Signals

Quarterly security assessment

Q3 2017

CommonwealthBank

Yuval Illuz
Chief Information Security and Trust Officer, Commonwealth Bank

I'm proud to present to our valued clients and partners our ninth edition of Signals.

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 is an example of our ongoing program of work to raise the bar for cyber security among our clients and the broader digital economy.

In this issue, we outline a range of new threats to feed into your threat models – and also discuss how to feed knowledge of these threats into a model that helps to quantify cyber security risk.

We hope and anticipate our analysis will provide context and confidence for your security strategy.

Contents

Horizon Scan

Upcoming events of interest

2017 Oct 10-12

Sydney

AISA National Conference

The Australian Information Security Association hosts its annual conference for members.

2017 Nov 14 — **Sydney**

2017 Nov 15 — **Sydney**

2017 Dec 1 — **Brisbane**

Malware and Fraud Awareness Workshops

Representatives from Commonwealth Bank and the Australian Federal Police will present a security awareness session for finance executives on the link between malware infection and payment fraud. Email cyber-outreach@cba.com.au if you wish to attend (CBA clients only).

2017 Nov 15-17

Canberra

Honeynet Project Workshop 2017

Learn the art of deception at the Honeynet Project Workshop.

Editorial Panel

Contributors


Brett Winterford
Senior Manager, Cyber Outreach


Fred Thiele
Executive Manager, Cyber Security Portfolio


Tim Peel
Cyber Intelligence Researcher


Jessica Woodall
Manager, Cyber Outreach

Reviewers


Yuval Illuz
Chief Information Security and Trust Officer


Arjun Ramachandran
Executive Manager, Cyber Outreach


Young Jeong
Senior Incident Responder


Kevin Cleary
Cyber Intelligence Researcher

Thanks To

Kai Ta
Cyber Security Services Manager

Boris Dvojakovski
Cybercrime Researcher

Welcome

Brett Winterford
Senior Manager,
Cyber Outreach and Research

The $X million dollar question

A recent ASX and ASIC study found that 40% of ASX100 companies consider cyber security their number one area of risk in 2017, and 80% expect the level of risk to rise over time.[1]

We've seen a deluge of interest from the boards and executives of our clients over the past two years who have asked us to help them understand how we measure and mitigate risks to cyber security.

We usually begin these conversations by framing cyber security as an ecosystem issue that impacts the whole economy, and provide a foundation for them to help understand the threat landscape and how we are choosing to respond. That tends to drive the conversation to one key question: *What risks does my organisation face, and what level of investment is appropriate to manage it?*

I typically warn people to avoid holding up what other organisations are spending on cyber security as a yardstick. Your peers may offer similar services, be of similar size and be subject to the same regulatory constraints, but decades of technology choices – not to mention the maturity or capability you've already developed - necessitate fundamentally different approaches.

In this issue of Signals, we provide a primer to conceptualising and measuring cyber security risk. It's designed to help those of you starting your security journey from scratch. I look forward to sharing more observations with you on this subject in the next issue.

> "What risks does my organisation face, and what level of investment is appropriate?"

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.

Cyber Security:

Trends and Observations

Key trends observed during the quarter

Major cybercrime forums taken down

A globally coordinated law enforcement effort has dismantled two of the world's largest dark web markets, Alphabay[viii] and Hansa[ix]. Criminals used these online, anonymous bazaars to advertise and sell illegal goods and services such as drugs and weapons alongside user credentials and credit cards stolen in cybercrime campaigns. While the "takedowns" resulted in arrests of site administrators and some vendors, buyers and sellers appear to have migrated their business to alternative markets, where in many cases, they already had a strong reputation.

CHECKLIST

- Disrupting dark web activity requires meticulous, time-consuming and expensive law enforcement investigations. We assert with high confidence that irrespective of the resounding success of this operation, there will continue to be sufficient incentive for other markets to take their place – as occurred after the widely heralded Silk Road takedown in 2013.
- Dark web markets are a good source of intelligence for cyber security teams to monitor where the wares stolen in credential phishing campaigns or other hacking campaigns are traded.
- It is probable that some cybercriminal groups will revert to forums with higher barrier to entry. While this slows the pace of campaigns in the short-term, it creates fresh challenges for law enforcement and intelligence analysts when attempting to monitor illegal activity.

Cybercriminals use renewal notice themes for bait

The CBA Cyber Security Centre has observed an increasing number of phishing campaigns that warn users that a service they (might) subscribe to requires renewal or some other form of action to avoid being deactivated. This technique – which relies on appealing to the user's sense of urgency – is used in a wide range of phishing lures. Over the last few quarters, we have seen lures that threaten revocation of everything from drivers' licenses to popular cloud services, bank accounts and subscription television services.

CHECKLIST

- Teach your staff the various 'triggers' used by cybercriminals to tempt a user to open an attachment or click on a hyperlink.
- Phishing campaigns often rely on an urgent call-to-action. Consider working with your marketing teams to help them avoid sending communications to your customers that appeal to the same triggers, to ensure customers can discern between legitimate and illegitimate communications.

Poor configuration makes for leaky clouds

Pushing workloads into public clouds has provided development teams with far greater agility. From a security perspective, public clouds also allow for non-security professionals to tap into security features they might not have otherwise used. But conversely, public cloud dramatically increases an organisation's attack surface, leaving less room for error. Security researchers and malicious actors routinely find vulnerable assets using simple scans that target configuration errors. In the last quarter alone, a large number of organisations were found to have failed to secure storage volumes (S3 buckets) hosted in Amazon Web Services, including Dow Jones[xii], Groupize[xiii], Time Warner[xiv], Verizon[xv], Viacom[xvi] and an organisation that leaked the details of 9,000 US military veterans[xvii].

CHECKLIST

- While using public cloud frees developers and third party application service providers from infrastructure constraints, this mode of deployment often bypasses mature internal IT controls that ordinarily would check for configuration errors. Security teams should work with these teams to develop repeatable architecture patterns for deploying systems to the cloud securely. AWS offers reference material for producing architecture patterns[xviii].
- Educate developers and partners on the distinction between configuration settings that allow authenticated users of your service to access a data store, versus those that allow all authenticated users of Amazon Web Services (over a million users) to access it. AWS infrastructure can be readily monitored and free tools are available to check services are configured correctly[xix].
- Consider broadening the scope of your assurance practices. Many organisations now complement tightly-scoped penetration testing with objective-based testing by "red teams", who are empowered to proactively search for data left unsecured online, including by third parties. Australian Daniel Grzelak has developed free tools[xx] for taking a red team approach to services hosted on AWS.

By the Numbers

96%
of China's 750m internet users connect on smartphones.[ii]

US$300 million:
Estimated losses for Maersk (shipping) from [Not]Petya infection.[iii]

US$300 million:
Estimated losses for TNT Express from [Not] Petya infection

21,000
customer records were stolen from UK telco TalkTalk via its outsourcer, Wipro.

£100,000
fine was levied on TalkTalk by UK regulators.[iv]

Cyber Security:
Trends and Observations

Software supply chains targeted for mass compromise

Aggressive, well-resourced cyber-attacks continue to target private organisations in contested territories, raising further concern that some nation-state aligned actors view industry as a legitimate target during periods of increased geopolitical instability. The [Not] Petya network worm was initially propagated[xxi] by the compromise of a server[xxii] that distributes software updates to customers of Ukrainian accounting software vendor M.E.Docs. The compromised update resulted in immediate disruption to over 2000 Ukrainian firms and multinationals that do business in the region and ultimately led to billions of dollars' worth of damage to the global economy. In August 2017, a similar backdoor was detected in a software update distributed by NetSarang, a South Korean provider of remote administration software used[xxiii] at large firms around the globe.[xxiv]

CHECKLIST

- Establish a governance program to identify and manage risks posed by your software supply chain. Commonwealth Bank's Cyber Outreach team is hosting further workshops on this topic in early 2018 – talk to your relationship manager to participate.
- Where practical, evaluate the impact of software updates on test systems, prior to a broader rollout across production systems.
- The US National Institute of Standards and Technology has updated its overarching framework[xxv] to include more advice on managing third party cyber security risk.
- Strive to work with well-resourced suppliers that have demonstrated an ability to respond to cyber security incidents.

Breaches stem from flaws in web frameworks

Most modern web and mobile applications inherit their key features from web application frameworks and the software libraries and protocols they include. They are the scaffolding that enables rapid development and deployment of apps – they are typically freely available, broadly deployed and maintained by a community of users and enthusiasts. They are also a juicy target for attackers looking to achieve scale. Security vulnerabilities found in the Apache Struts framework and numerous JavaScript frameworks[xxvi] have demonstrated broad-scale impacts on hundreds of organisations at a time. As a case in point, attackers stole 143 million sensitive customer records from US credit monitor Equifax after it failed to patch a vulnerability in Apache Struts in a timely manner[xxvii]. The breach forced the early retirement of the company's CIO, CSO and CEO.[xxviii]

CHECKLIST

- Monitor closely for disclosure of vulnerabilities in the web application frameworks used by your organisation. Patch or update expediently.
- Your application security program should ideally be testing and endorsing software libraries, protocols and other components of web application frameworks to provide developers greater confidence over which versions to use.
- Smaller firms might assess a web application framework on how quickly and effectively the community has historically responded to vulnerability disclosures with patches.

Expired domains and browser plug-ins hijacked to host malware

Attackers continue to find creative places to host malware that circumvent detective security controls. In recent months, security researchers have discovered malware hosted on legitimate domains that organisations have neglected to renew, or have observed attackers hijacking abandoned or unsupported web browser extensions, CMS plugins and themes. More audacious attackers have compromised the developers of popular browser extensions in campaigns that impact millions of users, albeit for a shorter time. These domains and extensions are more likely to be trusted (and less likely to be blacklisted) by automated security tools, providing attackers a ready-made number of victims to infect and longer window of time to do so.

CHECKLIST

- Organisations with low thresholds for risk must decide whether certain types of sites or applications are adequately resourced from a security perspective to remain resilient. Some organisations, for example, choose to block sites built using the WordPress CMS by default - owing to a litany of unsupported plug-ins used in these sites – and only whitelist them on request. Check your logs: what impact would such a decision have on legitimate access of sites using these technologies?
- Equally, software development teams must think carefully about how to manage third party resources that load onto their web sites. What risks might your organisation face if these third party services were compromised? Do the providers of these resources have adequate security capability, or are they at least popular enough that developers have incentive to continue to support and update them?

By the Numbers

$417 million: online (card not present) credit card fraud in Australia (2016).[v]

83% of spam is sent during working hours.[vi]

US$7 – price-tag on a new family of credential stealing malware.[vii]

71 new ransomware families were released in the first half of 2017.[viii]

Locky was the most common family targeting Australians in September 2017.

Deep Dive:

Secure your cloud email

Social engineering – coupled with access to your inbox – presents attackers with many paths to profit.

Brett Winterford
Senior Manager, Cyber Outreach and Research

To a profit-motivated cybercriminal, access to your email inbox can be as valuable as your bank account. That sounds counterintuitive – until you compare the difficulties an attacker faces in trying to personally extract money directly from your bank account, versus convincing you or the people that you interact with to make a payment for them.

Over the last nine months, there has been a steady rise in the number of Australian businesses that have made payments to attackers after a compromise of their email account, or that of an entity they do business with.

Access to a victim's inbox isn't the only way an attacker can trick victims into make payments, as discussed in previous guidance on 'whaling'[xxxi] and other forms of Email Payment Fraud[xxxii]. Organisations continue to be duped into making payments in response to emails that impersonate a party to the transaction, either via spoofing of a legitimate domain, or registration of similar domains and webmail addresses. Education has slowed the growth of these campaigns, but they still responsible for a large volume of fraud.

As organisations move their email into cloud-hosted systems for the first time, many neglect to configure appropriate security controls. Cybercriminals have seized on this new opportunity - and the range and sophistication of scams that involve unauthorised access to email accounts has risen dramatically.

Leading indicators

One in four fraud losses tracked by CBA's cybercrime team over the past six months involved the compromise of a cloud-based email account.

The majority were Microsoft Office 365 cloud accounts, or consumer-grade Microsoft email accounts (Hotmail etc.) used by tradesmen and other small businesses. This reflects Microsoft's dominance in the enterprise market. Well over 100 million active users of Office 365 log in each month, and most of these users work for businesses in the developed world. A further 30 million log-in to Microsoft's consumer-grade email services each month – and a subset of these are small businesses that haven't migrated to Office 365. Microsoft's main competitor in cloud-based productivity, Google's G-Suite, has struggled to attract 10% of the business market.

Microsoft is subsequently an ideal brand for attackers to imitate. Over the last four weeks, no single brand was impersonated more often in credential phishing campaigns (fake web sites

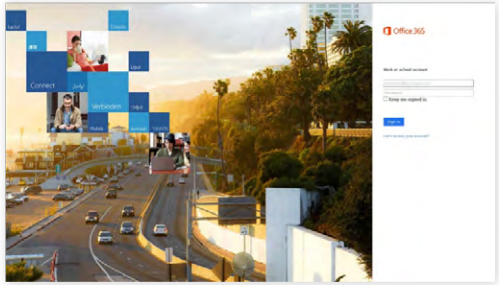


Image 1: Generic Microsoft Office365 phishing page

set up to steal user credentials) than Microsoft. On some of the abuse reporting channels we monitor, twice as many Office365 and Outlook Web Access phishing pages were stood up than those imitating Apple services (iCloud, iTunes etc.), and five times as many as phishing sites that mimic Google services.

Microsoft has reported a 300 percent increase in attacks on user accounts in the first quarter of 2017 compared to the corresponding quarter in 2016, while the number of account sign-ins attempted from malicious IP addresses increased by 44 percent over the same period.

The scam(s)

There are two primary ways for profit-motivated attackers to access cloud email accounts.

The first is "credential stuffing", in which the attacker attempts to use credentials (usernames and passwords) stolen in attacks on other online service providers, under the expectation that people often re-use passwords for multiple services.

The second is by acquiring credentials stolen in phishing campaigns. Perpetrators of phishing campaigns create web sites that mimic the branding of legitimate log-in pages (see Image 1), and send spam runs that try to convince legitimate users of those services to enter their credentials. Credentials harvested in phishing runs are often sold to other criminals whose

By the Numbers

Top 3 events that lead to fraud losses:

1. 'Spoofing' an email address to request payment
2. Unauthorised access to an email inbox
3. Unauthorised access to accounting software or bank account

One in four

losses involved the compromise of a cloud-based email account.

10:9

Scammers continue to imitate suppliers or other payment beneficiaries slightly more often than CFOs and Directors.

Deep Dive:
Secure your cloud email

> “Numerous phishing web sites are **set up to imitate Microsoft services – as well as banks and other popular online service providers** – on a daily basis”

intent is to commit fraud. Numerous phishing web sites are set up to imitate Microsoft services – as well as banks and other popular online service providers – on a daily basis. They are typically blacklisted or forced offline within hours, but not before a number of users have given away their credentials.

The criminals that run Business Email Compromise scams typically use these stolen credentials to log in and search an inbox for evidence of invoices, purchase orders or other documents and messages that relate to processing of large value payments.

Who is attacking us?

Research by SecureWorks and Trend Micro note that Business Email Compromise – in which attackers hack an email system as a precursor to tampering with payments – is a mature industry in West African countries like Nigeria, where employment prospects are otherwise slim. These criminal networks consist largely of graduates from simple social engineering scams. These actors have grown more patient, and are prepared to invest in malware (such as remote access trojans) or in buying access to stolen user credentials from phishing campaigns. While perpetrators are by no means limited to West Africa – indicators from many of the attacks we've seen (even those that originate in Asia) are very similar to practices West African cybercriminal groups are renowned for.

What payments are at risk?

Any payment arranged over email:

- Invoices between suppliers, especially among tradesman, engineering and construction firms, manufacturing and distribution.
- Payments to staff (payroll).
- Beneficiaries of property sales (trust accounts) or payment of rent.
- Beneficiaries from the sale of expensive items (vehicles etc.)
- Beneficiaries from settlement of a will.
- Beneficiaries from tax refunds.

The attacker's aim is (usually) to be the 'man in the middle' between buyers and sellers who establish the details of a transaction over email. Attackers will intercept and edit existing invoices to replace the bank account details listed for payment, or email customers from a compromised account advising of new account details for future payments. If the account they hack into belongs to a person with purchasing authority, they might simply demand a subordinate make a payment on their behalf.

The attackers have proven to be very patient. They refer to these scams as the “long con” – and will monitor an inbox for some time while waiting for a large payout opportunity. Often the attackers set up mail forwarding rules to automatically send messages to the webmail accounts they log into more regularly.

Strategies for protecting your cloud email

The most critical defence against business email compromise is multi-factor authentication (MFA).

Multi-factor authentication challenges users to authenticate (prove their identity) in more than one channel before they can access a system. They usually must combine *something they know* (a username and secret password on a web interface, for example) via one channel, and confirm with *something they have* (such as a random set of characters sent to their mobile device, for example) in another.

Microsoft and Google both offer multi-factor authentication 'out-of-the-box' for business customers. Provisioning to users is straightforward, as is choosing what second factor is most appropriate and when users should be presented with a multi-factor challenge.

Instructions for setting up multi-factor authentication

- For Microsoft Office 365 administrators[xxxiv]
- For Google G-Suite administrators[xxxv]

The typical argument against MFA is that it inconveniences users. Both of the major cloud email service providers offer ways to reduce this friction. Google G-Suite users can check a box to “remember verification for the computer”, which sets up an authentication cookie between the user's browser and their G-Suite account. The cookie expires (and an MFA challenge is presented to the user) every 30 days. Office 365 users can set up passwords for bypassing the second-factor on mobile devices, for example, but keep it in place for log-in over the web.

A range of other suggested security controls are outlined on the following page.

Deep Dive:
Secure your cloud email

> “Multi-factor authentication **limits attackers from accessing a service** using only a stolen username and password”

More information

- Microsoft’s security best practice for O365
- Google’s security best practices for G-Suite
- Microsoft’s guide to detection of an attack
- Microsoft’s guide to triage of a compromised O365 account
- Google’s guide to detection and triage of a compromise G-Suite account

Strategies for protecting your cloud email

1: Theft of Credentials

METHOD OF ATTACK	ESSENTIAL DEFENCE	ADVANCED DEFENCE
Attackers acquire user credentials stolen in phishing campaigns. ‘Credential stuffing’ – attacker tries usernames and passwords stolen in other data breaches to log in to your email account.	**1.** Multi-factor authentication limits attackers from accessing a service using only a stolen username and password. **2.** Password Wallets/Managers help users create unique and complex passwords for every service they use. **3.** Enforce password policies that lock a user out for a period of time after a number of failed attempts.	Consider deploying physical security tokens for multi-factor authentication on high-risk workstations.
Attackers infect a user’s device with malware to steal credentials.	**1.** Set web browsers to automatically update and keep operating systems patched. **2.** Ensure users operate as the least privileged user (not admin/root). **3.** Filter web traffic (via internet security software/antivirus.) **4.** Implement security awareness programs.	Talk to your relationship manager about whether NetLock is appropriate for your business.

2: Unauthorised access to email account

METHOD OF ATTACK	ESSENTIAL DEFENCE	ADVANCED DEFENCE
Attacker is able to log-in using stolen credentials on an account that is not protected by multi-factor authentication.	Use the ‘Conditional Access’ rules offered by Microsoft Office365 and Google G-Suite. While their approaches vary, these rules allow an administrator to set conditions of access according to whether the user is inside or outside the enterprise network, whether they are on managed or unmanaged devices or according to a set of whitelisted IPs addresses, for example. For any combination of these scenarios, rules can be set to accept, deny or force a multi-factor challenge for access to the inbox.	Microsoft offers additional rules-based and machine learning algorithms to detect and block anomalous log-in behaviour as a premium (paid) service. Google uses a range of machine learning-based detection into its standard G-Suite offering.
Attacker is able to log-in using stolen credentials of an administrator’s account that is not protected by multi-factor authentication.		Limit the number of accounts that require ‘global’ or ‘super user’ administrative access. Microsoft offers a premium (paid) privileged access management solution.

3: Reconnaissance of the inbox

METHOD OF ATTACK	ESSENTIAL DEFENCE	ADVANCED DEFENCE
Attacker sets mail forwarding rules to send mail to their own account.	Consider conditional formatting mechanisms that distinguish (through colours or alerts) when email is being sent to or received from internal versus external domains. If users report any strange behaviour in their inbox, check if any mail forwarding rules have been applied. While these can usually be seen in the user interface of Office 365, administrators should also check under the hood using PowerShell commands.	Microsoft offers additional rules-based and machine learning algorithms to detect and block anomalous mail forwarding behaviour as a premium (paid) service.

4: Fraudulent request for payment

METHOD OF ATTACK	ESSENTIAL DEFENCE	ADVANCED DEFENCE
Whaling attack (attacker impersonates staff with purchasing authority and requests a payment) Attacker impersonates a supplier (or other party to a transaction) and requests a change of beneficiary details or submits a new invoice.	Ensure your payments authorisation process “assumes compromise”: **1.** Make use of multiple authorisers for payments and enforce strict separation of duties for payments. **2.** Require large payments or change of beneficiary details to be verified via additional checks in multiple channels. No payment should be authorised on the basis of emails from a single account. **3.** Education your treasury and accounts teams in how to recognise Email Payment Fraud.	

5: Fraudulent payment is made

- Contact the CommBiz helpdesk and your relationship manager immediately.
- Report the matter to the Police.
- Use the following guides to triage of compromised accounts provided by Google[xxxvi] and Microsoft[xxxvii].

Deep Dive:

A beginner's guide to quantifying cyber risk

Establishing the foundations of a cyber security program

Fred Thiele
Executive Manager,
Cyber Portfolio, Commonwealth Bank

Historical records of disruptive events like floods or power outages provide the insurance industry the data required to model the likelihood and impact of future events within such a degree of accuracy, they can base a business on it.

Threats to cyber security, by contrast, are relatively new phenomena. In our two decades connected to the internet, the threat landscape has been anything but predictable. As the volume of vulnerabilities in the technologies we use amass, the capability of threat actors evolves and the number of high profile security incidents ensues, uncertainty abounds. The under-resourced CISO measures risk to cyber security with a wet finger in the air.

As boards of Australian organisations grow more engaged on cyber security, CISOs should anticipate demands for a more rigorous approach to quantifying risk.

While there is insufficient public data available to accurately predict low probability, high impact events, there are numerous frameworks, models and thought exercises that can help an organisation approximate cyber risk, and over time, refine it into something resembling a science.

Directors, CEOs and CFOs can play an important role in the process.

Key concepts

Before we begin, it's best to agree on some high level concepts. **Risk** is a measure of potential loss if an event were to occur. 'Cyber risks' are a subset of organisational risks that are caused by a cyber security threat. A cyber security **threat** is an event with the potential to cause harm to an organisation's information assets by circumventing confidentiality (via unauthorised access and/or disclosure), integrity (via modification of data) or availability (via destruction or denial-of-service).

In cyber security, we usually talk of **vulnerability** to describe specific weaknesses in systems. But when quantifying risk, we are referring more generally to an organisation's 'susceptibility to a threat'.

Security **controls** are countermeasures to a threat that attempt to prevent, detect or recover from a cyber security event. When we **remediate** an identified risk, we're reducing its impact to near zero, while when we **mitigate** a risk we're accepting that there will be a residual risk and that the best we can do is to monitor and respond to events to minimise their impact.

How do we get started?

First, you need to understand the threat. Why would various actors – whether malicious or otherwise, inside or outside your network – seek to gain unauthorised access to your data or disrupt your systems? You'll need to get a measure of the threat landscape to understand what threats have targeted or are likely to target your organisation. *Signals* is a good place to start!

Next, the board and executive need to define and endorse an acceptable level of risk. Most organisations use a risk matrix, with likelihood of an event on one axis (expressed as probability or %), and impact on the other (expressed on a scale of inconsequential or negligible up to severe or critical).

Determining an acceptable level of risk is often best arrived at by talking about what's unacceptable. *For how long would the organisation accept an inability to serve customers online? How much money would the organisation be prepared to lose each year to fraud events?* Think about risks to customers, to staff, to brand or reputation. Answering these questions helps to define your 'risk appetite statement' – an expression of where in that matrix would you feel comfortable to sit, knowing that not all risks can be remediated.

A generic risk matrix

LIKELIHOOD	1	2	3	4	5
5	L	M	M	H	S
4	L	L	M	H	S
3	N	L	M	H	S
2	N	L	M	H	S
1	N	N	L	M	H

IMPACT

Negligible Low Medium High Severe

Once you quantify your risks, you'll be able to visualise where you are now and where you need to get to.

An invaluable pre-requisite to the exercise is a living register of the organisation's IT and data assets. This might be a hard ask in large and complex organisations, but it's important to at least get a handle on what the 'crown jewels' are. Organisations that do this the best tend to have benefited from strong executive support to get everyone on board with how critical this register is.

Deep Dive:

A beginner's guide to quantifying cyber risk

> "Cyber security professionals can rattle off an inexhaustible number of ways an organisation can be attacked, but **risk analysis requires structure**"

With these in hand, the security team have what they need to start threat modelling.

Modelling cyber risk

There are numerous theories on how best to quantify cyber security risk. Most follow a similar process and are distinguished by the level of mathematical detail required to reach conclusions. (The authors of the most scientifically rigorous model - Factor Analysis of Information Risk (FAIR)[xxxviii], for example, claim the standard for risk metrics originally established by NIST is too loosely defined. But they'd also concede that their work inherits its foundations from it.)

Just about every model attempts to calculate the inherent risk (a measure of risk before compensating controls) for a range of threat scenarios, using something like the following model: **Cyber risk = threat (#) x vulnerability (%) x impact ($).**

As the table below demonstrates, for any given threat scenario, you need to assess (or predict) how often you should expect to encounter the threat scenario over a given period of time, what percentage of your systems would be vulnerable if the threat were to play out, and an expected loss your organisation would face if the threat were to play out.

Cyber risk per threat scenario

	Threat	Vulnerability	Impact
Expressed as	**A number**	**A percentage**	**A cost**
Question:	How often have you or do you expect to encounter this threat scenario over a given period of time?	What percentage of your systems or data would be vulnerable to the threat scenario?	What would be the expected loss your organisation would face if this threat scenario were to play out?
Example:	*The organisation has detected x malware campaigns each year that combine that spread via SMBv1 and deliver a ransomware payload.*	*What percentage of systems are not yet patched against known vulnerabilities in SMBv1?*	*What is the estimated cost of an infection, taking into account the ability of the network worm to spread through vulnerable systems, the cost of rebuilding systems and potentially the costs of managing reputational damage or shareholder value if the infection were to be known to the public?*

Data quality

Cyber security professionals can rattle off an inexhaustible number of ways an organisation can be attacked, but risk analysis requires some structure. You can group cyber risks by asset, for example, or by whether the threat scenario would impact the confidentiality, integrity or availability of data. You might also classify by actor group (insider, third party partner, external party). Every risk framework tends to include its own taxonomy to follow, and all aim to consider a broad coverage of threats.

As you think through threat scenarios, you'll undoubtedly stumble onto those for which you don't have the required data to measure. This can be problematic if you are yet to implement an incident response or vulnerability management capability – both of which provide strong metrics to compare with.

So to some degree, the initial assessment in an organisation thinking about cyber security for the first time might need to include desktop research. MITRE's CVE database provides a global view of vulnerability data, the Californian State register of data breaches is the longest running register of breach events, and Verizon's annual data breach investigations report also has a long history. (NB: always seek to validate data provided by parties that have skin in the game - such as vendors of security software – by correlating with independent, trusted sources.)

The more meticulous you are, the better. But you will have to accept, at some point, that until you stand up some semblance of security capability, your numbers are going to include approximations. Even the authors of the FAIR model, who believe that everything can be measured, concede that the main aim of the exercise is to "reduce management's uncertainty about risk" rather than calculate it with absolute accuracy.

There are other reasons this game of mental gymnastics is valuable. Your initial aim might be to quantify your total exposure to cyber risk. But it's an important baseline for other reasons. In an environment with an unknowable number of emerging threats, quantifying cyber risk can also provide a way of prioritising investment in cyber security programs - a subject that demands its own deep dive.

Tracking your progress

The exercise we've described should spare directors and business leaders from the gory detail of every security threat to the

Deep Dive:

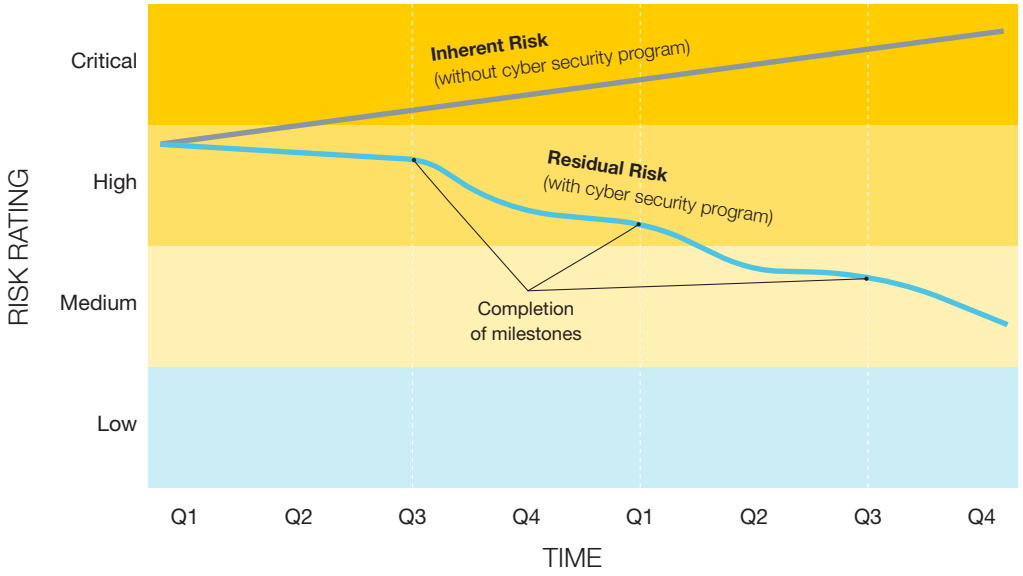
A beginner's guide to quantifying cyber risk

organisation, but nonetheless deliver a reasonably consistent, "10,000 foot view" of aggregate risk. It may be beneficial to illustrate what you've measured – preferably in a way that pinpoints where you've started, what your total inherent risk would have looked like without your security programs in place, and a decline in your residual risk as new controls or programs are delivered. This is something you should return to repeatedly, adjusting for changes in scope or shifts in the threat landscape.

You should also assume that the quality of data you're feeding into your model will improve as you mature your security capability. We'll dive deeper into this in a future edition of Signals.

Brett Winterford contributed to this report.

Buying down risk



Regulatory & Legal

New laws and legal precedents relevant to security strategy

> "A public response to a data breach that **prioritises legal considerations above responsibility** to affected customers tends to result in poor reputational and regulatory outcomes."

China, Russia ban anonymity services (VPN, TOR)

Legislation seeking to ban Virtual Private Networks (VPNs) successfully passed through both houses of the Russian Federal Assembly in July 2017. The Bill achieved unanimous support following a secret briefing held for the parliamentary members by the head of the FSB intelligence agency, Alexander Bortnikov, and was signed into law by President Vladimir Putin just a week later. The new law prohibits the use of VPNs and anonymizing services such as TOR that circumvent controls instituted by the government to block 'restricted' websites. Similar laws were introduced in January 2017 by the Chinese Government, which now requires its mobile telcos to block VPN apps on their networks. Web-based VPN services operating in China must agree to not circumvent the government's 'block list' or face a similar fate.

CHECKLIST

- Executives that use VPN services to protect their communications when travelling to China or Russia should consult with their security teams, as should businesses that currently use VPN services in these countries.
- The Australian Signals Directorate maintains a useful set of general advice for travelling overseas with electronic devices[xxx].

U.S. Government blocks Kaspersky

The Trump administration has banned the use of Kaspersky antivirus products in all US Federal Government departments and agencies, and has given agencies 30 days to remove the software. The Department of Homeland Security (DHS) released an advisory stating: "the risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalise on access provided by Kaspersky products to compromise federal information and information systems directly implicates US national security." The move follows a Senate hearing in May where US intelligence chiefs voiced concerns over use of the company's products. Headquartered in Moscow and founded by former Russian military intelligence officer Eugene Kaspersky, accusations of state collusion are not new to the company; but to date they were confined to media commentary. Kaspersky, in response, have offered to share their source code with the US Government.

CHECKLIST

- Organisations should consider the level of privilege granted to applications in their environments during threat modelling, including security software. A recent compromise of the popular CCleaner antivirus software[xxxi] - which affected at least 700,000 users - is a good illustration of how these risks might be realised.
- As DHS has not (to date) produced evidence to justify their advisory, US and Western vendors may face reciprocal bans on 'national security' grounds by Russian or third-party nations.

Legalistic responses to data breaches fall flat

One of the world's largest credit reporting companies, Equifax, has withdrawn an attempt to reduce its liability to lawsuits after it fell victim to a large data breach. After disclosing that the personal data of 143 million Americans - including social security numbers, birth dates and home addresses – had been compromised – the company offered free credit monitoring to affected users. Victims signing up for this monitoring were asked to agree to terms and conditions under which they waived their legal rights to take action against Equifax over the breach. This clause was later swatted down by US lawmakers, and withdrawn by Equifax – following widespread uproar. Class action lawsuits have ensued.

CHECKLIST

- A public response to a data breach that prioritises legal considerations above responsibility to customers and affected stakeholders tends to result in poor reputational and regulatory outcomes. In response to a data breach in 2015, TalkTalk initially played down its severity, then publically claimed it had no legal obligation to encrypt its customer's data. This resulted in damning media coverage and a £100,000 fine from regulators.
- Organisations that offer online services to US residents should reconsider whether a social security number should constitute a 'secret' for the purpose of authenticating a user. It wasn't appropriate before the Equifax breach, and most certainly isn't now.
- The UK Government's National Cyber Security Centre (NCSC) has highlighted the secondary risk posed by scammers who might abuse the details stolen in the Equifax breach to craft convincing phishing emails.

Better Practice:

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

> “How an organisation deals with vulnerability disclosures is **an important signal to the public** about security maturity.”

Prepare for ransomware

A team at NIST and MITRE have collectively drawn up a comprehensive guide to recovering from ransomware and other destructive malware attacks[xlii]. The top-level advice: segregate your network and remove unnecessary administrative access to systems to prevent an infection spreading, monitor log data (and consider file integrity monitoring) for improved detection and triage, and practice backup and recovery.

The end of Flash

Vulnerabilities discovered in Adobe’s Flash media player - once a de facto standard for multimedia on the web – have been exploited by numerous APT and cybercrime campaigns. Multiple operating systems – starting with Apple’s iOS in 2010, and more recently web browsers, have subsequently stopped supporting Flash content. Adobe has finally conceded that Flash has no future and announced that it will no longer be supported by Adobe by the end of 2020[xliii]. It is highly probable that most use of Flash will be phased out much sooner.

Find the bugs first…

One of the most critical components of a cyber security capability is establishing an assurance program where applications and/or infrastructure are tested by professional “white hat” hackers. The UK National Cyber Security Centre now provides high-level advice on how your organisation can build the foundations of an assurance function – a penetration testing team.[xliv]

… Before somebody else does

Even organisations with strong assurance practices can be surprised by vulnerabilities discovered in their internet-facing systems by external researchers. The way in which an organisation deals with these reports is an important signal to the public about your security maturity. One of the world’s best authorities on ‘coordinated vulnerability disclosure’ is the Computer Emergency Response Team (CERT) at Carnegie Mellon University, who have published a very comprehensive guide[xlv] for both security researchers and defensive teams.

Know your adversary

Imagine if there was one wiki where all the known TTPs (tactics, techniques and procedures) could be summarised to make your threat modelling that little bit easier. BAM! The good people at MITRE have published one. It’s called ATT&CK[xlvi] and it looks to be a well-thought out product.

It’s not too late to be infected with [Not]Petya

The news headlines may have slowed, but we’re still seeing indicators consistent with the [Not]Petya network worm light up every so often. It’s not too late to read US CERT’s revised advice[xlvii] on how to prevent and remediate these infections.

Shape a NICEr security team

What are the typical roles and responsibilities of a cyber security team? Cyber security operations and US tertiary education providers have for the last three years used the NICE cybersecurity workforce framework published by NIST to answer this question. In August 2017, NIST updated the framework[xlviii] to reflect shifts in workforce demand.

Phish Eyes

Recent phishing lures for your security awareness teams. Report hoax emails to hoax@cba.com.au

A large number of phishing campaigns over the last quarter impersonated billing notifications from energy providers, telecommunications companies and other providers of utility services. Very few of the major brands in Australia escaped unscathed.

Origin Energy

Origin Energy was impersonated in multiple malware campaigns between May and late August. Typically the email arrived with variations on the subject line "Your Origin electricity bill". Most arrived in email inboxes from suspicious sounding domains that would illicit skepticism from anyone with basic security awareness training. (We did, however, see one crafty campaign from a more creative domain - noreply[at]originofenergy.net.)

These emails lure victims into clicking on a link called 'View Bill', which prompts the user to download a .zip archive. Once downloaded, it drops a JavaScript file onto the user machine that downloads the Gozi/Ursnif Trojan, a nasty piece of malware often used to steal online banking credentials.

For well over a year, these phishing sites have been hosted using compromised Microsoft OneDrive accounts (the domains typically end in <accountname>-my.sharepoint.com).

The folks at Origin Energy have published advice to help customers differentiate between real communications and those that impersonate them.

Energy Australia

In June and September 2017, attackers borrowed from the same playbook, developing campaigns that abused the brand of Energy Australia.

Typical subject lines included: "View your EnergyAustralia Electricity Bill" or "Your Energy Australia Gas Bill".

These campaigns also took advantage of compromised Microsoft OneDrive accounts, also attempted to convince victims to download .zip archives, and also dropped JavaScript files that download the Gozi/Ursnif Trojan onto the victim's machine.

Energy Australia provides online security advice on its website.

AGL

These tactics are not new to energy company AGL. The AGL brand was abused in a long series of malware campaigns for most of the latter half of 2016, and in a smattering of campaigns in 2017.

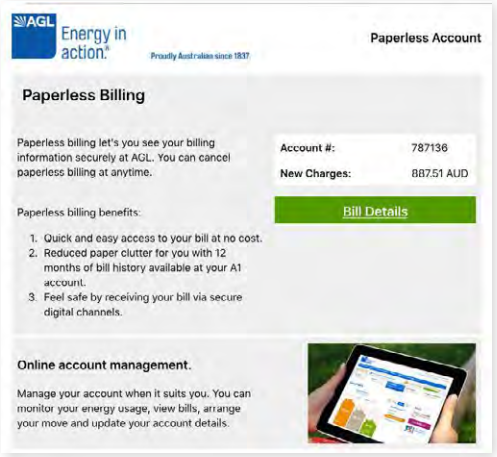
These campaigns typically arrived with the

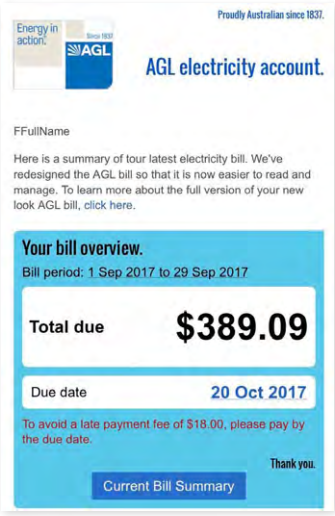
subject line "Paperless Bill", "My Monthly Bill" or "Bill Copy". In earlier campaigns, victims were prompted to click a button called "Manage Your Bill", which directed users to legitimate sounding web sites and asked the user to download a.zip archive that (again) dropped a JavaScript file onto the victim's machine.

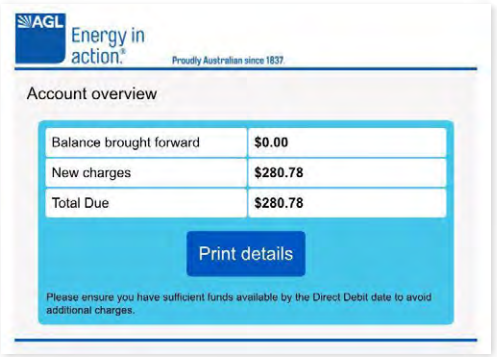
Most of the AGL-themed campaigns infected victims with ransomware – a form of malicious software that encrypts the user's data and offers a decryption key only if the user pays a large ransom via cryptocurrency. The web address generated from each email was personalised using the victim's email address. A smaller number of campaigns in 2017 dropped various other forms of malware – but nothing like the scale of the earlier ransomware campaigns.

Even as these campaigns petered out in early 2017, they resulted in a sustained impact on customer trust. AGL customers are now far more likely to mistake legitimate marketing campaigns for scams – we saw a number of false positive reports submitted to scam-watch sites, including the CBA Hoax Mailbox in May 2017.

AGL provides advice on hoax emails on its website.







Phish Eyes

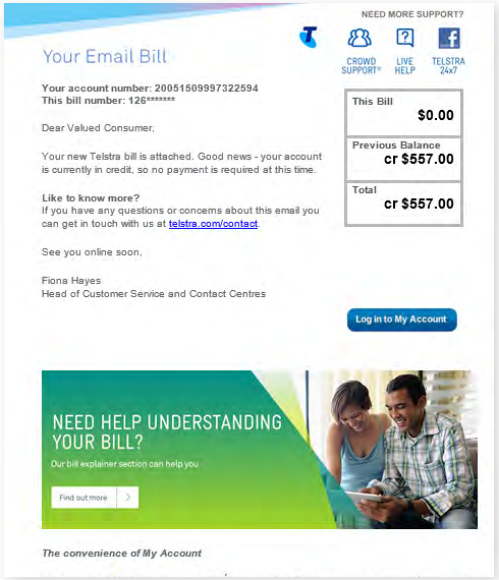
Telstra

Australia's largest telecommunications company was also impersonated in numerous campaigns over the last quarter – each using different infrastructure and dropping different forms of malware.

In one July campaign, victims were sent emails with subject lines such as "Your Telstra Bill", and were presented with a fake Telstra Bill. Upon clicking for more details they were asked to download an executable file or .zip archive with a legitimate sounding name (usually a date range, such as May-June2017.zip), which on execution downloads the TrickBot credential stealing Trojan. This campaign appears to have spoofed a legitimate Telstra domain - notifications@in.telstra.com.au

In the same month we detected campaigns that used identical techniques to the Origin Energy and EnergyAustralia campaigns mentioned above. They arrived with the subject line: 'Telstra Bill – Arrival Notification', directed victims to malware hosted on a compromised Microsoft OneDrive account (<accountname>-my.sharepoint.com) and dropped the Gozi/Ursnif variant of malware.

Telstra provides advice on email scams on its website.



A screenshot of the most recent iteration of Telstra Bill themes, from September 2017. Telcos and other utilities advise customers that they will only send out bills via email that are attached as .pdf files.The malware in this case was contained in an attached word document.

Don't fall for it

- Avoid downloading .zip or .doc files from emails that purport to be your service provider.
- Take note of the email address you usually receive bills from. If bills or requests for payment arrive from a new email address or domain, use your search engine or the community forums provided by your utility to check its authenticity.
- Some service providers will notify you of new bills when you are logged in to their service. If you are unsure about a bill sent over email, don't click on anything. Instead, log-in to your account with the service provider to check if a new request for payment had been scheduled.

Footnotes

i: http://www.asx.com.au/documents/investor-relations/ASX-100-Cyber-Health-Check-Report.pdf
ii: https://www.chinainternetwatch.com/whitepaper/china-internet-statistics/
iii: http://investor.maersk.com/releasedetail.cfm?ReleaseID=1037421
iv: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/08/personal-data-belonging-to-up-to-21-000-talktalk-customers-could-have-been-used-for-scams-and-fraud/
v: http://www.apca.com.au/docs/default-source/2017-media-releases/media_release_payments_fraud_03082017.pdf
vi: https://securityintelligence.com/all-in-a-spammers-workweek-where-do-the-busiest-spammers-work-around-the-clock/
vii: https://www.proofpoint.com/us/threat-insight/post/meet-ovidiy-stealer-bringing-credential-theft-masses
viii: https://blogs.technet.microsoft.com/mmpc/2017/09/06/ransomware-1h-2017-review-global-outbreaks-reinforce-the-value-of-security-hygiene/
ix: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down
x: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation
xi: http://www.bbc.com/news/technology-40788266
xii: http://www.ox.ac.uk/news/2017-08-08-cybercrime-latest-research-suggests-cybercriminals-are-not-%E2%80%98anonymous%E2%80%99-we-think
xiii: https://www.upguard.com/breaches/cloud-leak-dow-jones
xiv: https://mackeepersecurity.com/post/online-hotel-booking-service-allegedly-exposed-sensitive-data
xv: https://www.scmagazine.com/data-breach-exposes-about-4-million-time-warner-cable-customer-records/article/686592/
xvi: https://www.upguard.com/breaches/verizon-cloud-leak
xvii: https://www.upguard.com/breaches/cloud-leak-viacom
xviii: http://www.tigerswan.com/newsroom/statement-information-breach-talentpen-llcs-cloud-file-hosted-amazon-web-services/
xix: https://aws.amazon.com/security/security-resources/
xx: https://summitroute.com/blog/2017/05/30/free_tools_for_auditing_the_security_of_an_aws_account/
xxi: https://github.com/dagrz/aws_pwn
xxii: https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/
xxiii: http://blog.talosintelligence.com/2017/07/the-medoc-connection.html?m=1
xxiv: https://www.netsarang.com/news/progress_report_of_the_nssock2_dll_backdoor.html
xxv: https://arstechnica.com/information-technology/2017/08/powerful-backdoor-found-in-software-used-by-100-banks-and-energy-cos/
xxvi: https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf
xxvii: http://www.zdnet.com/article/an-insecure-mess-how-flawed-javascript-is-turning-web-into-a-hackers-playground/
xxviii: https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax
xxix: https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832
xxx: https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax
xxxi: https://www.commbank.com.au/content/dam/commbank/assets/business/can/business-insights/signals/commbank-signals-q4-2016.pdf
xxxii: https://www.commbank.com.au/content/dam/commbank/assets/business/can/business-insights/signals/commbank-signals-q3-2016.pdf
xxxiii: https://blogs.microsoft.com/microsoftsecure/2017/08/17/microsoft-security-intelligence-report-volume-22-is-now-available/
xxxiv: https://support.office.com/en-us/article/Set-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6
xxxv: https://support.google.com/a/answer/175197?hl=en
xxxvi: https://support.google.com/a/answer/2984349?hl=en
xxxvii: https://blogs.technet.microsoft.com/office365security/how-to-fix-a-compromised-hacked-microsoft-office-365-account/
xxxviii: http://www.fairinstitute.org/
xxxix: https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks
xl: https://www.asd.gov.au/publications/protect/electronic_devices_os_travel.htm
xli: https://www.piriform.com/news/release-announcements/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users
xlii: http://nccoe.nist.gov/publication/1800-11/index.html
xliii: https://blogs.adobe.com/conversations/2017/07/adobe-flash-update.html
xliv: https://www.ncsc.gov.uk/guidance/penetration-testing
xlv: http://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf
xlvi: https://attack.mitre.org/wiki/Main_Page
xlvii: https://www.us-cert.gov/ncas/alerts/TA17-181A
xlviii: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

CommonwealthBank