recruitment process is one thing, but of additional appeal to many grads is the opportunity to experience multiple roles before making a decision on where in the organisation they'd like to end up based on both what they enjoy and where their strengths lie.

Opportunities for continued professional development and options to learn and build skills were of particular appeal to those joining cyber security functions from university.

"Coming straight from uni, the biggest change was there it was all general knowledge and concepts of how security works. Then you come into a role and the challenge is to translate that. You are looking at a real product, trying to learn and understand it from scratch, then relate that back to the knowledge you have and figure out what it means for the business," said Bankwest's Noonan.

An organisation with the capacity to provide ongoing training was also key: "For me that's one of the things that attracted me to a bigger organisation. I felt a small company would pay you and expect you to know everything, whereas in a bigger company there would be more opportunity to learn products and the industry in a structured way," Noonan said.

For CBA Cyber Security Analyst Jessica Mitchell, the provision of training is not just about the option to continue developing her skills and gaining further accreditation, it also sends a positive message from the organisation regarding a commitment to investing in her future, which can be a benefit of the current skills shortage.

"The skills shortage means there are opportunities to progress and move from role to role and they support you. It's also nice to think you're working to protect the bank and customers," she said.

Deep Dive:
Building the cyber talent pipeline

> “Businesses looking for people with traditional **technology credentials to fill cyber security vacancies** may be limiting the talent pool”

Making and shaping the talent

While developed grad programs with structured ongoing training opportunities may be easier for larger organisations to accomplish, one option open to those of varying sizes and degrees of sophistication is PR work aimed at drawing the talent to you.

Cybersecurity Associate at PwC, Peter Capon references the Industry Based Learning (IBL) program he participated in during his degree.

“I completed a placement at a large financial services organisation within their Information Security team. The experience was great, however I found the organisational structure to be quite rigid in terms of career pathways. From this experience I knew I eventually wanted to work somewhere which offered me a high degree of flexibility in terms of career experiences and opportunities, and consulting was an area which met that criteria,” Capon said.

“Around the same time as my IBL placement I participated in CySCA (Cyber Security Challenge Australia), a 24-hour hacking challenge. PwC was one of the main sponsors of the event, and I appreciated how they were actively investing in upskilling the next generation of cyber security professionals. This was what first interested me in working for PwC.”

Creating a name and a reputation for your organisation as one in which employees are likely to meet future influencers may be playing the long game, but it is an approach that nonetheless has the potential to be effective, particularly in attempting to recruit from non-traditional disciplines and backgrounds – a strategy which is gaining popularity.

A 2017 article published in the *Harvard Business Review* pointed to the reality that businesses looking for people with traditional technology credentials to fill cyber security vacancies may be limiting the talent pool and is at odds with the manner in which the “bad guys” are growing their ranks.[55]

The article, written by IBM’s General Manager of Security, Marc van Zadelhoff spoke about IBM’s “new collar” jobs program, which looked at the underlying characteristics of a successful cyber security professional: natural curiosity, strong ability to problem solve, ethics and an understanding of risk.

IBM found those with these traits had the ability to quickly pick up the technical skills through a combination of on-the-job training and modern education programs.

Such has been the commitment to this approach that 20% of IBM’s US hiring in cyber security since 2015 has been “new collar” jobs, according to van Zadelhoff.

Outreach activities and investments aimed at strengthening community capability are among those which will be at the forefront of enabling these kinds of alternative approaches to addressing the skills shortage challenge.

Here at CBA we often make reference to “uplifting the ecosystem” and through connecting with government, investing heavily in partnerships with both industry and educational providers we are acting in the belief that it’s in everybody’s interests to grow our collective cyber skills and knowledge.

These are seen as necessary pathways not just to lifting the number of people we have equipped and available to fill vacant roles in the future, but also to ensuring we have the skills we need to adopt a ‘collective defence’ mentality, keeping everyone more secure.

Profile

Name: Brody Noonan

Current role: Cyber Security Engineer, Bankwest

Degree: Computer Science, Edith Cowan University (2016)

Top three things you looked for in an employer/role:

1. Opportunity to work in a dedicated security role
2. Opportunity for continued professional development
3. Opportunity for interesting work

Profile

Name: Clancy Rye

Current role: Security Intelligence Intern, Atlassian

Degree: Computer Science, UNSW (2018)

Top three things you looked for in an employer/role:

1. An engaging, rewarding and fulfilling role
2. A collaborative, friendly culture
3. Competitive salary, benefits and flexibility

Profile

Name: Peter Capon

Current role: : Cyber Security Associate, PwC

Degree: : Information Technology & Systems, Monash University (2015)

Top three things you looked for in an employer/role:

1. Opportunity to work across different capabilities within cyber
2. Somewhere staff enjoy working
3. Opportunity to do meaningful, interesting work

Regulatory and Legal

New laws and legal precedents relevant to security strategy

> “Australia’s decision represents **growing concerns by governments** and businesses alike”

Dedicated minister for cyber security falls in Government reshuffle

Stronger ministerial accountability for cyber security was a key expectation from industry during the Government cyber security review that culminated in the national cyber security strategy released 2016[57].

The creation of a Minister for Cyber Security, most recently held by Angus Taylor, appeared to have answered that need. However, there is no longer a dedicated ministerial position for cyber security, following Prime Minister Scott Morrison’s cabinet reshuffle. Cyber security functions continue to be managed by the Department of Home Affairs under Minister Peter Dutton. Shortly before the reshuffle, Angus Taylor – as Minister for Cyber Security – had announced a revitalised government approach to cyber security[58] and formally opened the Australian Cyber Security Centre[59].

CHECKLIST

- The national cyber security strategy saw the establishment of various government bodies and agencies tasked with improving the nation’s cyber resilience. These organisations include the Australian Cyber Security Centre, Joint Cyber Security Centres[60] and AustCyber[61] and offer a means – at least at an operational level – for industry to contribute to and receive assistance on national initiatives in cyber security.
- The Australian Cyber Security Centre in particular is a key vehicle for industry-government collaboration, particularly in the areas of threat information sharing and education and awareness. Organisations can contact the ACSC via 1300 CYBER1.

Further steps towards government access to encrypted communications

Under new legislation introduced by the Australian Government, communications companies could receive a mandatory “technical assistance notice” to assist in decryption of communications. The notice is one of a series of tools outlined in the Assistance and Access Bill 2018, which the Government argues will better enable law enforcement to investigate serious crimes in the digital era[62]. While the Government insists the new powers do not require companies to introduce ‘backdoors’ (or systemic weaknesses) into their systems, the bill has attracted criticism. Industry groups including the Digital Industry Group Inc – which represents large technology companies such as Facebook, Google and Twitter – and the Internet Architecture Board voiced concerns that the bill will ultimately weaken overall security in internet infrastructure[63]. The bill was introduced to parliament in late September.

CHECKLIST

- Review the Government’s explanatory document on the Assistance and Access Bill, in particularly the framework by which it will seek industry assistance.[64]
- Data protection is a strong expectation of consumers and regulators alike, and organisations should continue to protect client data with the strongest available security mechanisms.

Government bans Huawei from Australian 5G network

Following months of public debate and speculation, the Australian Government in August formally banned Chinese telecommunications equipment provider Huawei from supplying equipment to Australia’s 5G network[65]. Though Huawei is one of the world’s largest suppliers of telecommunications equipment, in its decision the Government cited security concerns and, specifically, the risk of utilising “vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law”. India has reportedly followed suit[82] and Japan is said to be considering a similar ban[66].

Australia’s decision represents growing concerns by governments and businesses alike in relation to securing the supply chain.

The Huawei decision was criticised by China as prejudicial and the Australian arm of the company denies it’s controlled by Beijing.[84] After the ban, the ABC website was blocked in China for breaching the country’s regulations.[67]

CHECKLIST

- The security standards of potential suppliers and their ability to meet security obligations should be key factors in procurement decisions for all organisations, not just governments. Ensure you have an active security compliance program that compels suppliers and other partners to protect your data to an expected standard.
- Globally, national governments have intensified their focus on cyber security and data protection regulation in recent years, to protect their citizens and national interests. Businesses with a global presence should make themselves aware of these regulations, and the implication of differences across various regions.

Better Practice

The latest advice to consider when setting security policies

Updated standard ISO/IEC 27005

For: CISOs, risk, regulatory and compliance teams
The International Standards Organization (ISO) has released an updated version of its security risk management guidelines, ISO/IEC 27005:2018[72]. The standard is one of a dozen standards in the 27000 series of standards that outlines best practices in information security. ISO/IEC 27005 outlines the "why, what and how" for organisations seeking to manage information security risks.
What's changed? *ISO/IEC 27005 has been updated to reflect a new version of ISO/IEC 27001.*

US government DMARC adoption progress report offers useful insights

For: CISOs and security teams
Domain Message, Authentication, Reporting and Compliance, or DMARC, is a free standard that can be used to protect your organisation from email spoofing based attacks. Given the increase in email-based attacks, including business email compromise, the US Government last October mandated the implementation of DMARC for agencies that operate government email domains. Its most recent progress report[73] offers useful insights into how to implement this increasingly important email security measure.

Setting up two-factor authentication (2FA)

For: Businesses owners, security awareness teams and all staff
The UK's National Cyber Security Centre has created easy-to-consume advice[74] on setting up two-factor authentication for important accounts. As detailed in the Trends and Observations section of this edition of Signals, the need for 2FA and multi-factor authentication to protect critical online services continues to gain focus. The NCSC's guide describes types of 2FA and how to set them up.

Security advice from the Australian government

For: Businesses owners, security awareness teams and all staff
The Australian Government has created a new website – cyber.gov.au[75] – offering security advice to businesses and individuals, as part of the opening of its Australian Cyber Security Centre in August. Among the topics for businesses are how to mitigate cyber security incidents, patching systems and cloud security.

FBI launches education campaign

For: Businesses owners, security awareness teams and all staff
Wary of efforts by cyber actors to influence US elections, the FBI has launched a new initiative[76] to educate political campaigns to protect themselves against cyber threats. But the videos – which cover everything from password management to device hardening and incident response – are a great tool for any business looking to secure itself.

Phish Eyes

Recent phishing lures for your security awareness

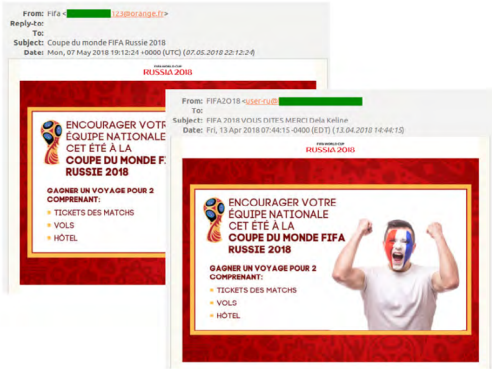
Report hoax emails to hoax@cba.com.au

Capitalising on currency

The last quarter saw a number of opportunistic phishing schemes coming to the fore as attackers looked to exploit major events, including intentionally targeting those more likely to click a link or inadvertently provide their credentials.

The FIFA World Cup held in Russia from June to July saw a spate of activity aimed at phishing personal information, enticing users to click on malware links or to open malicious attachments.

The most prevalent scam involved fraudsters posing as sellers or third party providers of match tickets to fans who may have missed out in the general sale via official channels.



Source: https://securelist.com/2018-fraud-world-cup/85878/

With fans desperate to see their teams in action, many were prepared to pay well above the face value of tickets, making them susceptible to scams of this sort.

When brand trust is used against you

'Brandjacking' is the term commonly used to describe cyber scams in which criminals fake an email or website that looks like one belonging to a well-known and recognised company.

For years advertisers have tapped into our trust of known brands and products to give us a sense of security around our purchase decisions. But when it comes to brandjacking, that trust is being used against us (fig1).

Looking at this example, the branding is what you would expect and in many cases, such as this one, the malicious link is hidden and it also looks as though it comes from a similar email to what you might anticipate.

The complexity and sophistication of campaigns has evolved as demonstrated in the following sequences where a phishing page can be used across multiple devices. This means the campaign can be distributed to a wider audience via emails and SMS, increasing the likelihood of someone getting hooked. This effectively allows the attacker to use the same landing page through multiple methods of distribution (figs 2&3).

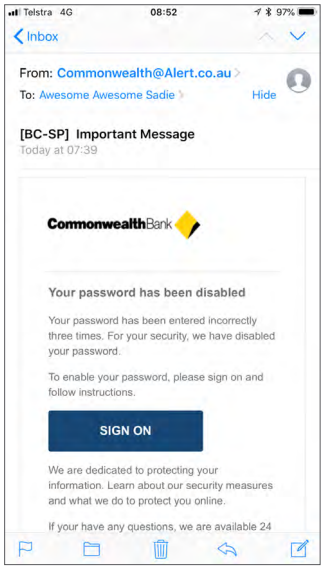


fig1 *Source: CBA Cyber Security Centre*

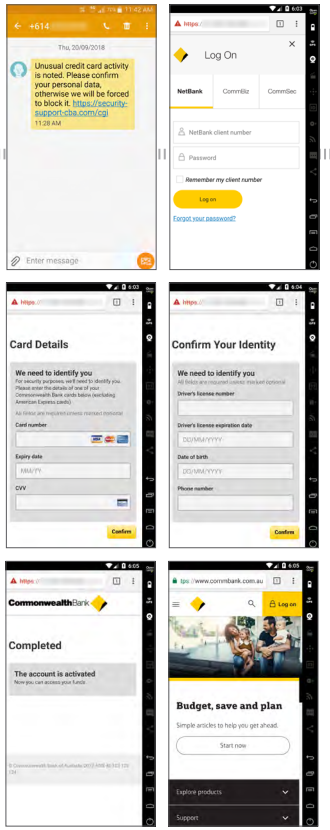


fig2 *Source: CBA Cyber Security Centre*

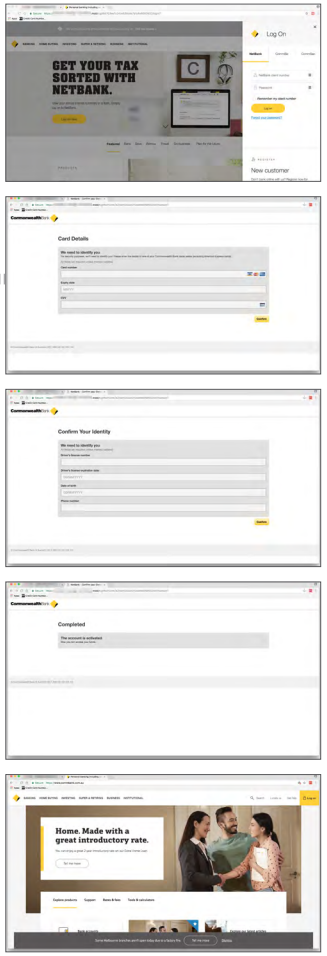


fig3 *Source: CBA Cyber Security Centre*

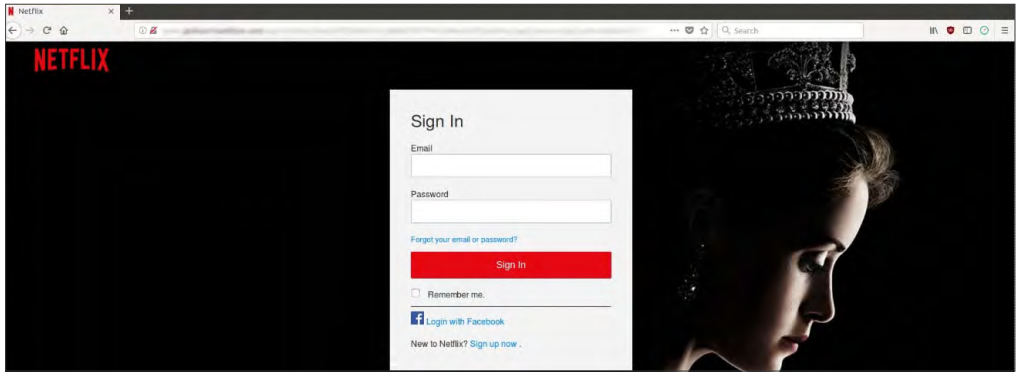
At the successful completion of the phish, the most common technique for handling the victim is to redirect them from the phishing site to the legitimate website they thought they were interacting with. The aim is to make the victim think they have either completed the required task or that it must have been a glitch and they are now logged off in order to avoid raising the alarm.

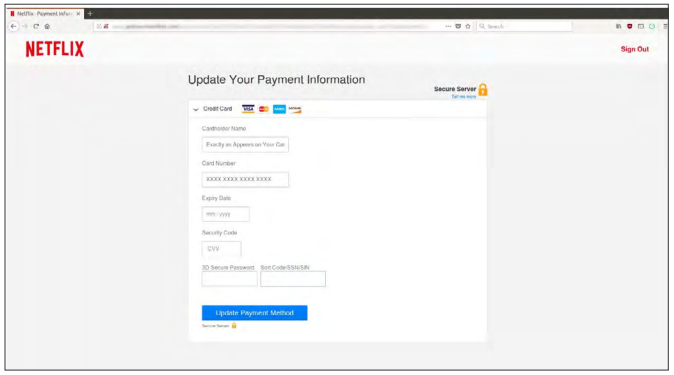
The year to date has seen a number of big tech brands targeted, including Netflix. In April this year the Australian Communications and Media Authority (ACMA) used the Netflix scam to highlight the increasing sophistication of scammers.

The Netflix scam starts with an email, commonly delivered with the subject line 'Netflix membership on hold' and tells the

Phish Eyes

> These scams **seamlessly replicate the experience of using a company's legitimate website**, whether it is being accessed through a smartphone, tablet or desktop computer





Source: https://www.mailguard.com.au/blog/netflix-scam-180329

recipient that Netflix "failed to validate your payment information", requesting they undertake a verification process. Upon clicking the link, the target would be taken to a phishing website that looks like the real Netflix logon and requested to enter their email address, Netflix password and credit card details.

ACMA named the fake site as an example of 'smart phishing' – a scam which "dynamically adapts to your online interactions and prompts you for your data in a clever and realistic way."

"These scams seamlessly replicate the experience of using a company's legitimate website, whether it is being accessed through a smartphone, tablet or desktop computer," according to ACMA[81], which explained how the Netflix scam works:

1. When you 'sign in', the fake website feeds your username and password to the real website and, if the log in details are correct, retrieves your first and last name. If the details are incorrect, you will receive the normal login error message and be prompted to enter your correct details

2. The next page shows the account verification form where the first and last name fields are pre-populated with data obtained from the real Netflix website

3. Once you complete the rest of the fields, you are prompted to share your credit card details

4. At this point the fake site dynamically changes – asking for additional authentication based on the credit card number, for example using 'Mastercard SecureCode' or 'Verified by Visa' boxes

Endnotes

1 https://www.scamwatch.gov.au/news/beware-scammers-wanting-access-to-your-computer-and-bank-account

2 https://www.scamwatch.gov.au/news/beware-scammers-wanting-access-to-your-computer-and-bank-account

3 https://www.auspaynet.com.au/sites/default/files/2018-07/PaymentFraudStatistics_Jan-Dec2017.pdf

4 https://www.wired.com/story/exactis-database-leak-340-million-records/

5 https://www.ic3.gov/media/2018/180712.aspx

6 https://www.oaic.gov.au/media-and-speeches/news/notifiable-data-breaches-second-quarterly-report-released

7 https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018#executive-summary

8 https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

9 https://www.oaic.gov.au/media-and-speeches/news/notifiable-data-breaches-second-quarterly-report-released

10 https://www.independent.co.uk/news/business/news/data-breach-complaints-increase-gdpr-came-into-force-cybersecurity-a8506711.html

11 https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation

12 https://www.commbank.com.au/content/dam/commbank/assets/business/can/business-insights/signals/signals-q2-2018.pdf

13 https://instagram-press.com/blog/2018/08/28/new-tools-to-help-keep-instagram-safe/

14 https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Baseline-security-policy-for-Azure-AD-admin-accounts-in-public/ba-p/245426

15 https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/

16 https://krebsonsecurity.com/2018/08/reddit-breach-highlights-limits-of-sms-based-authentication/

17 https://acsc.gov.au/publications/protect/multi_factor_authentication.html

18 https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/comment-page-3/

19 https://www.commbank.com.au/content/dam/commbank/assets/business/can/business-insights/signals/Signals-Q12018.pdf

20 http://www.abc.net.au/news/science/2018-07-16/my-health-record-experts-say-its-safe-privacy-concerns-remain/9981658

21 https://www.singhealth.com.sg/AboutSingHealth/CorporateOverview/Newsroom/NewsReleases/2018/Pages/cyberattack.aspx

22 https://www.oaic.gov.au/media-and-speeches/news/notifiable-data-breaches-second-quarterly-report-released

23 http://thehill.com/policy/cybersecurity/404477-hackers-increasingly-target-reputations-through-reviews-sites-experts

24 https://motherboard.vice.com/en_us/article/xwk3wq/hackers-sextortion-half-million-blackmail-caught-watching-porn

25 https://pdf.ic3.gov/2017_IC3Report.pdf

26 https://newsroom.fb.com/news/2018/04/hard-questions-protecting-peoples-information/

27 https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/

28 https://www.afr.com/business/media-and-marketing/advertising/facebook-working-with-australian-authorities-ahead-of-federal-election-20180901-h14ts1

29 https://newsroom.fb.com/news/2018/09/security-political-campaigns/

30 https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

31 https://www.ic3.gov/media/2018/180802.aspx

32 https://www.zdnet.com/article/new-hakai-iot-botnet-takes-aim-at-d-link-huawei-and-realtek-routers/

33 https://www.zdnet.com/article/first-iot-security-bill-reaches-governors-desk-in-california/

34 https://www.forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies/amp/

35 https://www.cyberscoop.com/cellebrite-iot-data/

36 https://www.ic3.gov/media/2018/180802.aspx

37 www.staysmartonline.gov.au

38 www.nomoreransom.org

39 https://www.telstra.com.au/business-enterprise/solutions/security/security-report-2018

40 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kansas-hospital-hit-by-ransomware-extorted-twice

41 https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/

42 https://www.nomoreransom.org/en/ransomware-qa.html

43 https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/

44 https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

45 https://www.fortinet.com/blog/threat-research/ransomware-as-a-service-rampant-in-the-underground-black-market.html

46 https://www.smh.com.au/politics/federal/increasing-cyber-crime-attacks-costing-up-to-1b-a-year-20180410-p4z8ui.html

47 https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

48 https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe

49 https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

50 https://www.computerweekly.com/news/450426854/NotPetya-attack-cost-up-to-15m-says-UK-ad-agency-WPP

51 https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

52 https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff

53 https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

54 https://cybersecuritystrategy.homeaffairs.gov.au/

55 https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

56 https://www.cyberchallenge.com.au/

57 https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

58 https://www.itnews.com.au/news/australias-filtered-new-cyber-doctrine-just-became-stop-the-bots-499747

59 https://www.itnews.com.au/news/cyber-security-centre-opens-in-new-canberra-facility-500338

60 https://www.cert.gov.au/jcsc

61 https://www.austcyber.com/

62 https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018

63 https://www.iab.org/wp-content/IAB-uploads/2018/09/IAB-Comments-on-Australian-Assistance-and-Access-Bill-2018.pdf

64 https://www.homeaffairs.gov.au/consultations/Documents/explanatory-document.pdf

65 https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers

66 https://www.theinquirer.net/inquirer/news/3061909/japanese-government-weighs-up-5g-ban-on-huawei-and-zte

67 http://www.abc.net.au/news/2018-09-03/china-officially-bans-abc-website/10193158

68 https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

69 https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

70 https://www.cyberscoop.com/lazarus-group-charges-wannacry-ransomware-symantec-fireeye/

71 https://www.justice.gov/file/1080281/download

72 https://www.iso.org/news/ref2309.html

73 https://3l9nb01u2hkq4cz5053evqwi-wpengine.netdna-ssl.com/wp-content/uploads/2017/08/Agari_DMARC_Adoption_Report_Federal_2018.pdf

74 https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa

75 https://cyber.gov.au/

76 https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices

77 https://www.justice.gov/opa/press-release/file/1092091/download

78 https://blog.barkly.com/wannacry-ransomware-statistics-2017

79 https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

80 https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

81 https://www.acma.gov.au/Citizen/Internet/esecurity/Online-identity/netflix-fake-email-scam-welcome-to-smart-phishing

82 https://www.zdnet.com/article/huawei-and-zte-excluded-from-5g-trials-in-india-report

83 https://www.acsc.gov.au

84 http://www.abc.net.au/news/2018-08-23/huawei-banned-from-providing-5g-mobile-technology-australia/10155438

CommonwealthBank