ASB

Signals

Quarterly security assessment

› Q4 2017

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.

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

Contents

Cyber Security:

Trends and Observations

Key trends observed during the quarter

Hardware bugs to plague computing for a generation

The security research community has turned its attention to how processors, memory and other hardware-based mechanisms can be abused to dramatic effect. Two CPU-based flaws disclosed in January 2018 have caused consternation: Meltdown[I] (affecting Intel processors) and Spectre (affecting AMD and ARM processors) attacks exploit performance-enhancing features of modern processors known as "speculative execution" in order to leak information. Meltdown enables an attacker with local access privileges to access memory that should be privileged to the operating system kernel. This 'privilege escalation' could allow one customer in a multi-tenant cloud to access data (including passwords, cryptographic keys, etc.) used by other tenants on the same hardware. Spectre uses additional techniques to trick processors into leaking information both from the OS kernel and from other applications running on the same hardware. It could, for example, expose the cookies or credentials stored in one browser session if the attacker can trick a victim into visit a compromised web site.

CHECKLIST

- These vulnerabilities will have a broad impact. It is not a practical mitigation for generations of hardware to be replaced. Focus on patching.
- Consult with your vendor for instructions on patching operating systems and web browsers.
- Major cloud providers AWS, Azure and Google have introduced fixes for Meltdown attacks, but users may need to also update guest operating systems.
- Patch your operating systems, but only after thorough testing. Be warned that the Windows patch made available January 3 can conflict with some antivirus engines, causing stability issues. An update for MacOS (10.13.2) was released January 8.
- Web browser vendors have removed some exploitable features from their updated browsers and plan to introduce further mitigations in the future. (Mozilla users should update to Firefox 57.0.4 – released January 4) You can also mitigate the risk of data leakage in the browser using features like site isolation in Google's Chrome browser.

SMB protocol an ongoing target for attack

Attackers continue to abuse the SMB protocol to infect vulnerable devices discovered over the internet and neighbouring devices on local networks. SMB (or Server Message Block) is a network protocol which provides machines with access to resources on the local network such as shared file servers and printers. In 2017, hacking group "Shadow Brokers" released exploits that propagated (spread) via abuse of SMB. These exploits ('Eternal Blue' and 'Eternal Romance') were included in several of the most damaging network worms to emerge in 2017 (including WannaCry, [Not]Petya and BadRabbit). At the peak of WannaCry's spread in May 2017, Symantec blocked up to 400,000 attempts by infected systems to exploit systems over SMB each day. Honeypots set up to detect and study these exploits were found to be infected within three minutes of being brought online.

CHECKLIST

- Patch! Ensure Microsoft's MS17-010[II] is installed on your machine to protect from Eternal Blue-based SMB exploits.
- Consider how rapidly your team can respond to the next exploit that targets this and other widely-deployed protocols (consider the open source alternative, SAMBA). Do you actively maintain a register of your organisation's IT assets? Are resources available to assess the severity of a newly discovered vulnerability, or to patch systems expediently?
- Consider network segmentation as a means of containing future infections.

Wireless security under scrutiny

Between late July and October 2017, three long-running security research projects disclosed weaknesses in the security of wireless protocols used to connect mobile devices. In July, a researcher disclosed vulnerabilities[III] in Broadcom WiFi chipsets embedded in iOS and Android smartphones that– if unaddressed – could be exploited to produce the world's first 'WiFi worm' ('Broadpwn'). In September, researchers disclosed several bugs in implementations of the Bluetooth protocol in everything from Windows and Linux devices to Android and iOS handsets.These vulnerabilities[IV] (dubbed 'Blueborne') could theoretically allow for attacks 'over-the-air'. In October, researchers published a flaw in the WPA2 handshake performed to establish and secure WiFi connections[V]. Left unaddressed, the 'KRACK' series of bugs could allow for man-in-the-middle attacks against WiFi connections.

CHECKLIST

- This security research hasn't yet resulted in over-the-air WiFi or Bluetooth-enabled worms. Keep your operating systems up-to-date.
- Turn Bluetooth off if you're not using it. Consider disabling it altogether for devices that don't need it.
- Patches were released for all devices vulnerable to Blueborne in mid-September 2017.
- Patches for the Broadpwn vulnerability were released for Android and Apple in July 2017.
- Patches to protect consumer devices against KRACK attacks are available (Windows, Ubuntu, Debian, Android, MacOS, iOS).
- Network administrators need to be more proactive. Download the latest firmware for network devices affected by KRACK. Patches for end-of-life equipment may not be made available and require other workarounds (see updates from enterprise-grade vendors Cisco, Juniper, Netgear, for example).

By the Numbers

1.4 billion
plain-text credentials stolen from past data breaches are circulating online[VI].

14,529
Number of vulnerabilities published in 2017[VII]

US$568 million
Western Union settlement over 'willful' facilitation of online scams[IX].

US$100K
paid by Uber to a 20-yr old hacker to stay mum on data breach[VIII]

Cyber Security:
Trends and Observations

Malware authors target Android

The Android operating system offers developers and users greater flexibility than other mobile platforms. This freedom carries a price. An increasingly fragmented ecosystem leaves older versions unprotected against new vulnerabilities and malware. Malware campaigns routinely target older versions of Android with everything from trojaned apps to mobile ransomware. Google has struggled to keep malicious apps out of the 50 billion+ apps listed in its official Google Play store. In the last quarter, malicious apps discovered in the store included malware designed to steal online banking credentials, SMS, social media credentials and the contents of Bitcoin wallets. It also included droppers (beachheads for download of other malicious software) and apps designed to build a profile on unsuspecting users. Over 1m users downloaded a fake Android app pretending to be WhatsApp. In August, Google removed 500 apps infected with the same spyware (collectively downloaded 100m times).

CHECKLIST

- Don't panic! An ecosystem that includes over 50 billion apps is bound to include more than a few bad apples. Check the publisher of any new app you wish to download – is it an institution you trust?
- Keep your mobile operating system up-to-date. Important new security features were included in the most recent major update to the Android OS (Android 8 or 'Oreo'). Options to enable installation of apps from outside the Google Play store are replaced with permissions that must be applied to individual apps before they can download software from untrusted sources.
- Only download mobile apps from official app stores (Google Play) or from an institution you trust (such as your employer).
- Check which permissions an app will request before download. Are they appropriate for the stated functionality of the app?
- Do not 'jailbreak' or 'root' a device. This removes key operating system measures designed to protect your device from malware.
- Consider switching on Android's rebranded Verify app (now called 'Google Play Protect'), which scans devices for signs of malicious apps previously identified in App stores or on devices.

Domain registrars make juicy targets

A number of serious cyber-attacks continue to stem from redirection of DNS (Domain Name System) records at third party domain registrars. In September 2017, Dutch threat intelligence firm Fox-IT detected unauthorised access to its DNS records by attackers that compromised its account with a third party domain registrar. Attackers were able to access documents Fox-IT clients uploaded to the company via its web portal. This drew parallels with a 2016 attack in which attackers hijacked the domains of a Brazillian bank, redirecting customer traffic to phishing sites that encouraged users to download malware, reportedly for up to six hours. There have also been recent abuses of DNS en masse: In July 2017, an attack on a single French domain registrar redirected traffic from 751 domains (many of which were Australian entities) to websites that hosted exploit kits designed to infect clients with malware.

CHECKLIST

- Protect and limit access to your domain registrar with strong access controls. Use unique, long, complex passphrases.
- Use a registrar that requires multi-factor authentication for access and multiple authorisers to make changes to domain settings.
- Set clear accountability for ongoing renewal of domains in use.
- Proactively monitor for changes to DNS settings (or for imminent expiration of a domain) – see the 2010 paper by ICANN's Security and Stability Committee[XII].
- Consider 'locking' your domain via registry locking to protect against unauthorised changes.

Democratisation of email spoofing tools

New vulnerabilities have been publicly disclosed that demonstrate how attackers can bypass integrity checks made by many email clients. 'Mailsploit' is a collection of bugs found in email clients and Mail Transfer Agents (email servers) that allow attackers to circumvent spoofing protection mechanisms such as DMARC and SPF/DKIM[X]. It is probable that the disclosure – combined with the availability of numerous tools used for crafting of spoofed messages (legitimate and otherwise) make it easier for low-skilled attackers to launch social engineering campaigns such as Email Payment Fraud[XI], under which attackers often 'spoof' the email address of a victim's supplier or senior executive in an attempt to legitimise a fraudulent request for payment.

CHECKLIST

- Check your mail client has been patched against Mailsploit flaws. While over 30 different mail clients were found vulnerable to Mailsploit prior to November 2017, many have since been patched.
- Continue to run integrity checks on your mail server and protect the use of your domain. Check your SPF/DKIM and DMARC settings.
- Assume your domain – and those of your suppliers/ business partners – can be spoofed. Enforce strict staff compliance with payments processes, ensuring clear separation of duties. Large or unexpected payments should not be made on the basis of an email without additional verification.
- Ensure staff with the authority to make large transactions have completed security awareness training.

By the Numbers

Over **NZ$1.1 million** in direct financial loss due to cyber incidents was reported to CERT NZ in Q3 2017.[XIV]

1m downloads of a fake WhatsApp app in the Google Play store before it was removed[XV]

Over **NZ$300K** was lost by a single company to a scammer impersonating a supplier in Q3.[XIII]

Deep Dive:

Six principles of a strong cyber security response

The good oil on giving bad news

Arjun Ramachandran
Executive Manager, Cyber Outreach

The slogan "it's not a question of if, but when you get breached" comes in for heavy use in cyber security circles. The key take-away is not necessarily that security incidents are inevitable, more so that we need to be prepared to respond.

Many countries, including our Australian neighbours, have enacted data breach disclosure laws that require companies by law to report to regulators and affected shareholders any data breach that poses a risk of serious harm to citizens. In countries with these laws, a much higher number of cyber security incidents have been disclosed to the public. Affected organisations are judged as much on the effectiveness of their response as on the severity of the events. Whether the country you're in has data breach disclosure laws or not, having a plan for "when you get breached" and not "if you get breached" can make a huge difference to an event's severity.

Provided on Page 5 is a list of six principles that we espouse as key to a sound public response: Empathy, Accountability, Responsiveness, Accuracy, Transparency and Competence.

Understanding cyber security incidents

The first step towards an effective public response is to recognise that cyber security incidents have inherent characteristics that differentiate them from other events:

The need for speed – As news stories go, those about cyber-attacks inherently carry a sense of urgency and sensationalism. Agility is thus a key hallmark of an effective response. It requires a well-rehearsed playbook for incident response – covering both your technical capability (detection and post-incident forensics) and your broader organisational response (communications, etc.)

Diverse stakeholders – While cyber security is ostensibly a technical domain, security incidents impact a broad set of stakeholders across the community. Data breaches ultimately affect individuals, often in a deeply personal way. At the same time, large cyber security incidents can invoke regulatory concerns and even geopolitics. A breached organisation may need to respond to competing demands from law enforcement, intelligence services and multiple regulators.

An influential technical community – Cyber security remains a specialist technical field about which a vocal community of experts and researchers actively publish and commentate. This community invariably sets the agenda for mainstream news coverage following an incident. Organisations are held to a high standard by this community, particularly in relation to the level of detail and technical accuracy of any public response. Faced with contradictions or speculative responses, this community often has the means to uncover details of a breach via third parties.

> "The first step towards an effective public response is to recognise that cyber security incidents have inherent characteristics that differentiate them from other events"

Information asymmetry – Whether your breached data has been posted on a public website, security vulnerabilities have been found in your products by an external researcher, or third-party scanning tools have exposed your lax security posture – you're not always in full command of information about cyber security incidents that impact your organisation. In many cases, external parties may know more than you about the key details. In the wake of this asymmetry, conventional and defensive PR approaches of presenting a small target (saying "no comment", or issuing statements that are vague and limited) are ill-advised. They can leave your organisation looking disconnected and cede the public narrative to external parties.

Principles of a good cyber security response

An effective public response to a security incident is critical to preserving – and potentially even enhancing – trust in an organisation's brand. The National Institute of Standards and Technology's globally recognised Cybersecurity Framework[XVI] accordingly identifies "response" and "recovery" as core functions of a cyber security program (alongside "identify", "protect" and "detect"). In particular, the framework highlights the critical role communications play in preparedness and response, outlining the steps required to preserve reputation.

Recognising the inherent characteristics of cyber security incidents, and building on our own experiences and analyses of public responses, we've outlined six key principles of a strong response to a cyber security incident below.

Deep Dive:

Six principles of a strong cyber security response

1 Empathy

Unauthorised disclosure of personal information is deeply upsetting for victims. The guiding principle for any response must be to understand the harm caused for your customers or staff, and to respond with empathy and caring. In a practical sense, adopting this principle will result in public messages that show genuine expressions of contrition, outline specific actions you're taking to minimise further customer harm, and provide reassurances about likely customer fears. An empathetic approach prevents overly legalistic responses – a characteristic of poor responses that incenses customers and earns the ire of the media.

"I want to personally apologise to each of you for what has happened, as I know you expect us to protect your information."

- Joseph R Swedish, CEO and President, Anthem
(Response to 2015 data breach)

"We have complied with all of our legal obligations."

– Dido Harding, CEO, TalkTalk
(Response to 2016 data breach[xvii] resulted in the loss of 100,000 customers and a record £400,000 fine).

2 Accountability

Security incidents that affect your organisation may not be entirely your fault. Of the top 100 breaches of the last decade, almost one-third involved compromise of a third party of the organisation. Under public pressure, the temptation to point the finger at others is strong. However, the shortest path for an organisation to restore trust in the wake of an incident is to accept full responsibility. This provides the strongest indication that you are going to do what is required in the future to protect customers.

"We take full responsibility and I assure the public we are doing everything in our power to not only right this but to prevent it from happening again."

– Shelly Park, CEO, Red Cross Blood Service.
(Response to 2016 incident[xviii] in which a contractor/web developer left a backup file exposed on the public internet).

"Overwhelmingly the failure was IBM's, they've acknowledged that, they've paid up, they've accepted the blame. And they should have."[xix]

- In response to a three-day outage of the online systems running the 2016 Australia Census.

3 Responsiveness

Organisations deemed to have mishandled public responses to a data breach often draw ire for taking too long to inform customers and the broader public. Organisations such as Hilton Hotels (2015), Equifax (2017) and Uber (2017) have been roundly criticised for delaying the disclosure of a security incident. However, responsiveness is broader than notification and public disclosure, and must reflect a general sense of urgency to minimise customer harm. This can include taking (and announcing) measures such as immediate password resets or publishing portals where customers can learn if they are affected and where to get help.

"We have directly contacted all guests for whom we have appropriate contact information that checked in to an affected hotel during the at-risk dates."

- Chuck Floyd, Global President of Operations, Hyatt Hotels
(Response to a 2017 breach[xx]).

"You may be asking why we are just talking about this now, a year later."

Dara Khosrowshahi, CEO, Uber, 2017
(Response to a 2016 breach[xxi] which was not disclosed for over 12 months).

4 Accuracy

Notwithstanding the need for speed, responses that are fast but incorrect will ultimately wound trust. When facing pressure to respond publicly, avoid the temptation to speculate about impact, scope or root cause before all facts are known. Our analysis suggests that the best course of action when public disclosure is deemed necessary is to focus on customer concerns in any initial statement that acknowledges an incident, along with a commitment to issuing regular updates as facts are verified.

"The company's IT security team has been working around the clock with IT security firms, its banking partners and the Secret Service to rapidly gather facts, resolve the problem and provide information to customers. The company's ongoing investigation has determined the following..."

- Updated response to 2014 breach at Home Depot[xxxiii]

"On October 2, 2017, Equifax announced that additional consumers may have been impacted. To minimise confusion, Equifax will mail written notices to all of the additional potentially impacted U.S. consumers identified since the September 7 announcement."

- Updated response to 2017 Equifax breach[xxxvi]

5 Transparency

As we've already outlined, information about a security incident often sits outside the organisation. As such, statements that are vague, use 'legalese' or seek to obscure can be quickly determined by this community as inadequate in light of known facts observable from outside your organisation. Obvious attempts to limit future damages will only exacerbate the problem. Transparency offers a preferable path.

"We believe that transparency builds more trust than secrecy and there are lessons to be learned, both good and bad, that we want to share."

- Erik de Jong & Frank Groenewegen, Fox-IT
(Response to 2017 security incident impacting clients of security vendor Fox-IT)[xxii]

"It is troubling that Equifax is forcing people to waive legal rights in order to receive fraud monitoring after the company's breach put their personal information at risk."

- Statement[xxiii] by the US Consumer Financial Protection Bureau (on the terms and conditions applicable to the free credit monitoring offered by Equifax after its 2017 breach).

6 Competence

Security incidents are often viewed solely as media stories that need to be managed. Equally, once an incident is disclosed and publicly known, media stories provide the opportunity to rebuild trust by demonstrating your competence. Providing detail about how the incident occurred (with due sensitivity to any ongoing investigations), and the steps your security teams are taking in response will engender confidence. Disclosing more detail can allow you to shape the public narrative - an important consideration given cyber security incidents are often first disclosed by an external party, placing your organisation in a reactive PR situation. For these reasons, while statements about an incident are best made by your senior-most leaders, consider making your Chief Information Security Officer or other subject matter experts available for media comment to reflect security expertise in media coverage. Also be aware that contradictory statements or incorrect terminology will undermine trust and confidence.

"We detected and addressed the breach, limiting the total effective MitM (Man-in-the-middle) time to 10 hours and 24 minutes."

- Erik de Jong & Frank Groenewegen, Fox-IT
(Responding to 2017 domain hijacking attack against Fox-IT's DNS registrar[xxiv])

"TalkTalk suffered a 'sequential attack'"

– Dido Harding, CEO, TalkTalk, attempting to describe a SQL Injection attack.
(Response to 2016 data breach[xxiv] resulted in the loss of 100,000 customers and a record £400,000 fine).

Deep Dive:

Six principles of a strong cyber security response

Brett Winterford
Senior Manager, Cyber Outreach and Research

Markets hate uncertainty

Mandatory data breach disclosure has been enforced in some jurisdictions for well over a decade. Customers, investors, regulators and other stakeholders have developed a sharp sense for what an effective response to a breach looks like. Failure to meet a minimum standard tends to result in negative media and social media commentary. But does any of this impact investor confidence in a company?

The case studies illustrate that the quality of an organisation's response to a data breach has as much bearing on share prices as the magnitude of what was stolen or exposed.

Case studies: Hilton and Hyatt

Between 2013 and 2015, a large number of hotel groups were targeted by profit-motivated criminals that used malware to scrape transaction details from point-of-sale devices. Breaches at Hilton Hotels, Hyatt Hotels, Intercontinental Group, Mandarin Oriental, Trump Hotels, White Lodgings and Wyndham Hotels and others shared many characteristics and were in some cases attributed to the same threat actors.

HILTON HOTELS

Investigative journalist Brian Krebs first raised suspicions about a breach at Hilton Hotels on September 25, 2015, based on feedback from card schemes and US banks. The company did not respond and its share price dropped 4.5% in a single day.

Hilton Hotels did not acknowledge the breach until November 24, 2015 – some two months later. Even then, Hilton's published statement omitted any details about which of its hotel outlets had been affected. It was assumed, on this basis, that the organisation either didn't have the visibility or capability to fully understand the scope of the breach, or intended to play it down. This uncertainty drove Hilton's share price down a further 29% over the next two months. It took a further nine months to recover to the (average) price of the stock in the 100 days prior to disclosure of the breach.

In November 2017, Hilton Hotels paid US$700k in fines and admitted to New York Attorney General Eric Schneiderman that it knew of the first of two breach events for over nine months before it disclosed to the public, and knew of a second breach for more than three months before disclosure.

In a statement filed after its investigation, the Attorney General said the hotel group was fined because it "did not provide consumers with timely notice and did not maintain reasonable data security."[xxv]

HYATT HOTELS

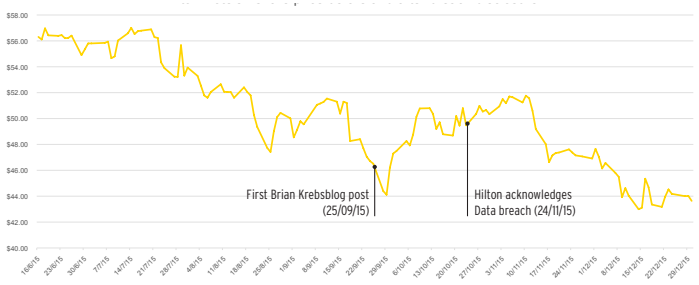
Hyatt Hotels notified customers of a data breach on December 23, 2015. With the lessons from Hilton Hotels' response fresh in the memory of the hospitality industry, Hyatt published a microsite (/protectingourcustomers) about the breach three days later, promising to disclose more information once investigations were complete. Hyatt customers, like those that stayed at Hilton Hotels, were asked to check their credit card statements for anomalies, and investors were again unsure of the scope of the breach. Hyatt stock dropped steadily over the holiday period (by 25% in just two weeks). Around three weeks later, Hilton updated its microsite with further details, including:

- The "at-risk" window in which attackers were present on systems;
- What systems were affected (point-of-sale systems at hotel restaurants) at what hotels (searchable by country);
- Details about precisely what type of information was stolen;
- Advice for affected customers.

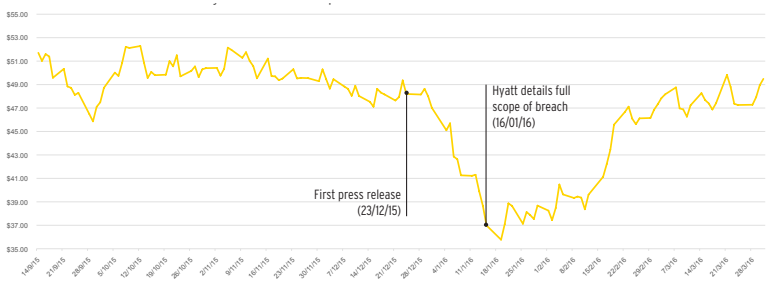
With these details available – and the company living up to its promise of transparency, customers, investors and other stakeholders were able to more accurately gauge the impact of the event. Hyatt's stock price leaped 38% in the 10 weeks from this more detailed disclosure to the end of March 2016 and has not stopped rising since.

This dual display of patience and transparency continues to pay dividends. The hotel group used the same web site to disclose details of a further breach on October 12, 2017[xxvi], after which its share price has suffered little noticeable impact.

Hilton Hotels - share price before and after breach disclosure



Hyatt Hotels - share price before and after breach disclosure



Deep Dive:

Six principles of a strong cyber security response

Case studies: Target and Home Depot

Between 2013 and 2015, US retailers were also targeted by profit-motivated criminals that used malware to scrape transaction details from point-of-sale devices. The resulting breaches shared multiple characteristics and some were attributed to the same actors.

The events impacting Target and Home Depot, specifically, were both disclosed by banks and/or card schemes to an investigative journalist (Brian Krebs) before the affected retailers confirmed them to the public. They were likely targeted by the same actor group using very similar malware. The starkest distinction between the two events was how the two companies responded.

TARGET

Target was notified by the US Department of Justice on December 12, 2013 that attackers had been present on its network for close to a month. By December 18 (six days later), a media story had broken on the breach[XXVII] – which was confirmed by Target the following day. The retailer's initial estimate of impact (40m cardholders) had to be revised on January 10, 2014, to include personally identifiable data on a total of 70m customers[XXVIII]. This update had the most significant impact on Target's share price. In the fortnight following the initial (40m) disclosure, the share price dropped by a sizeable 3.8%. By comparison, it fell by over double that amount (7.8%) in the fortnight following the revised (70m) disclosure.

By March Target's CIO had resigned. By May, its CEO was ousted. The company has since reported close to US$200 million in breach related expenses[XXIX].

HOME DEPOT

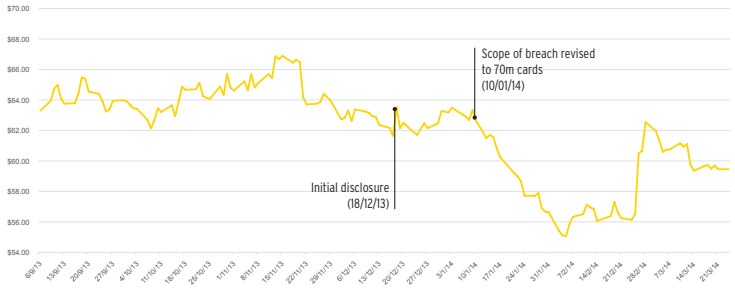
Like Target, news of a data breach at Home Depot emerged before the company had disclosed the incident. Home Depot's share price dropped by 2 percent within a day of Brian Krebs' September 2, 2014 story reporting suspicious activity on cards used at Home Depot outlets[XXX]. The company's share price had otherwise been growing steadily. Over the next six days, Krebs wrote two further articles detailing what malware had been used in the breach and which actors were responsible. Home Depot confirmed the breach on September 8, 2014, resulting in a further 2% hit on its share price.

Despite the significant scale of the impact (50m+ email addresses and 40m+ credit card details), Home Depot's share price regained what it had lost within 9 days of the first disclosure, and gained further following a second disclosure that expanded on known details about the breach on September 18, 2014. This second disclosure informed the market of several steps Home Depot would now take to ensure it can be confident in its security posture[XXXI].

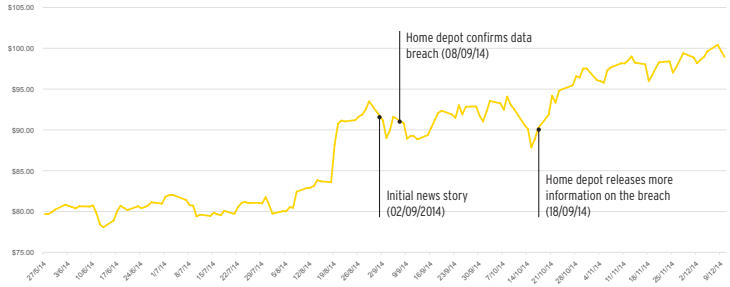
Home Depot suffered similar breach-related expenses as Target, has had to pay compensation to card schemes and affected customers and had the benefit of several months to analyse the impact and response to Target's data breach. But it felt less of an impact. While the upward trajectory of Home Depot's share price was likely due to other factors, investors were evidently reassured by the company's orderly, accurate and timely release of information about the breach.

> "Investors were evidently reassured by the company's orderly, accurate and timely release of information"

Target - share price before and after breach disclosure



Home Depot - share price before and after breach disclosure



Deep Dive:

Six principles of a strong cyber security response

> “Anthem provided stakeholders a rapid and effective response to the breach once it was discovered”

Case studies: Anthem and Equifax

Data breaches at US health insurer Anthem (2015) and credit bureau Equifax (2017) affected tens of millions of customers. Both disclosed the breach prior to media coverage – but where one took little over a week to do so, the other took many months. And while both published a web site for affected customers and made ongoing edits to their version of events, Anthem's earnest attempts to adhere to the principles outlined above enabled it to set the news agenda, while the latter was made to respond to it.

ANTHEM

For a company that suffered one of the longest and most impactful data breaches in history, health insurer Anthem is held in some quarters as a good example of response to a data breach.

After discovering suspicious activity on its network on January 27, 2015, Anthem quickly informed US law enforcement and hired private sector incident response specialists. It announced the breach via its own web site on February 4, 2015 via a bespoke web site (http://www.anthemfacts.com)[xxxii]. The web site featured an apology from CEO Joseph Swedish (demonstrating empathy) and was supported by a Frequently Asked Questions page outlining what the insurer knew at the time (demonstrating transparency).

When the breach was announced, news outlets were offered supportive email statements by the FBI that spoke to Anthem's responsiveness: “Anthem's initial response in promptly notifying the FBI after observing suspicious network activity is a model for other companies and organizations facing similar circumstances. Speed matters when notifying law enforcement of an intrusion,” an FBI spokesperson offered the New York Times[xxxiii]. This helped to shape the narrative around the breach from this point on.

Anthem's microsite was continually updated as facts were confirmed: first with details about the impact on other insurers that used Anthem services, then with warnings about phishing emails (Feb 7) and phone scams (Feb 12) targeting affected customers. The site was overhauled February 17 to inform customers how to access “Identity Theft Repair” and credit monitoring services made available by the company.

Like many other breached entities, Anthem stock fell 2% lower within the first three days of initial disclosure, but regained those losses within a week. Anthem's first response did not specify how many clients were affected, beyond saying that the breach affected “all product lines”. The insurer had 37.5m active customers at the time – and media commentary led with this figure until Anthem updated its microsite on February 17 to state that both current and former customers (from the last 10 years) were affected. By February 24, 2015, this led to news that the number of victims was closer to 78.8 million. While Anthem stock took a short-term hit of close to two percent over the three weeks following the second wave of stories, it remained above the pre-breach price for this entire period.

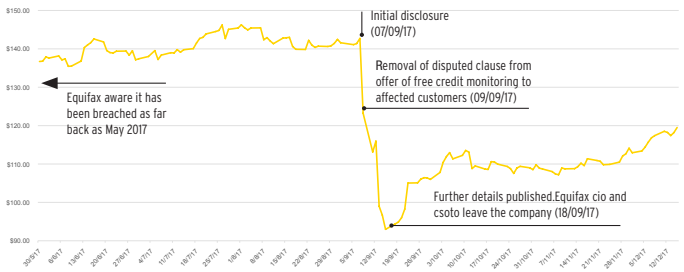
In January 2017, California's Department of Insurance announced that an independent security audit had confidently attributed attacks on Anthem to nation-state aligned actors. Anthem, it said, provided stakeholders a “rapid and effective response to the breach once it was discovered”. Despite incurring breach-related expenses of close to US$260 million, Anthem's stock outperformed its industry peers and continues to climb.

EQUIFAX

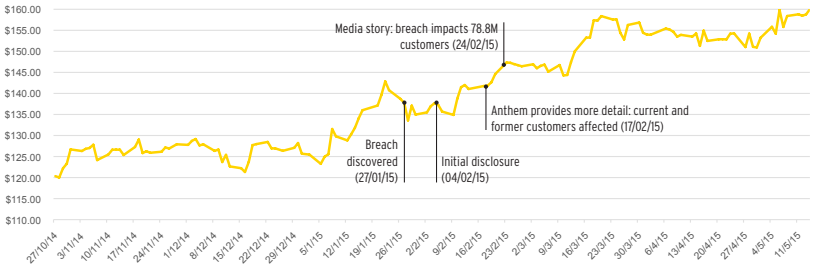
The 2017 data breach affecting 143 million customers of credit bureau Equifax is widely cited among the less ideal responses to security incidents. Equifax took 78 days to notice it had suffered a breach event, and 117 days to notify the public. Upon disclosure of the breach on September 7, 2017 – again via a micro-site[xxxiv] (https://www.equifaxsecurity2017.com), the company was accused of trying to dupe victims into accepting an offer of free credit monitoring that included a clause designed to limit their right to sue the company. Equifax removed the clause within two days after New York Attorney General Eric Schneiderman described the terms of service as “unacceptable and unenforceable”.[xxxv]

The company's share price dropped by over 13% on the day of the breach, and dropped by a whopping 33% within a fortnight of the disclosure. Further losses were only stemmed by a clarifying statement released on September 18 under which Equifax announced the replacing of the company's CIO and CSO (demonstrating accountability) and produced a timeline of the events leading up to the initial disclosure (demonstrating transparency).

Equifax - share price before and after breach disclosure



Anthem - share price before and after breach disclosure



Incident Report

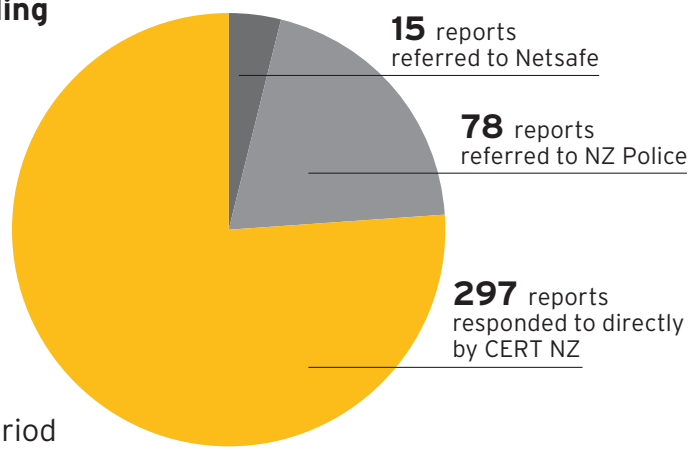
CERT NZ's cyber security incident statistics from around the country[xiv]

certnz

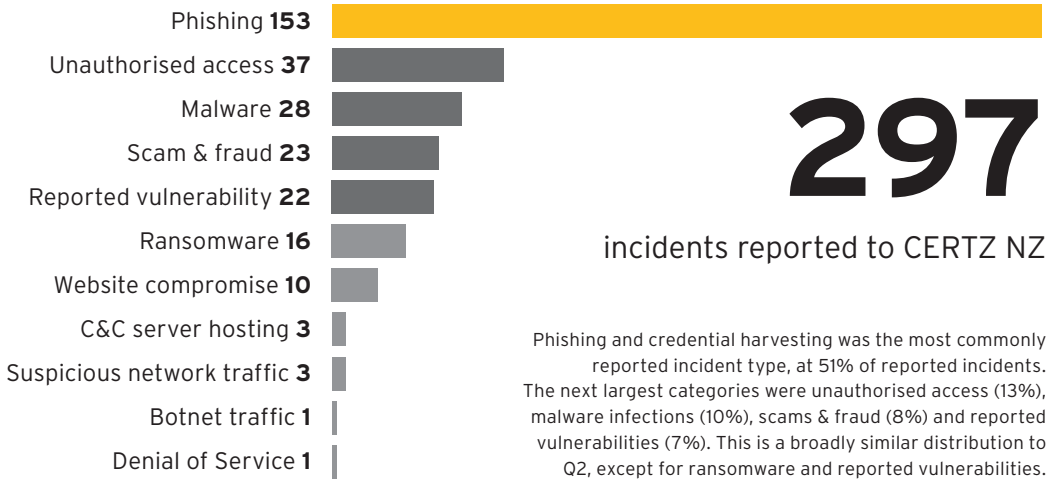
Breakdown by responding organisation

390

incident reports received for the 1 July – 30 September 2017 period



Breakdown by category: Incidents CERT NZ responded to directly

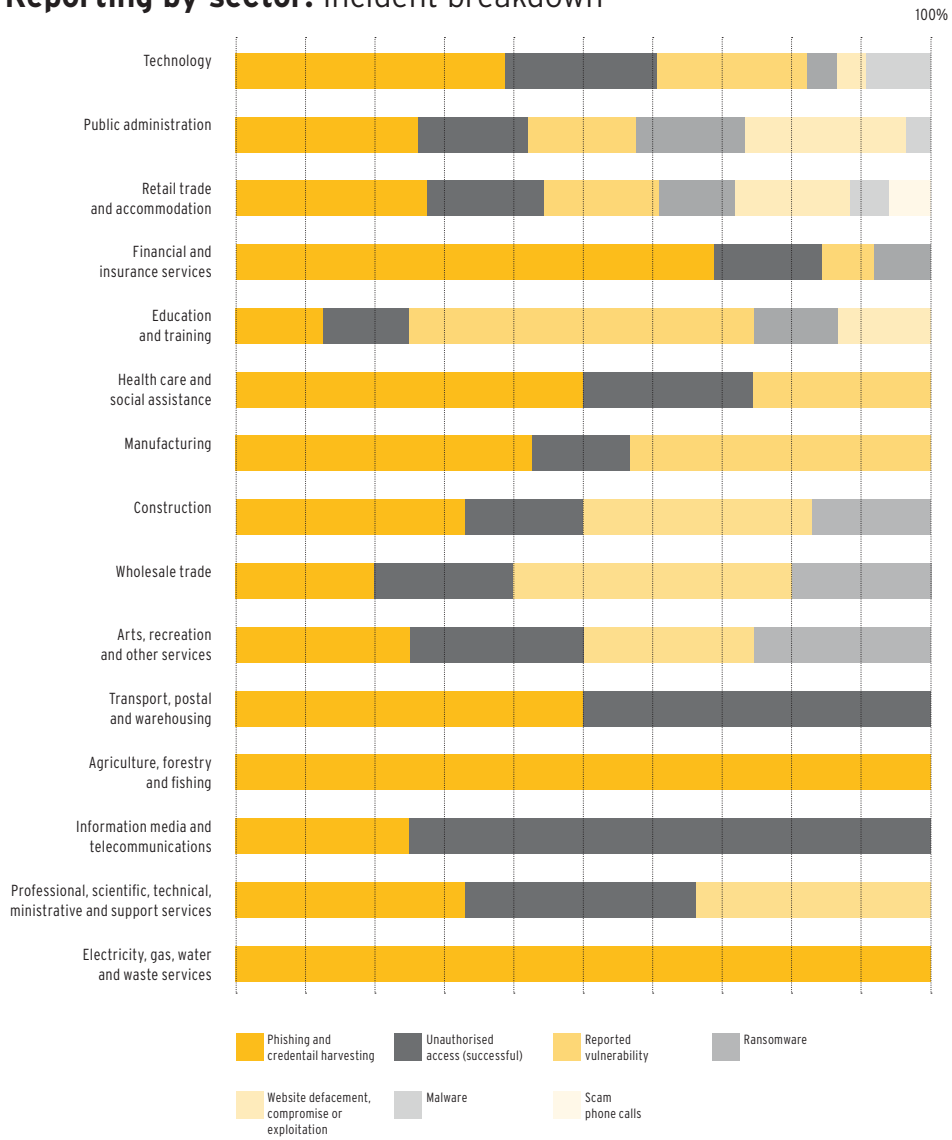


297

incidents reported to CERTZ NZ

Phishing and credential harvesting was the most commonly reported incident type, at 51% of reported incidents. The next largest categories were unauthorised access (13%), malware infections (10%), scams & fraud (8%) and reported vulnerabilities (7%). This is a broadly similar distribution to Q2, except for ransomware and reported vulnerabilities.

Reporting by sector: Incident breakdown



Better Practice

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

> “It is unsustainable to assume password complexity can keep up with the computational power available”

CERTNZ’s critical controls 2018

For: *CISOs, cyber security strategy teams, system administrators, solution architects, and Security professionals*

CERTNZ has recently released its ten critical controls list [https://www.cert.govt.nz/it-specialists/guides/10-critical-controls/] that are designed to mitigate the majority of attacks they have analysed to date. The controls list will be updated on an annual basis. CERTNZ advises that this is not a complete list and those usual best practices, such as maintaining an effective password policy and firewall configuration, are followed.

Squash those bugs

For: *Software development teams, solution architects.*

Volunteers at the Open Web Application Security Project (OWASP) have published the definitive list of the 2017 ‘Top 10 web application vulnerabilities’. OWASP’s Top 10 list[XXXVI], compiled from data sourced from over 40 security firms and a survey of 500 members, is updated every 2-3 years.

What’s changed? The new OWASP Top 10 includes ‘Insecure Deserialisation’[XXXVII], which covers vulnerabilities created when deserialising data based on untrusted user input. It also includes ‘Insufficient Logging and Monitoring’[XXXVIII] – key to detection of common attacks against web applications. To make way for these two items, several attacks were summarised as “Broken Access Control”[XXXIX] and Cross Site Request Forgery (CSRF) was removed altogether – recognising that most software development today uses development frameworks with built-in defences against CSRF.

New requirements for PCI compliance

For: *Compliance managers, software development teams, solution architects at any organisation that stores, processes or transmits credit card data.*

As of June 30, 2018, the minimum encryption protocol required for compliance with the PCI data security standard will be TLS 1.1[XL].

What’s changed? Serious vulnerabilities have been found in earlier versions of the SSL/TLS protocols that cannot be fixed with a patch. The PCI Council recommends organisations update to TLS 1.2, and to actively patch TLS software (such as OpenSSL) against new vulnerabilities that emerge.

Avoid bugs in the first place

For: *Software development teams, solution architects.*

The UK National Cyber Security Centre now provides high-level advice on secure development practices[XLI]. The advice is broken up into eight considerations, each with some ‘self-assessment’ questions for benchmarking the maturity of your development practices

.

Passwords are dead?

For: *System administrators, solution architects, Identity and Access Management specialists, Security Awareness professionals*

The Australian Signals Directorate has published guidance on password/credential management[XLII] that all but accepts defeat on convincing users to create unique, long and complex passwords for every online service they use. It is “unsustainable”, the ASD says, to assume password complexity can keep up with the computational power available to crack hashed passwords stolen in data breaches. With that in mind, the ASD recommends adoption of multi-factor authentication[XLIII]. Stay tuned to the next issue of Signals for our analysis of research papers that support the ASD’s thinking.

Updated NIST Cyber Security Framework

For: *CISOs and cyber security strategy teams*

A draft update of the NIST Cyber Security Framework has been published[XLIV]. The Framework is often used as a planning tool basis for large organisations to manage cyber security risk.

What’s changed? Among the changes, the framework is placing greater emphasis on (a) measuring cyber risk, (b) supply chain risks and (c) coordinated vulnerability disclosure.

Phish Eyes

Recent phishing lures for your security awareness teams. Report phishing emails to phishing@asb.co.nz

> “In Q4 2017, our security analysts responded to malware campaigns that utilise macros at a rate of more than one a day”

When teaching users how to detect malicious emails, typically they are warned to be cautious when interacting with emails from untrusted sources that contain:

- **Attachments** (especially executables, .zips and macro-enabled Office files (.doc, .xls et al) that seem out of context.
- **Web links** in the body of the email that direct the user to an untrusted web site.

Defending against macro-based attacks

- Survey users on use of embedded macros to inform your policy. If there isn't a strong business need for users to run Macros within their documents, system administrators can choose to disable Macros by default (with or without notification).
- A more pragmatic approach is for system administrators to digitally-sign (and whitelist) macros they trust (such as those developed by the organisation or its business partners), blocking all others by default.
- In most of the above scenarios, users nonetheless have the option to ignore security warnings by choosing to 'enable content' in an Office document they open. User education about how Macros are abused in email-borne malware campaigns is key.
- From Office 2016, Microsoft offers a 'Protected Mode' under which users can view the contents of a document that contains Macros on opening before choosing to enable the Macros. While it doesn't negate the need for user education, this feature gives users more information and context upon which to decide whether to enable the program embedded in the document to run.

The majority of email-borne attacks intercepted over the last 12-18 months made use of file attachments, and the majority of these campaigns asked the user to enable macros within an attached Microsoft Office document. (As an aside – the next most popular form of attack embedded JavaScript files within .zip files that were attached or linked to the email).

In Q4 2017, bank security analysts responded to malware campaigns that utilise macros at a rate of more than one a day. Macros remain the primary means by which malicious software such as downloaders and trojans are implanted on user devices.

MACRO-LESS CAMPAIGNS

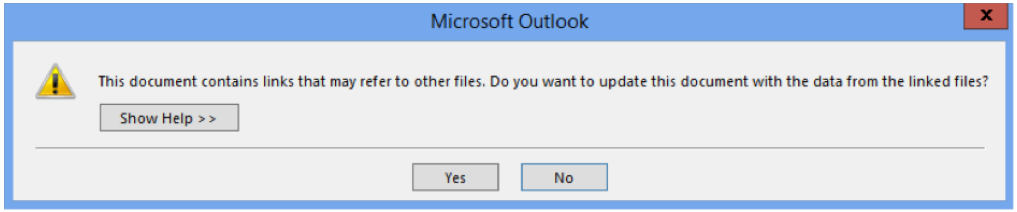
For a brief period in October 2017, some of the world's most notorious cybercriminal groups switched tactics.

Rather than sending victims file attachments that relied on embedded macros to execute code on the user's device, they experimented with abusing other native features of Microsoft software – specifically those that provide an ability to share and update data between multiple applications. Traditionally, tasks like mail merge, which links data between Microsoft Outlook and Microsoft Office files, relied on a protocol called Dynamic Data Exchange (DDE). More recent versions of Microsoft products rely on a new technology called Object Linking and Embedding.

In late 2017, security researchers (initially) and cybercriminal gangs (shortly afterwards) began experimenting with attacks that abuse the Dynamic Data Exchange (DDE) protocol to trick users into running the attacker's code on their device. In mid-late October, we briefly saw the number of campaigns using this new technique outstrip those abusing macros.

HOW THE DDE ATTACK WORKS

In the attacks we've intercepted that use DDE as an infection vector, the user is sent an email with a Word document attached. Upon opening the word file, the user is presented with the first of (usually several) Windows popup messages. The first popup looks like this:



If the user clicks 'Yes' to continue on both this pop-up and subsequent pop-up messages, they are effectively allowing the attacker's (linked DDE) code to be executed locally on the machine.

For its part, Microsoft argued that this is not a vulnerability in its software – the attack abuses a feature that otherwise provides users productivity gains. Nonetheless, the publishing of detailed blogs and social media posts in October 2017 on how the feature could be abused spurred a series of attacks – some by known criminal groups. These attacks – and ongoing pressure from large Microsoft clients – convinced Redmond to offer mechanisms by which system administrators could protect users from these forms of attack.

Until older versions of Microsoft Office (and other Microsoft software) are phased out, security awareness professionals must consider whether to include attacks that rely on abuse of linked data between files (using either of DDE or OLE) in education campaigns around safe handling of file attachments.

Defending against DDE attacks

- Test and deploy the workarounds released by Microsoft[XLV].
- Educate users to look out for the system warnings generated during a DDE attack (as above).
- NVISO Labs have published YARA rules for detection of DDE attacks.

Endnotes

I https://meltdownattack.com/
II https://support.microsoft.com/en-au/help/4023262/how-to-verify-that-ms17-010-is-installed
III https://blog.exodusintel.com/2017/07/26/broadpwn/
IV https://www.armis.com/blueborne/
V https://www.krackattacks.com/
VI https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14
VII https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time
VIII https://www.reuters.com/article/us-uber-cyber-payment-exclusive/exclusive-uber-paid-20-year-old-florida-man-to-keep-data-breach-secret-sources-idUSKBN1E101C
IX https://www.ftc.gov/enforcement/cases-proceedings/refunds/western-union-settlement-faqs
X https://www.mailsploit.com/index
XI https://www.commbank.com.au/content/dam/commbank/assets/business/can/business-insights/signals/commbank-signals-q4-2016.pdf
XII https://www.icann.org/en/system/files/files/sac-044-en.pdf
XIII https://www.cert.govt.nz/about/quarterly-report/q3-report/
XIV https://www.cert.govt.nz/about/quarterly-report/q3-report/
XV https://motherboard.vice.com/en_us/article/evbakk/fake-whatsapp-android-app-1-million-downloads
XVI https://www.nist.gov/cybersecurity-framework
XVII https://www.thetimes.co.uk/article/talktalk-hit-by-customer-backlash-k2ws0vvqfx6
XVIII http://www.donateblood.com.au/media/news/blood-service-apologises-donor-data-leak
XIX https://www.itnews.com.au/news/ibm-paid-very-substantial-compensation-for-census-failure-442563
XX https://www.hyatt.com/notice/protectingourcustomers/
XXI https://www.uber.com/en-AU/newsroom/2016-data-incident/
XXII https://www.fox-it.com/en/insights/blogs/blog/fox-hit-cyber-attack/
XXIII https://www.cnbc.com/2017/09/08/were-you-affected-by-the-equifax-data-breach-one-click-could-cost-you-your-rights-in-court.html
XXIV http://www.ft.com/cms/s/0/d17f77ee-7b0e-11e5-a1fe-567b37f80b64.html
XXV https://ag.ny.gov/press-release/ag-schneiderman-announces-700000-joint-settlement-hilton-after-data-breach-exposed
XXVI https://www.hyatt.com/notice/protectingourcustomers/
XXVII https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/
XXVIII https://corporate.target.com/press/releases/2014/01/target-provides-update-on-data-breach-and-financia#?v=1B16TW011014
XXIX https://www.reuters.com/article/us-target-cyber-settlement/target-in-18-5-million-multi-state-settlement-over-data-breach-idUSKBN18J2GH
XXX https://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/
XXXI http://ir.homedepot.com/news-releases/2014/09-18-2014-014517752
XXXII http://www.anthemfacts.com/
XXXIII https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html
XXXIV https://www.equifaxsecurity2017.com/
XXXV https://twitter.com/agschneiderman/status/906195350532304896?lang=en
XXXVI https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
XXXVII https://www.owasp.org/index.php/Top_10-2017_A8-Insecure_Deserialization
XXXVIII https://www.owasp.org/index.php/Top_10-2017_A10-Insufficient_Logging%26Monitoring
XXXIX https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control
XL https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls
XLI https://www.ncsc.gov.uk/guidance/secure-development-and-deployment
XLII https://www.asd.gov.au/publications/protect/passphrase-requirements.htm
XLIII https://www.asd.gov.au/publications/protect/multi_factor_authentication.htm
XLIV https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf
XLV https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170021

ASB

Editorial Panel

Contributors

Brett Winterford
Senior Manager, Cyber Outreach, Commonwealth Bank

Arjun Ramachandran
Executive Manager, Cyber Outreach, Commonwealth Bank

Luke Hopewell
Manager, Cyber Outreach, Commonwealth Bank

Martha McKeen
Senior Manager, Cyber Outreach, Commonwealth Bank

Reviewers

Ryan Cotterell
Head of Information Security, ASB

Yuval Illuz
Chief Information Security and Trust Officer, Commonwealth Bank

Kevin Cleary
Cyber Intelligence Researcher, Commonwealth Bank

Thanks To

Dilshan Rajapakse
Cyber Intelligence Engineer, Commonwealth Bank