Signals

Quarterly security assessment

Q1 2017

CommonwealthBank

Yuval Illuz
Chief Information Security and Trust Officer, Commonwealth Bank

I'm proud to present to our valued clients and partners our seventh edition of Signals, and my first as Chief Information Security and Trust Officer at Commonwealth Bank.

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

This advisory was prepared as part of Commonwealth Bank's ongoing commitment to raising the bar for cyber security within the broader Australian economy.

In this edition we lay the foundations to assist clients and partners to prepare for new mandatory data breach reporting obligations.

We hope and anticipate this report will filter out the noise from public discourse about these laws and provide context and confidence for your security strategy.

Cyber Security:

Trends and Observations

Key trends observed during the quarter

> “Links to **cloud storage** sites require careful inspection.”

Cloud storage infrastructure used in malware campaigns

CBA’s security incident response team and several other sources have noted a marked increase in scams that either employ branding or co-opt infrastructure of popular cloud storage providers such as Google and Dropbox. The branding of these companies is imitated primarily to steal user credentials for password re-use on other services. Phishing campaigns, meanwhile, increasingly include links to pages that feature malicious links or content hosted by these cloud storage services. While cloud service providers continually fine-tune detection of malicious content on their platforms, cybercrime actors appear willing to risk detection in order to make their phishing campaigns appear more legitimate. US organisations are increasingly seeing similar campaigns that host malicious files in cloud software services provided by Adobe, Mailchimp and others. Several such campaigns have targeted Australians. Campaigns that rely on lesser known domains are also employing URL shortening services such as Bit.ly to disguise the destination of a phishing link.

CHECKLIST

- Given the co-opting of legitimate cloud services, controls that block traffic to known bad domains will largely be ineffective against these attacks. Detection logic needs to inspect the malicious file, or what executes from it (macros etc.). If your organisation does not have the capability to break and inspect HTTPS traffic, consider preventative measures included in the Australian Signals Directorate’s revised Essential Eight controls – especially disabling of macros and timely patching of operating systems and browsers (if not full application whitelisting and hardening of user devices). Organisations with a low risk threshold may need to consider blocking access to cloud storage services by default.
- Users need to be made aware that links to cloud storage sites may not be safe and require careful inspection. Commonwealth Bank offers our clients eLearning on cyber hygiene, which includes modules on safe use of email. Contact your account manager or relationship manager should you wish to deploy these learning products to your staff.

Ransomware actors chasing bigger, juicier targets

Attacks by criminal groups that make use of file-encrypting malware to extort payment from infected victims, commonly known as ransomware, have continued unabated despite collaborative efforts by the security industry to share decryption keys and detection indicators. Attackers have in recent months stepped up their game, using scripts to scan the public internet for large, unstructured ‘big data’ databases that could be encrypted. Ransoms have been sought from tens of thousands of administrators of internet-exposed MongoDB, Hadoop and Elasticsearch databases.

CHECKLIST

- Any means of connectivity to your database should be protected, irrespective of platform. Most platforms recommend Kerberos for authentication and SSL/TLS between nodes.
- Ensure the database and underlying operating system are patched at all times.
- Test and development deployments require a basic level of protection the moment they are loaded with real data.
- MongoDB allows for its enterprise security features to be accessed free of charge in development environments. The company has published secure configuration advice and offers a rented hosted service should developers or data analysts wish to experiment without having to invest time in secure configuration.
- Administrators of Elasticsearch should consider installation of the X-Pack extension for bundling of security and monitoring features.
- Administrators of Apache Hadoop should consider running the service in Secure Mode.

By the Numbers

123
data breaches
have been reported to Australian regulators to date.

Verizon will pay
US$350 million less
to acquire Yahoo after a breach of **1 billion** customer records.

Phishing attacks that imitate tax authorities grew
300%
in 2016[viii]

Facebook has paid out
$5m in 5 years
in bug bounties[ix]

Cyber Security:
Trends and Observations

SMiShing campaigns target Australia

Several Australian service providers have noted a significant increase in SMiShing (phishing messages that arrive via SMS). These messages typically include an urgent call to action – such as to re-verify or unfreeze an account that is 'suspended' or set to 'expire', or to claim a tax refund. The message will typically encourage the recipient to click a link to a site controlled by the attacker and ask the recipient to enter credentials. Both the link and the web site will mimic a common service provider, both in terms of branding and registration of similar domains.

CHECKLIST

- Teach your staff to recognise common features of SMiShing scams. CBA and most other banks will never send customers a hyperlink – whether via SMS or email - that asks customers to enter a client number, password, verification code or credit card details. If you receive a suspect message, please screenshot it and forward to hoax@cba.com.au.
- Our partners at SecEDU (the University of New South Wales) are collecting a wider range of SMiShing screenshots for a project that aims to train machines to recognise the common features of a SMiShing campaign. If your organisation runs its own hoax reporting service and wishes to contribute samples of SMiShing emails to the project, please email us.

Threat actors 'blend in'

Post-incident analysis of a number of high-profile attacks in recent months have revealed gains that advanced actors have made in evading detection and forensic analysis. Several actor groups have used a combination of simple social engineering techniques (spoofing, phishing and credential theft) for initial compromise. They then target accounts with administrator privileges and make use of administrative processes (such as the command line and PowerShell, as opposed to download of malware) to ensure their actions "blend in" with legitimate activity on the network. Similar attacks by profit-motivated actors have used what is touted as 'fileless' malware. This term describes a type of malware that – following initial infection – resides in memory to avoid post-incident detection in file systems.

CHECKLIST

- Ensure access to privileged accounts are subject to additional layers of protection. Limit access to system administration tools and processes (such as PowerShell) to specific devices or via multi-factor authentication. Monitor the use of administrator accounts appropriately.
- Disable access to system management tools (PowerShell, for example) in default user configurations.
- Consider providing your incident responders the tools and training required for memory analysis. Most so-called fileless malware does in fact leave some traces of activity in the Windows registry - just in places that may not be as readily monitored as on system files.
- The delivery mechanism for variants of this malware have to date used very traditional means of infection: a macro-enabled Word document attached to a phishing email. Blocking macros by default is the easiest way to avoid initial infection.
- Security functions that automate detection and triage of commodity threats create more bandwidth for a regular cadence of 'hunt' missions that can discover anomalous network activity. The clues to a patient, concealed attacker may be observable in your logs, even if alarms haven't triggered.

Concerns over use of destructive malware

Malware that wipes the data on infected systems, while occasionally utilised by nation-state actors against state-owned entities, is rarely used against private-sector companies[i]. But as geopolitical tensions rise in Eastern Europe, the Middle East and North Asia, an alarming cluster of recent attacks have utilised these destructive capabilities against a broader set of targets. In November 2016, a new variant of the Shamoon/Disstrack malware that was originally used to wipe 35,000 devices of Saudi state-owned oil company Saudi Aramco[ii] was reportedly used against new public sector targets[iii] in the Middle East[iv]. In December 2016, attacks on the Ukrainian power grid used malware dubbed Killdisk to both inflict damage and erase event logs that would aid investigation. The same malware was detected on the systems of Ukrainian banks[v] in January 2017. In March, a third strain of Shamoon – dubbed 'StoneDrill' was found to have infected targets in both the Middle East and Europe[vi]. While some of these attacks appear targeted[vii] to only fire if the infected entity operates in a conflict zone, the increase in activity compelled a consortia of US financial services regulators (the FFIEC) to formally warn banks of the risks the malware represents to business continuity.

CHECKLIST

- The increased use of both file-encrypting ransomware and file-wiping destructive malware requires organisations to renew their focus on business continuity and rapid incident response.
- Several of the aforementioned malware campaigns relied on the oldest and most effective tricks in the book to compromise a target – via a phishing email that comes with an attached Word file with embedded malicious macros. At-risk industries should consider blocking or disabling the execution of macros that are downloaded from email in the first instance.
- Backup your systems. Practice restores.
- The US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has released an overview of destructive malware detected in the wild and some related mitigation advice.

By the Numbers

Over **100,000 Australians** have now been trained in security awareness using **CBA**'s 'Cool, Calm and Connected' suite.

62 new ransomware families appeared in 2016[x]

27 Adobe Flash vulnerabilities were used in exploit kits in 2016[xi]

Deep Dive:

Data Breaches: Discovery to Disclosure

How quickly do companies typically disclose data breaches once discovered?

Brett Winterford
Senior Manager, Cyber Outreach and Research

Jessica Woodall
Manager, Cyber Outreach

Australia will have a mandatory data breach notification scheme after the Australian Parliament passed the Privacy Amendment (Notifiable Data Breaches) Bill 2017 on 13 February 2017. [xl] For details on the Act, see 'Regulatory and Legal" in the pages ahead.

The Bill amends the Privacy Act 1988 (Cth) to introduce a mandatory requirement for agencies and companies subject to the Privacy Act to notify the Office of the Information Commissioner and affected individuals of privacy breaches that are "likely to result in serious harm." [xli]

The new "likely to result in serious harm" threshold is similar to the existing "real risk of serious harm" benchmark set out in the current set of voluntary data breach notification standards which many organisations will be familiar with.

The change that will perhaps drive the biggest rethink is the provision that compels organisations to conduct an investigation within 30 days to determine whether a data loss event warrants notification.

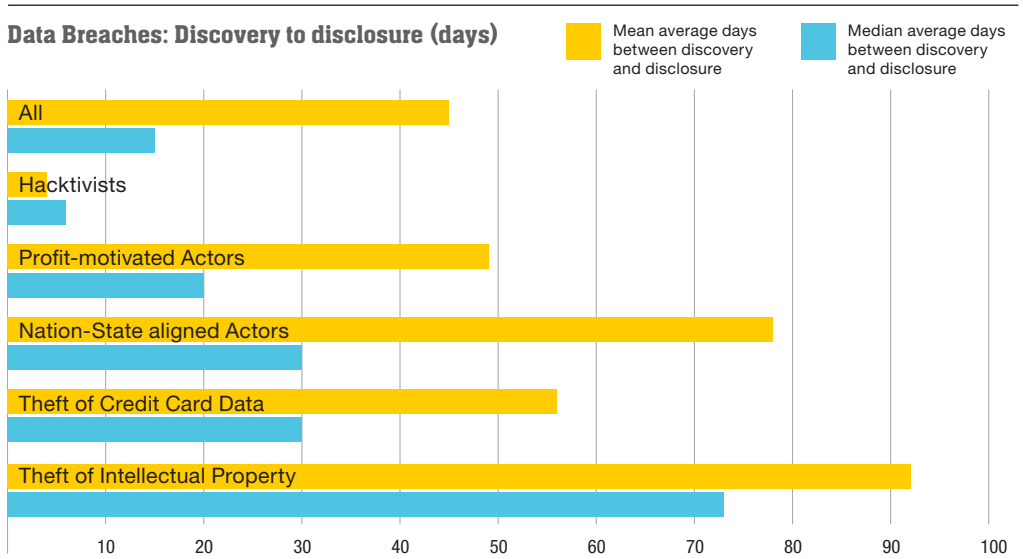
This raises the question of whether 30 days is a realistic timeframe within which an organisation - upon first becoming aware of a large scale breach - can properly assess the potential impacts of the breach and, therefore, the need to notify.

International comparisons

Australia's implementation of mandatory data breach notification is broadly consistent with existing requirements in many US states, and proposed requirements in Canada and Europe. But there is distinct variation across these laws when comparing the amount of time allowed by organisations to investigate a breach before a determination must be made to notify or not.

As of 2016, 45 of the 50 US states were not explicit in this regard – relying on a principles-based approach. In the main, these states require that a breach is reported "expeditiously" and "without unreasonable delay", subject to both the needs of law enforcement and usually the time required "to determine the scope of the breach" and/or to "restore the integrity of the system."

Three US states set an explicit threshold for response. Like Australia, Florida requires a breached entity to notify within 30 days, while Ohio and Wisconsin set a threshold of 45 days (with some allowance for the volume of customer notifications required to be sent). [xlii] The European Union's new General Data Protection Regulation (GDPR), which will apply to organisations holding EU citizen data by May 2018, makes a distinction between obligations to regulators and to customers. It will require that a breached entity notify regulators "not later than 72 hours after having become aware of it" and to notify customers "without undue delay". However, authorities acknowledged that breach investigations take time and made provisions for information to be provided in phases. In assessing the need to report to regulators, organisations will be motivated to err on the side of caution, as fines of up to 20 million Euros or four percent of the entity's turnover from the previous year can be levied for non-compliance. [xliii]



Our analysis

We conducted an analysis of 94 of the largest data breaches made public over the last 10 years and plotted the time between discovery and disclosure of data breaches.

In the chart, we have presented the median and average duration between an entity becoming aware of a breach and its disclosure.

The median number of days between discovery and disclosure during major data breach events was 15 days, well below the 30-day threshold set in Australian legislation.

Deep Dive:

Data Breaches: Discovery to Disclosure

> “The median number of days between **discovery and disclosure** during major data breach events was **15 days**.”

The median number of days between discovery and disclosure of a breach provides stronger guidance than the average, as it accounts for outlier events in the data set in which security incidents were subject to long law enforcement investigations prior to disclosure.

Motivations

When breaking down incidents by motivation, breaches that involved theft of significant intellectual property or that were conducted by nation-state aligned actors took considerably longer to report to the public. Attacks attributed to profit-motivated criminals or involving theft of customer data were given more urgent attention.

Breaches caused by hacktivists, predictably, drew the most immediate response. Often hacktivists will publicly release details of a data breach, forcing an immediate reaction from the compromised organisation.

Our analysis also noted a correlation between the initial point of compromise and the time required to respond.

Organisations whose networks were breached after a phishing attack took around 30 days (median) to disclose, while those compromised via a vulnerability in a web application only took a week (median). As with attacks perpetrated by hacktivists, this highlights the urgency with which an organisation needs to respond when information about the attack is already available to the public via some other means.

Capacity to respond to data breaches will vary from organisation to organisation. Putting in place a strong data breach response strategy will help position companies and agencies subject to the Privacy Act to undertake a quicker response in line with their new legislative obligations.

Over 40%
of data breaches in 2016 were discovered by law enforcement

Over 30%
by other third parties,

Under 20%
by internal security teams.

Source: Verizon DBIR 2016[xix]

How big is the problem?

In the absence of mandatory reporting of data breaches, it has been difficult for government to get a clear view of the scale of security incidents occurring in Australia.

Existing data from jurisidictions with mandatory reporting regimes, or indeed from incidents managed within the Australian Government, provide some context:

- **123 breaches** were voluntarily reported to the Office of the Australian Information Commissioner in 2015/16;
- Between January 1 2015 and June 30 2016, **1095 incidents** in Australian Government systems warranted “an operational response” from the ACSC.
- There were over **1000 data breaches** reported to US authorities in 2016.
- **2260 data breaches** were recorded by Verizon in its global 2016 data breach investigations report.

Read on for more on data breach notification laws, including:

- A brief description of new Australian and European legislation;
- Deep Dive: How do (the worst) data breaches happen?
- Deep Dive: How markets respond to data breaches.

Deep Dive:

How (the worst) data breaches happen

A study of the top 100 data breaches of the last ten years

Brett Winterford
Senior Manager, Cyber Outreach and Research

Australia's business community has – in the main - evolved its security practices considerably over the past 3-5 years in response to a series of very large, public data breaches.

The imminent introduction of mandatory data breach notification will nonetheless provide further incentive to invest in cyber security capabilities, and generate better data on how attacks are typically perpetrated against Australian organisations.

The most reliable insights into how organisations have typically been attacked has to date been either (a) US-centric, owing to the earlier adoption of notification laws in some states, or (b) provided by security service providers that hold some interest in elevating cyber security issues into public discourse.

For a more global sense of the control gaps most often exploited, and the costs and impact of a data breach, this series of Deep Dives analyses the top 100 breaches made public over the past ten years. Owing to the relatively small size of the sample set, and relatively large scale of the breaches analysed, its value lies as a point of comparison upon which to validate existing studies and security advice.

Initial attack vector (point of compromise)

While there are many ways an adversary might gain unauthorised access to an organisation's data, the world's largest and most damaging data breaches have generally commenced with one of two initial vectors, or methods, of attack, which are expressed in the table below.

Almost one-third (29%) of the intrusions in the top 100 list involved an attacker compromising a third party of the organisation (e.g. a supplier). This could be through compromising the third party's integrations or connections into the organisation, or acquiring stealing credentials into the organisation that the organisation itself had provided to the third party.

Mitigations

Most security teams have programs in place to blunt the efficacy of phishing campaigns (such as analysis and filtering of web and email traffic and security awareness programs for staff and suppliers) and to stem the most common forms of attacks against web applications (such as penetration testing and a rigorous vulnerability/ patch management process).

Even the best resourced security teams, however, don't assume that today's tools and processes can keep out 100% of targeted intrusions, especially from determined and well-funded adversaries. So in addition to refining the preventative and detective measures, security teams must increasingly focus on thwarting the actions an adversary will likely undertake to achieve their objectives after an initial compromise – actions like downloading of malicious software payloads, further reconnaissance and lateral movement across an organisation's network, and access and exfiltration of sensitive data.

The top mitigations recommended by the Australian Signals Directorate, each rated according to complexity and ongoing cost, are reproduced in full over the coming pages for your security team to consider.

No security control is a silver bullet and very few are easy to implement effectively. But collectively they impose costs on an adversary that they seek easier wins elsewhere.

49% OF THE TOP 100 DATA BREACHES 2007-2016 WERE CAUSED BY TARGETED PHISHING

Description	Top 5 brands imitated in Phising attacks (2016)
An attacker sends a spoofed email or SMS to trick a legitimate user into either sharing their credentials or downloading malicious software from a page accessible by the attacker. The credentials provide the attacker initial access to the network for further reconnaissance and lateral movement.	1. Australian Federal Police-branded traffic infringement notice 2. Australian Federal Police notice of criminal charges 3. AGL (electricity) bill 4. Australia Post missed delivery notice. 5. State Debt Recovery Office notice.

xliv

41% OF THE TOP 100 DATA BREACHES 2007-2016 WERE CAUSED BY A WEB APP VULNERABILITY

Description	Top 5 most exploited web app vulnerabilities (2013)
An attacker exploits a misconfiguration or vulnerability in an internet-facing website/ application in order to compromise the web server, gain a foothold on a network or harvest user credentials.	1. Injection 2. Cross-Site Scripting 3. Broken Authentication and Session Management 4. Insecure Direct Object References 5. Cross-Site Request Forgery

xlv

Deep Dive:

How (the worst) data breaches happen

> “Newer groups of profit-motivated actors are **gravitating to ransomware** and **email payment** fraud.”

Threat Actors (Top 100 Data Breaches, 2007-2016)

Actor Profile	Responsible for (%) of the Top 100 Data breaches, 2007-2016	Typical characteristics	Historical targets/victims
PROFIT-MOTIVATED ACTORS (CYBERCRIME)	**60%** (approx)	Profit-motivated criminal groups have traditionally relied on exploitation of web application vulnerabilities (especially SQL Injection) for initial access, but are today as likely to use any combination of techniques to achieve their objectives. These actors might seek to exfiltrate payment card data from retailers for use in fraud, or user credentials and other personally-identifying data for sale or use in future criminal endeavours. Newer groups of profit-motivated actors are gravitating to ransomware and email payment fraud.	• Financial service providers. • Retailers that collect or store payment card data. • Cloud service providers. • Organisations that store or process privileged or share price-sensitive information. • Organisations that hold significant volumes of user credentials.
NATION-STATE ALIGNED ACTORS	**30%** (approx)	Since 2009, targeted attacks by nation-state aligned actors have been responsible for a growing share of attacks that have later been made public (~30%), with awareness of these attacks peaking between 2011 and 2014. The majority of these attacks (over 85%) began with targeted (spear) phishing. Typically, these actors have sought to collect information about government and defence industry employees and contractors as part of espionage operations, or have sought to steal intellectual property from foreign organisations as a means of providing advantage to domestic industry. In more recent times, nation-state aligned actors have gained greater notoriety via disruption and influencing campaigns (such as the attacks on the US electoral system and Ukrainian power grid) if not destruction (such as attacks on Sony Pictures and Saudi Aramco).	• Government agencies or state-owned enterprise. • Organisations in the military supply chain. • Organisations that provide services and hold data on government and military personnel (insurers, healthcare, financial services etc.) • Telcos and Internet Service Providers. • Organisations whose competitive edge stems from unique intellectual property. • Organisations in trade disputes within jurisdictions with scant regard for intellectual property protection. • Cloud service providers. • IT infrastructure providers.
ISSUE-MOTIVATED ACTORS	**7%** (approx)	The threat posed by issue-motivated actors (hacktivists) became a subject of intense public interest from 2011 after a spate of attacks that exploited known vulnerabilities in web applications. The ability (or willingness) of these actors to effect large scale data breaches has waned in recent years in the wake of significant arrests of members of such groups as Anonymous and LulzSec. The remaining issue-motivated actors of concern are largely aligned with or tolerated by nation-states.	• Government agencies or state-owned enterprise. • Online gaming providers. • Organisations that perform services for high-net worth individuals. • Organisations with poor environmental or human rights records. • Organisations that litigate against small targets. • Organisations with demonstrable lack of regard for security personal data.

Mitigation Strategies recommended by The Australian Signals Directorate (ASD) Feb 2017

Relative security effectiveness	Mitigation strategy	Potential user resistance	Upfront cost (staff, equipment, technical complexity)	Ongoing cost (mainly staff)
Mitigation strategies to prevent malware delivery and execution				
ESSENTIAL	Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	●●	●●●	●●
ESSENTIAL	Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.	●	●●●	●●●
ESSENTIAL	Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	●●	●●	●●
ESSENTIAL	User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.	●●	●●	●●
EXCELLENT	Automated dynamic analysis of email and web content run in a sandbox, blocked if suspicious behaviour is identified e.g. network traffic, new or modified files, or other system configuration changes.	●	●●●	●●
EXCELLENT	Email content filtering. Whitelist allowed attachment types (including in archives and nested archives). Analyse/sanitise hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros.	●●	●●	●●
EXCELLENT	Web content filtering. Whitelist allowed types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains.	●●	●●	●●
EXCELLENT	Deny corporate computers direct Internet connectivity. Use a gateway firewall to require use of a split DNS server, an email server, and an authenticated web proxy server for outbound web connections.	●●	●●	●
EXCELLENT	Operating system generic exploit mitigation e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	●	●	●
VERY GOOD	Server application hardening especially Internet-accessible web applications (sanitise input and use TLS not SSL) and databases, as well as applications that access important (sensitive or high-availability) data.	●	●●	●●
VERY GOOD	Operating system hardening (including for network devices) based on a Standard Operating Environment, disabling unneeded functionality e.g. RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR and WPAD.	●●	●●	●
VERY GOOD	Antivirus software using heuristics and reputation ratings to check a file's prevalence and digital signature prior to execution. Use antivirus software from different vendors for gateways versus computers.	●	●	●
VERY GOOD	Control removable storage media and connected devices. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth/Wi-Fi/3G/4G devices.	●●●	●●●	●●
VERY GOOD	Block spoofed emails. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail' SPF TXT and DMARC DNS records to mitigate emails that spoof the organisation's domain.	●	●	●
GOOD	User education. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as well as unapproved: removable storage media, connected devices and cloud services.	●●	●●●	●●
LIMITED	Antivirus software with up-to-date signatures to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.	●	●	●
LIMITED	TLS encryption between email servers to help prevent legitimate emails being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted.	●	●	●
Mitigation strategies to recover data and system availability				
ESSENTIAL	Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.	●	●●●	●●●
VERY GOOD	Business continuity and disaster recovery plans which are tested, documented and printed in hardcopy with a softcopy stored offline. Focus on the highest priority systems and data to recover.	●	●●●	●●
VERY GOOD	System recovery capabilities e.g. virtualisation with snapshot backups, remotely installing operating systems and applications on computers, approved enterprise mobility, and onsite vendor support contracts.	●	●●●	●●

Relative security effectiveness	Mitigation strategy	Potential user resistance	Upfront cost (staff, equipment, technical complexity)	Ongoing cost (mainly staff)
Mitigation strategies to limit the extent of cyber security incidents				
ESSENTIAL	Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.	●●	●●●	●●
ESSENTIAL	Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.	●	●●	●●
ESSENTIAL	Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.	●●	●●●	●●
EXCELLENT	Disable local administrator accounts or assign passphrases that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials.	●	●●	●
EXCELLENT	Network segmentation. Deny network traffic between computers unless required. Constrain devices with low assurance e.g. BYOD and IoT. Restrict access to network drives and data repositories based on user duties.	●	●●●	●●
EXCELLENT	Protect authentication credentials. Remove CPassword values (MS14-025). Configure WDigest (KB2871997). Use Credential Guard. Change default passphrases. Require long complex passphrases.	●●	●●	●
VERY GOOD	Non-persistent virtualised sandboxed environment, denying access to important (sensitive or high-availability) data, for risky activities e.g. web browsing, and viewing untrusted Microsoft Office and PDF files.	●●	●●	●●
VERY GOOD	Software-based application firewall, blocking incoming network traffic that is malicious/unauthorised, and denying network traffic by default e.g. unneeded/unauthorised RDP and SMB/NetBIOS traffic.	●	●●	●●
VERY GOOD	Software-based application firewall, blocking outgoing network traffic that is not generated by approved/trusted programs, and denying network traffic by default.	●●	●●	●●
VERY GOOD	Outbound web and email data loss prevention. Block unapproved cloud computing services. Log recipient, size and frequency of outbound emails. Block and log emails with sensitive words or data patterns.	●●	●●	●●
Mitigation strategies to recover data and system availability				
ESSENTIAL	Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.	●	●●●	●●●
Mitigation strategies to detect cyber security incidents and respond				
EXCELLENT	Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access and network activity.	●	●●●●	●●●●
VERY GOOD	Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	●	●●	●●
VERY GOOD	Endpoint detection and response software on all computers to centrally log system behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry-level option.	●	●●	●●
VERY GOOD	Hunt to discover incidents based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analysed threat data with context enabling mitigating action, not just indicators of compromise.	●	●●●●	●●●●
LIMITED	Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	●	●●●	●●
LIMITED	Capture network traffic to and from corporate computers storing important data or considered as critical assets, and network traffic traversing the network perimeter, to perform incident detection and analysis.	●	●●●	●●

Read more at https://www.asd.gov.au/infosec/mitigationstrategies.htm

Deep Dive:

How markets respond to data breaches

Do the share prices of listed companies suffer after reporting a data breach to the public?

Brett Winterford
Senior Manager, Cyber Outreach and Research

The introduction of mandatory data breach reporting in the United States led to a deluge of information about security incidents. Given Australia's legislation is not dissimilar to that of many US states, we can anticipate a similar trend here. However many Australian organisations have little or no experience speaking publicly about their security posture. Understandably, many will be anxious about the commercial impacts resulting from security-related disclosures. To bring some clarity and confidence to the subject, we sought to analyse the market impact for organisations publicly reporting a data breach. We studied the medium-term impact of a major data breach event on 75 publicly-listed organisations, to conclude that:

- The US market tends to accept that a well-protected organisation can nonetheless be breached;
- The impact of a breach on a company's share price is largely determined by what data was pilfered and the magnitude of the loss, as well as what the market might infer about the organisation's security capability from the level of protection applied to the data prior to its theft, and the confidence with which the breached entity communicates how it will remediate customer impacts.

Companies that suffer data breaches will perform...

1.5% Lower
... than their medium term trajectory

2% Lower
... than the broader market

3-4% Lower
... than competitors

11.5% Lower
... if financially sensitive information is stolen.

Methodology

Our approach borrows from the work of Sean Mason, a US-based security engineer who posited that since at least 2014, there has been little discernable impact on a US organisation's share price within a week or a year of a major data breach. To validate his hypothesis, we took a thorough look at a larger sample of entities – many from outside the US – that were breached over the last ten years.
Instead of focusing on point-in-time events, we compared average growth in a breached

Table 1: Who was hit the hardest?

Company	Records Stolen	Type	Year	Stock Performance (100-Day Moving Average)	Market Adjusted
Heartland Payment Systems	133 million	Credit Card/Payment data	2009	-56.70%	**-49%**
Target	70 million	Credit Card/Payment data, PII data	2013	-46.03%	**-48%**
TalkTalk	~157K	Bank Account Numbers, PII data (customer Details)	2015	-28.78%	**-28%**
Wyndham Hotels	~600K	Credit Card/Payment data	2008	-38.17%	**-23%**
Belfius Bank (Dexia)	~3K	Highly sensitive data (customer income, ID card numbers)	2012	-35.09%	**-23%**
Sony (PSN Breach)	77 million	Credit Card/Payment data, PII data	2011	-20.37%	**-22%**
Zappos.com (Amazon)	24 million	PII data (customer details)	2012	-6.51%	**-19%**
Deutsche Telekom	17 million	PII data (customer details)	2008	-18.50%	**-15%**
Global Payments	1.5 million	Credit Card/Payment data	2012	-13.63%	**-14%**
Hilton Hotels	Unknown	Credit Card/Payment data	2015	-12.54%	**-14%**
eBay	148 million	PII data (customer details)	2014	-5.99%	**-12%**

Deep Dive:
how markets respond to data breaches

> “we can say with confidence that **1 in 2 breached organisations shift to a lower rate** of share price growth.”

entity’s share price in the 100 days immediately after the public learns of the breach with the 100-day moving average of the same stock immediately prior to the event. We also controlled for general trends in the broader share market and for similar companies in the same period.

The questions we sought to answer were: Did the breach event materially change the trajectory of the organisation’s fortunes? Under what conditions is there a greater or lesser impact?

Results

While individual share prices are subject to a wide variety of influencing factors, in aggregate we can say with confidence that 1 in 2 breached organisations shift to a lower rate of share price growth in the 100 days that follow publicity of a breach event. The stocks of companies whose data breach is known to the public will, on average:

- Perform 1.5% worse in the 100 days after the public learns of the breach than it performed in the 100 days prior;
- Underperform against the broader stock market by an average of 2-4%, in the 100 days after the public learns of the event.

The share price for organisations that have lost payment or card data will also perform close to 11.5% lower in the 100 days after a breach than the 100 days prior, and lag the broader share market by up to 20%.

This suggests the ability of card associations (Visa, Mastercard etc.) to seek legal relief against the fraud losses caused by a breach of payment data is more of a market mover than public disclosure of the breach.

We can also say – again in the aggregate – that the share market is more forgiving where a nation-state actor has been blamed for a data loss incident (no net negative impact), than situations where profit-motivated criminals are responsible, even when intellectual property has been stolen. That said, there are several examples where cyber-enabled intellectual property theft has hurt an entity’s long-term competitiveness.

Impacts are inconsistent

As anticipated, the magnitude of high profile data breaches that occurred at Heartland (133m records stolen), Sony (77m) and Target (70m) led to them being among the poorest performing stocks over the 100 days following the incident. The absence of Yahoo (1 billion

Table 2: Costs To Consider

Type Of Cost	Example	Year
Market valuation	Yahoo has agreed to accept a valuation at US$350m+ lower than it had originally negotiated with acquirer Verizon[xx] after discovery of a breach of over a billion user credentials.	2017
Settlement with card associations	Of the US$139m+ of costs from a 2007 breach of 94 million customer records, TJX paid over US$70m to card associations Visa and Mastercard[xxi].	2007
Credit protection for affected customers	Of the US$260m+ expenses incurred to data from a 2014 breach of 78 million healthcare records from insurer Anthem, the company spent at least US$112 million on providing credit protection to affected customers.[xxii]	2014
Intellectual Property theft	Microsoft and several partners in its gaming business (Xbox) claimed that the cumulative costs of attacks that stole critical intellectual property exceeded US$100m.[xxiii]	2014
Customer notification	Of the US$260m+ expenses incurred to data from a 2014 breach of 78 million healthcare records from insurer Anthem, at least US$31 million was spent on processes to identify to notify affected customers.[xxiv]	2014
Legal fees	Of the US$140m+ of costs from a 2009 breach of 133 million records, Heartland Payment Systems spent at least US$26m in legal fees.[xxv]	2009
Settlement with issuers	Of the US$291m+ in breach related expenses reported by Target after the theft of 40m payment card details and PII data on 70 million customers, the retailer paid at least US$67m to card associations, US$40 million directly to banks and credit unions (issuers) and US$10m to customers.[xxvi] Of the US$263m+ in costs associated with a breach of 50 million records in 2014, retailer Home Depot paid at least US$25 million in damages to card issuers.[xxvii]	2013 2014
Regulatory fines	AT&T paid a US$25m settlement with the US Federal Trade Commission after an insider-led data breach involving third party data centres led to a loss of 278,000 customer records.[xxviii] Regulatory fines in the UK have rarely exceeded 2-3 million pounds, but will be far larger under the proposed EU GDPR [xxix] Recent regulatory fines imposed in the US against Adobe[xxx] and LinkedIn[xxxi] have not exceeded US$1.5m.	2015

Deep Dive:
how markets respond to data breaches

> “the total cost of responding to a breach is **rarely realised immediately** or in the medium-term”

Table 2: Costs To Consider *(continued)*

Type Of Cost	Example	Year
Investigation costs	Of the ~US$100 million in costs incurred by Global Payments after a 2012 breach of several million payment records, the company reported that close to half was spent on investigating and remediating the breach to achieve the necessary compliance to continue doing business.[xxxii]	2012
Business interruption	A data breach affecting Ireland-based LoyaltyBuild caused the organisation to withdraw services from the market for several months. Profits subsequently dropped from 1m pounds in 2013 to a 2014 loss of 18m pounds.[xxxiii]	2013
Loss of market share	Australian electronics manufacturer Codan was forced to slash the price of some of its products after foreign competitors gained unauthorised access to its intellectual property and began producing cheaper units. In the year following the attack, net profit fell from AU$45m to US$9.2m.[xxxiv]	2011
Customer class action	Of the US$178m+ in post-breach expenses, Sony Online Entertainment agreed to pay US$15 million of settle a class action lodged by customers affected by the 2011 breach of the Playstation network.[xxxv]	2011
Settlement with affected staff	Sony Pictures agreed to spend U$S8 million to settle legal action lodged by staff impacted by the 2014 cyber-attack on the company.[xxxvi]	2014
Lost opportunities	A targeted cyber intrusion by a nation-state actor was blamed for the breakdown of Coca Cola’s US$2.4 billion acquisition of a Chinese drink manufacturer, Huiyuan Juice.[xxxvii]	2009
Loss of leadership	High profile data breaches have led to senior resignations at Target[xxxviii] (70m records stolen) and the US Office of Personnel Management[xxxix] (21 million records).	2015
IT security uplift	Data breaches have encouraged many organisations to make considerable investments in cyber security capability. JP Morgan doubled its cyber security budget from US$250 million to US$500 million a year in 2014 after cyber-enabled fraud events . Both Anthem and Target spent over US$100 million in the immediate aftermath of breaches to improve cyber security capability.	2014

records stolen), Adobe (153m) and LinkedIn (117m) from nearer to the top of the ‘most impacted stocks’ list – and, conversely, the presence of firms that disclosed much smaller breaches – suggests the market considers a broader set of factors than the size of a breach.

These might include the sensitivity of the information stolen. Client loan applications stolen from Belfius, a subsidiary of Belgium’s Dexia Bank, provided cybercriminals a full range of sensitive financial information about victims, and was held by a malicious actor with clear intent to extort or damage the company.

Other considerations include indicators of the organisation’s competency – for example, whether stolen credentials were stored unprotected in clear text (as per 2011-era Sony Pictures breach), or whether the attack exploited known vulnerabilities that the organisation could not or chose not to address expediently. Wyndham Hotels, for example, lost ~600,000 payment card details (versus the many millions of records stolen in other breaches), but the lack of network segmentation, storage of payment data in clear text and an unsatisfactory response to three consecutive breach events led to regulatory action, which typically stokes anxiety among investors.

In conclusion

While this analysis reflects that investors may be more forgiving of public disclosure of a data breach than would typically be assumed, the total cost of responding to a breach is rarely realised immediately or in the medium-term.

The largest share of costs [see Table 2] are likely to be borne by a breached entity irrespective of any legal duty to report the breach.

The impact regulators or investors are likely to play in adding to those costs are largely determined by how prepared you are to respond.

Regulatory & Legal

New laws and legal precedents relevant to security strategy

> “Entities will have to report eligible breaches **“as soon as practicable”** after becoming aware of them”

Australian data breach laws pass Parliament

Australia’s Privacy Amendment (Notifiable Data Breaches) Bill 2017 became law in February. Government agencies and private sector organisations with an annual turnover of more than $3 million will be required to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals if they experience an ‘eligible data breach’. Eligibility is determined by whether in the opinion of a ‘reasonable person’, *“access or disclosure [to personal information] would be likely to result in serious harm to any of the individuals to whom the information relates”*. Entities will have to report eligible breaches “as soon as practicable” after becoming aware of them, and if unsure must investigate within 30 days or seek an extension from the regulator. The OAIC has authority to pursue civil penalties of up to $1.8 million for ‘serious and repeated’ breaches, but has historically preferred to offer non-compliant organisations to enter into enforceable undertakings[xii] and leave open the option of a civil penalty if that offer is refused. Timing for when the mandatory scheme will take effect has not yet been announced, though it must commence by 22 February 2018 at the latest.

CHECKLIST

- Australian organisations have a short window with which to ensure that policies, processes and systems are in place for compliance within the new laws. Read on to pages 8-16 for our analysis of how organisations are typically breached, how quickly they tend to respond, and how markets tend to react to disclosure of these events.

Big fines for breaches of new EU privacy laws

The European Union has set fines of 20 million euros or up to 4% of a company’s annual turnover for breaches of new privacy law that come into effect on May 25, 2018. The EU General Data Protection Regulation (GDPR) will, among other rules, compel companies to notify affected individuals when a loss of their personal data occurs. All companies with a presence in the EU are subject to the new rules, as are companies outside the EU that store information relating to EU citizens.

CHECKLIST

- Personally identifiable information includes technical data such as passwords, pin numbers and IP addresses and data about physical characteristics such as age, race, physical attributes, and gender.
- Visit the GDPR portal to assess if these new regulations apply to your organisation.
- Preparing for compliance with Australia’s new mandatory data breach legislation in the first instance will put an organisation that operates in Europe in good stead prior to May 2018.

A right to spy?

The UK is now subject to the Investigatory Powers Act 2016, which aims to improve transparency and clarity of law by consolidating existing powers available to the UK security and intelligence agencies to obtain communications data and metadata. The Act compels any “Communications Service Provider” (including telcos, ISPs, providers of online applications, websites or online messaging services) to retain internet connection records for 12 months and remove encryption from those records when given notice by a UK security authority. The Act also brings into law the right of security agencies to engage in bulk collection and analysis of communications data and to compromise (hack) CSP’s infrastructure without permission in order to monitor and analyse communication flows. The UK Government has pledged that it will reimburse any direct costs incurred by affected service providers as a result of these activities.

CHECKLIST

- The Act allows UK surveillance agencies to use the powers against foreign companies, via collaboration with local enforcement in the relevant foreign State. For example, Scotland Yard may request assistance from the Australian Federal Police to collect retained private data based upon approved warrant mechanisms. Concerned organisations that offer digital products and services within the United Kingdom should seek advice from your legal counsel.

Regulatory & Legal:

New laws and legal precedents relevant to security strategy

> “IoT devices should be **updated with security patches** as soon as they become available.”

Trump’s cyber plans take shape

A leaked draft of the White House’s first Executive Order on cyber security sought consolidation of responsibility for the protection of government networks under the White House’s Office of Management and Budget. President Trump intends to nonetheless hold agency heads accountable for breaches on their networks and will likely encourage them to adopt a framework developed by the National Institute of Standards and Technology (the NIST cyber security framework). The draft Order was praised by former Obama Cybersecurity coordinator Michael Daniel for taking a “risk-based approach to cybersecurity” and working to deepen private sector ties[xiv]. In March, Trump released a budget proposal which included USD$1.5 billion for Homeland Security to assist with reinforcement of government networks, but the overall funding picture remains unclear[xv]. A revised version of the Order is rumoured to be close to release.[x i]

CHECKLIST

- The NIST cyber security framework is a respected, voluntary, cross-industry guide for private sector organisations on how to develop a prevention, detection and response strategy, and a good starting point from which senior security leaders can build a strategy.

FTC takes the fight to consumer device vendors

The US Federal Trade Commission (FTC) has stepped up efforts to crack-down on the unauthorised mining of customer information and data from ‘smart devices’. The FTC doled out AU$3.27 million worth of fines to Chinese electronics maker LeEco for mining activities undertaken by its U.S. subsidiary Vizio, which makes smart TVs. The FTC found that Vizio had gathered information on the viewing habits of its customers and on-sold the data to third parties without customer consent.[xvii] Concerns surrounding the security of IoT and smart devices following the Mirai botnet have previously led to the recall of thousands of devices configured with default passwords.[xviii]

CHECKLIST

- US CERT advice on how to prevent malware infections on IoT devices recommends that users change all default passwords to strong passwords (as default usernames and passwords for most devices can easily be found on the Internet).
- Universal Plug and Play, a communications protocol that supports seamless discovery of networked devices in homes (televisions, printers, etc.), is often enabled by default in consumer-grade broadband routers. Many implementations do not authenticate new devices connecting to the network. Subsequently, UPnP should not be considered as fit-for-purpose in business environments without the addition of compensating controls.
- IoT devices should be updated with security patches as soon as they become available.
- Organisations concerned with security should only purchase IoT devices from companies with a reputation for sound security practices and ongoing product support.

Active defence back on the table, briefly

The active defence debate has kicked off again in the United States after Republican Congressman Tom Graves introduced a bill that seeks to alter the Computer Fraud and Abuse Act to allow for more aggressive defensive measures. Graves wants to permit ‘the use of limited defensive measures that exceed the boundaries of one’s network in an attempt to identify and stop attackers.’ FBI Director James Comey quickly poured cold water on the idea: “it runs a risk of tremendous confusion in a crowded space … hacking back could cause all kinds of complications for things we’re trying to do to protect you.” [xix]

CHECKLIST

- Australian industry is split on active defence. According to a survey conducted by The Australian Strategic Policy Institute: 60% of respondents were against any form of hacking back, 10% agreed there should be a right to do so, and 40% were undecided.
- Currently in Australia, the Crimes Act and the Cybercrime Bill 2001 prevents the unauthorised access, modification or impairment of data held on a computer.

Better Practice:

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

Get the essentials right

The Australian Signals Directorate has updated the 'Top Four' strategies it recommends organisations adopt to mitigate cyber intrusions to what it now calls the 'Essential Eight'. A larger list of ASD recommended mitigations is included in this edition of Signals.

Protect your network from destructive malware

The US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has released a overview of destructive malware used in the wild and some related mitigation advice.

Secure by design

Google has bared all about its approach to embedding secure designs into every component of its stack from the ground up. While organisations running legacy systems don't have the luxury to re-think their entire approach, this document is a sound blueprint for those starting the journey fresh.

Lock down those life-saving medical devices, please

The US Federal Drug Administration has issued guidance for secure management of medical devices – guidance that may in the future inform an enforceable standard.

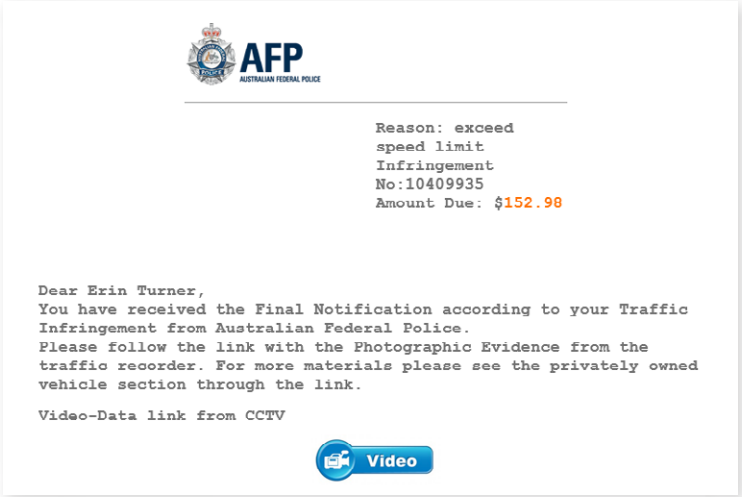
Going travelling?

The Australian Signals Directorate has refreshed its advice for government personnel travelling overseas with an electronic device. Much of the advice in this brief one-pager is pragmatic enough to be applied in the private sector. Enjoy your trip!

One last warning on macros

The last time the Australian Signals Directorate warned agencies about the dangers inherent in execution of macros in Microsoft Office files was 2012. Five years later and the problem isn't going away. The advice has been refreshed to reflect ongoing attacks.

Phish Eyes:



AFP
AUSTRALIAN FEDERAL POLICE

Reason: exceed
speed limit
Infringement
No:10409935
Amount Due: $152.98

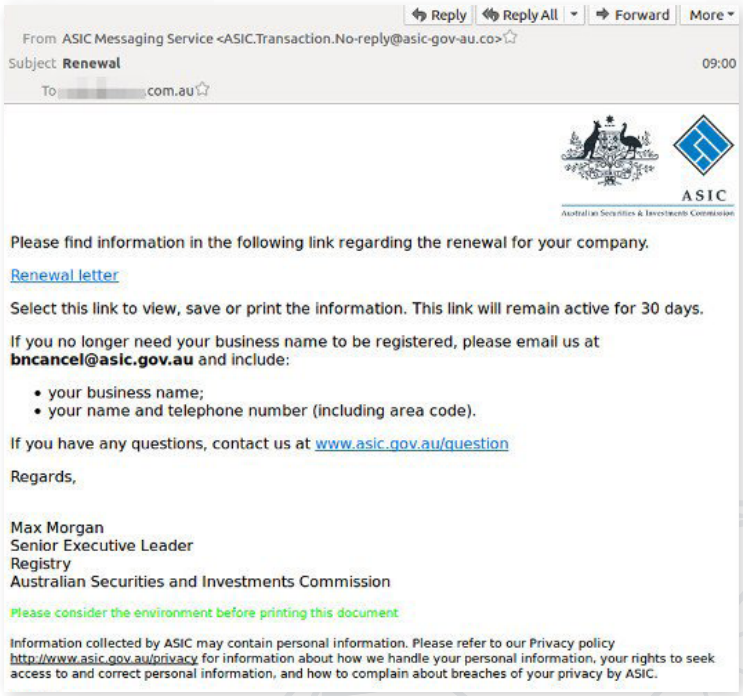
Dear Erin Turner,
You have received the Final Notification according to your Traffic Infringement from Australian Federal Police.
Please follow the link with the Photographic Evidence from the traffic recorder. For more materials please see the privately owned vehicle section through the link.

Video-Data link from CCTV

Video

Look familiar?! This, according to the Australian Criminal Intelligence Commission, is the most persistent phishing campaign used against Australians for some time.

Source: CBA staff



Reply | Reply All | Forward | More

From ASIC Messaging Service <ASIC.Transaction.No-reply@asic-gov-au.co>

Subject **Renewal** 09:00

To [redacted].com.au

ASIC
Australian Securities & Investments Commission

Please find information in the following link regarding the renewal for your company.

Renewal letter

Select this link to view, save or print the information. This link will remain active for 30 days.

If you no longer need your business name to be registered, please email us at **bncancel@asic.gov.au** and include:

- your business name;
- your name and telephone number (including area code).

If you have any questions, contact us at www.asic.gov.au/question

Regards,

Max Morgan
Senior Executive Leader
Registry
Australian Securities and Investments Commission

Please consider the environment before printing this document

Information collected by ASIC may contain personal information. Please refer to our Privacy policy http://www.asic.gov.au/privacy for information about how we handle your personal information, your rights to seek access to and correct personal information, and how to complain about breaches of your privacy by ASIC.

This phishing campaign has been targeting Australian businesses in early 2017 and for short periods of time will direct victims to pages that download malicious software onto their device. ASIC published a warning about the scam in January.

Source: Twitter

Horizon Scan

Upcoming events of interest

2017 April 4 Melb

2017 April 6 Sydney

Cybercrime Masterclass

Commonwealth Bank Fellow and Director of the Human Cyber Criminal Project at Oxford University, Jonathan Lusthaus, joins CBA's cybercrime team for a half-day masterclass in strategies to disrupt cybercrime.
Audience: Law enforcement, academics, fraud and cyber risk teams.

2017 July 3-4 Melb

2017 July 6 Sydney

Malware Reverse Engineering Conference (Melbourne) and Malware Reverse Engineering Workshop (Sydney)

SecEDU, a partnership between University of New South Wales and Commonwealth Bank, will sponsor the fifth annual Malware and Reverse Engineering Conference in Melbourne on July 3 and 4, 2017. In concert with the organisers of the conference at Federation University, we will also bring two of the keynote speakers to Sydney for a half-day technical workshop the following week.

2017 May 23-26 Gold Coast

AusCERT2017 Conference

Brett Winterford, Senior Manager of Outreach and Research at Commonwealth Bank, will present a session on security awareness at Australia's largest and oldest information security conference.

Footnotes

i: https://en.wikipedia.org/wiki/Sony_Pictures_hack
ii: http://money.cnn.com/2015/08/05/technology/aramco-hack/
iii: https://www.bloomberg.com/news/articles/2016-12-01/destructive-hacks-strike-saudi-arabia-posing-challenge-to-trump
iv: https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html
v: https://www.eset.com/us/about/newsroom/press-releases/destructive-killdisk-malware-encrypts-linux-machines-eset-reseachers-discover/
vi: https://securelist.com/files/2017/03/Report_Shamoon_StoneDrill_final.pdf
vii: http://researchcenter.paloaltonetworks.com/2017/01/unit42-second-wave-shamoon-2-attacks-identified/
viii: https://info.phishlabs.com/2017-phishing-trends-and-intelligence-report-pti
ix: https://www.facebook.com/notes/facebook-bug-bounty/facebook-bug-bounty-5-million-paid-in-5-years/1419385021409053/
x: https://securelist.com/analysis/kaspersky-security-bulletin/76757/kaspersky-security-bulletin-2016-story-of-the-year/
xi: http://info.digitalshadows.com/rs/457-XEY-671/images/IntheBusinessofExploitationReport.pdf
xii: https://www.oaic.gov.au/privacy-law/enforceable-undertakings/singtel-optus-enforceable-undertaking
xiii: http://www.politico.com/tipsheets/morning-cybersecurity/2017/03/russia-probe-takes-another-divisive-turn-219382
xiv: http://thehill.com/policy/cybersecurity/324238-trumps-budget-proposal-gives-dhs-15-billion-for-cybersecurity
xv: http://www.nextgov.com/cybersecurity/2017/03/trump-team-floating-cyber-executive-order-industry/135929/
xvi: https://www.itnews.com.au/news/smart-tv-vendor-penalised-for-massive-privacy-violation-450210
xvii: https://krebsonsecurity.com/2016/10/iot-device-maker-vows-product-recall-legal-action-against-western-accusers/
xviii: https://www.cyberscoop.com/hacking-back-bill-tom-graves-active-cyber-defense-certainty-act/
xix: http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf
xx: http://sydney.edu.au/engineering/it/courses/info5990/Supplements/Week07_Malware&Security/Supp07-4TJXCaseDetails.pdf
xxi: https://www.cesg.gov.uk/content/files/document_files/Password_guidance_-_simplifying_your_approach_back_cover.pdf
xxii: http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627
xxiii: https://www.justice.gov/opa/pr/four-members-international-computer-hacking-ring-indicted-stealing-gaming-technology-apache
xxiv: http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627
xxv: http://www.computerworld.com/article/2518328/cybercrime-hacking/heartland-breach-expenses-pegged-at--140m----so-far.html
xxvi: http://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203
xxvii: http://fortune.com/2017/03/09/home-depot-data-breach-banks/
xxviii: http://www.latimes.com/business/la-fi-att-data-breach-fcc-settlement-20150408-story.html
xxix: http://www.eugdpr.org/
xxx: https://www.scmagazine.com/adobe-will-pay-nearly-12-million-in-legal-fees-and-5000-per-named-plaintiff-in-class-action-lawsuit/article/534060/
xxxi: http://www.bankinfosecurity.com/linkedin-a-7229
xxxii: http://www.bankinfosecurity.com/global-payments-breach-tab-94-million-a-5415
xxxiii: http://www.irishexaminer.com/business/cyber-attack-victim-firm-loyaltybuild-in-clare-has-18m-loss-379472.html
xxxiv: http://www.itnews.com.au/news/aussie-mining-tech-firm-counts-cost-of-chinese-hacking-405753
xxxv: https://psnsoesettlement.com/english/
xxxvi: http://www.theverge.com/2015/10/20/9574995/sony-pictures-hack-settlement-employees
xxxvii: https://www.aspi.org.au/publications/special-report-enter-the-cyber-dragon-understanding-chinese-intelligence-agencies-cyber-capabilities/10_42_31_AM_SR50_chinese_cyber.pdf
xxxviii: https://www.forbes.com/sites/greatspeculations/2014/05/08/targets-ceo-steps-down-following-the-massive-data-breach-and-canadian-debacle/#3cedc0432ba6
xxxix: https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach
xl: http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5747
xli: https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches
xlii: http://www.dwt.com/statedatabreachstatutes/
xliii: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/
xliv: https://www.acorn.gov.au/
xlv: https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet