ASB

Signals

Quarterly security assessment

❯ Q2 2018

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

State-sponsored attackers targeting network infrastructure

Network infrastructure devices such as routers continue to be a prime target for attackers. While large amounts of critical data flow through them, these devices are known to often contain basic security weaknesses. Routers often ship with lower levels of security than other hardware and network and device operators can be less attentive to changing default settings or applying security patches. In April, the US, UK and Australian governments revealed Russian state-sponsored attackers had compromised routers of government and private-sector organisations, critical infrastructure providers, and the internet service providers worldwide[ixx]. In May, researchers revealed 500,000 routers had been infected by malware – dubbed VPNFilter – which was also attributed to Russian state actors[xi]. These forms of compromise could allow attackers to modify or monitor traffic passing through routers, or render them unusable. Commentators assessed these infiltrations were likely a case of actors establishing a foundation for a future attack.

CHECKLIST
› Authorities recommend rebooting network devices. This will potentially disrupt the malware and assist authorities to identify infected devices.[xii]
› Update your device firmware and continue to apply future updates rigorously in accordance with the manufacturer's instructions.
› Change default settings on routers, in particular admin passwords. Consider limiting device management access to whitelisted hosts and disable remote management settings.

New breaches and regulations intensify privacy focus

New data protection regulations and globally prominent data breaches coincided in the first half of 2018 to bring privacy to the fore. In the wake of the Cambridge Analytica scandal, Facebook's approach to data privacy was examined in detail in April when CEO Mark Zuckerberg testified to the US congress in April. The company acknowledged user data had been mishandled and has since announced changes to its privacy settings. Europe's General Data Protection Regulation (GDPR) scheme commenced in May, heightening public and regulator focus on privacy. Australian businesses may need to comply with the GDPR if they offer goods and services in the EU or monitor the behaviour of individuals in the EU.

CHECKLIST
› Consult the Office of the Privacy Commissioner for its guidance[xxix] for New Zealand businesses on the new requirements in the EU's General Data Protection Regulation, and how businesses can comply with Australian and EU privacy laws.
› A good data breach response plan is a fundamental precursor to a good breach response and to ensuring your organisation meets its legal obligations. Read our Deep Dive "Into the Breach" for our insights on implementing such a plan.

Email payment fraud spreading

Notwithstanding rapid development of exploits and sophisticated technical attacks, human deception remains a key backbone of success for financially-motivated cybercrime. A recent report[xvii] by the Australian Competition and Consumer Commission revealed Australian businesses suffered over $22.1 million in losses in 2017 as a result of business email compromise scams. These scams typically involve fraudulent email payment requests sent to accounts staff that appear to come from an organisation's supplier or CEO. A more recent variant has emerged in Australia's active property and real estate sector. The sector has been a particularly attractive to fraudsters of late according to analysts[xviii,] with deposits, settlement[xix] and bond payments being targeted. In June, e-conveyancing platform PEXA revealed the theft of $250,000 in settlement funds[xx], using tactics with similarities to email payment fraud.

CHECKLIST
› Assume your domain and those of your suppliers/ business partners can be spoofed. Whitelist use of your domain for sending email using SPF (Sender Policy Framework) and DMARC (Domain Message, Authentication, Reporting and Compliance).
› 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

$22.1 million
lost by Australians in 2017 through business email compromise[i]

63
data breaches in first six weeks of mandatory data breach notification scheme[ii]

15,000 hours
paid overtime by law firm DLA Piper's IT team to recover from NotPetya malware infection[iii]

39%
of malware cases are ransomware, making it the most prevalent form[iv]

Cyber Security:
Trends and Observations

Web platforms raise the bar

An organisation's presence on the internet involves interaction with a variety of stakeholders, including technology platforms, regulators, browsers and other entities that are responsible for administering aspects of the web. These parties can play a role in whether your digital assets are viewed as secure. One of the more influential web players – Google – is introducing updates to its Chrome browser (the most widely-used browser) to more overtly signal a website's lack of security. From July, Chrome will explicitly mark all HTTP pages (where communication is unencrypted) as "not secure". These steps are motivated by a view that the web should be "secure by default"[xxii], and are part of a broader move[xxiii] by browsers to highlight inferior security practices, such as serving forms over unencrypted connections. More generally, we see online security claims increasingly attracting scrutiny. In April, the UK's Advertising Standards Authority ruled[xxiv] a Barclays Bank advertisement to be misleading by implying a green padlock on a website indicated users were protected against online fraud.

CHECKLIST
› Consider protecting your websites with HTTPS, to protect communications with your customers and to continue to provide them with confidence in the security of your websites. This can also ensure your sites continue to support the latest functionality, with HTTPS increasingly considered a base requirement for new features.
› Review the published stance and guidance from major browsers[xxv] on the importance of HTTPS.
› In light of these changes to the way websites will be displayed, and increased scrutiny of the public and regulators, review any advice you're giving to customers about how to determine a website's security.

Supply chain attacks continue to dominate

As security company Kaspersky defends itself against growing assertions[xxvi] about links to Russian agencies, the risks associated with software supply chains has been further highlighted by malicious code found in software used by companies to track and recover lost laptops. In May, researchers revealed instances of the LoJack for Laptops software agent had been connecting to domains associated with Russian-aligned hacker group Fancy Bear. Attacks such as these – where malware is implanted into the software supply chain – have grown 200 per cent, according to security firm Symantec[xxvii]. NotPetya – one of the more prominent examples of a supply chain attack – has recently been dubbed by the White House "the most destructive and costly cyber-attack in history". We assess that supply chain risk looms as an increasing area of concern for industries rapidly embracing connectivity and technology. A recent report[xxviii] into the Australian health sector observed a number of internet-connected systems and tools used by healthcare organisations could be discovered online through scanning tool Shodan, and potentially exploited by attackers for remote attacks.

CHECKLIST
› The security standards of potential suppliers and their ability to meet your security obligations should be key factors in your procurement decisions, particularly in cases where customer data is being stored.
› Ensure you have an active security compliance program that compels suppliers and other partners to protect your data to an agreed standard.
› With increased scrutiny and obligations around reporting data breaches, it is vital to have a plan and in place for how your organisation would respond to a breach of customer data via a supplier or third party.

Web publishing tools exploited for cryptomining

Attackers continually seek to extract the largest possible impact from their efforts by targeting vulnerabilities in popular software platforms known to be used by many organisations. Content Management Systems (CMS), commonly used to maintain and publish websites, have long been a popular target for this reason. In April, researchers revealed that vulnerabilities in the Drupal CMS could allow attackers to remotely execute code on underlying servers. By May, hundreds of sites[xiii] were found to be running malicious code, including cryptomining malware that uses up server CPU power to mine cryptocurrency for attackers (the last edition of Signals outlined this trend). The vulnerabilities have also been used to install malware that would enable denial of service attacks. Similar remote code execution vulnerabilities have also recently been found in PHP[xiv], the popular programming language that also underpins the Drupal CMS.

CHECKLIST
› If your organisation is running a Drupal site/sites, ensure your administrators patch your systems immediately. If you had not patched by early April (when attacks against the vulnerabilities were being observed), you may need to assume the compromise of your site and consider restoring from a backup. Drupal's security team has published extensive guidance[xv] on the issue.
› Review the Australian Signals Directorate's lists of preventative controls to mitigate the risk of malware infection. The ASD's "Essential Eight' recommends – among other controls – that organisations prioritise vulnerability and patch management programs to prevent infections.
› In light of the continued exploitation of vulnerabilities by attackers in order to mine cyptocurrency, actively monitor CPU utilisation and network traffic for abnormalities. Systems showing high CPU usage or abnormal traffic might be suggestive of an infection.
› Continue to educate your software developers to write secure code and be aware of common vulnerabilities and how attackers exploit them. The Open Web Application Security Project[xvi] (OWASP) publishes guidance on the top 10 web application security risks. Consider sending developers to AppSecDay, OWASP's annual application security conference (sponsored by Commonwealth Bank).

By the Numbers

US$1.1 billion
in cryptocurrency-related thefts during the past six months[v]

58%
of Australia and New Zealand organisations increased security spending in 2017[vi]

76%
of breaches are financially motivated[vii]

Organisations have

72 hours
to report breaches under GDPR[viii]

Deep Dive:
Into the Breach

Turning your Data Breach Response Plan into a vehicle for change

Lucy Mannering
Portfolio Manager Digital Trust
& Privacy, Commonwealth Bank

Luke Hopewell
Manager, Cyber Outreach,
Commonwealth Bank

Readers may be aware that Australian organisations are now subject to mandatory data breach reporting obligations under the Notifiable Data Breaches (NDB) scheme. The scheme requires that businesses notify individuals likely to be 'at risk of serious harm' as a result of a data breach relating to their personal information. In New Zealand there is a Privacy Bill going through parliament that will repeal and replace the Privacy Act 1993 that proposes mandatory breach reporting. These new regulatory requirements, combined with continually evolving cyber threats and ever heightening expectations around privacy, have made a strong Data Breach Response Plan (DBRP) a fundamental necessity.

The need for a DBRP won't be news to many readers. In the lead up to the NDB scheme taking effect, much has been written on this topic and, specifically, on how to create a DBRP. In this feature, we share our insights from having implemented a DBRP, and lessons on turning the DBRP from an isolated artefact into a foundation for a strong response culture.

WHY HAVE A RESPONSE PLAN?
Let's briefly recap the benefits of having a DBRP. Most obviously, having a comprehensive plan in place ensures you are best prepared for a data breach. We've written in previous editions of Signals[xxx] that the quality of a breach response can be more impactful on public trust than the breach itself.

A DBRP allows you to clarify roles and responsibilities, highlight escalation guidelines and identify resources required in the event of a data breach incident. It's also an effective way to educate your organisation on what happens in the event of a breach.

The DBRP is also a key way to ensure compliance against the NDB scheme, and is itself a useful artefact to communicate your privacy practices to the Australian Information Commissioner, in the event of an investigation.

WHAT SHOULD BE IN A DBRP?
The Office of the Privacy Commissioner offers a Data Safety Toolkit which includes guidance on developing a data breach response plan[xxxi].

While the importance of responding quickly to a data breach response may be understood, for many staff the precise stages of a response will be unfamiliar. The DBRP is an effective tool to communicate the lifecycle of and drive consistency in data breach incident response. At a high-level, the DBRP should cover these stages:

Identification: Once identified, assign an incident owner to assess the scope of the event, contain the incident and minimise harm and commence investigation. The incident owner plays a key role in the response process. Considering this, it may be most appropriate for the incident owner to be someone with risk or compliance accountabilities.

Assessment: An impact assessment will determine whether notification is necessary, and whether a larger incident response team is

Source of the breaches reported in the quarter
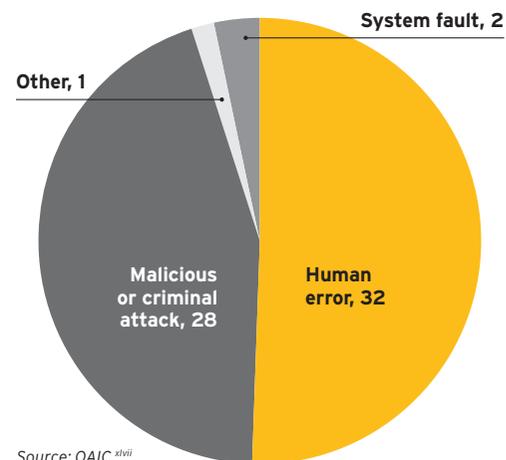
Other, 1
System fault, 2
Malicious or criminal attack, 28
Human error, 32

Source: OAIC [xlvii]

needed. Tools such as the 5x5 risk matrix can be used here.

Reporting & Escalation: For serious incidents, strategies to notify customers, the regulator and senior executive committees will be developed and executed at this stage.

Rectifying & Resolving: The incident should be reviewed to extract lessons and inform development of a prevention plan.

IMPLEMENTING A DBRP SUCCESSFULLY
Having built your plan, bringing it to life within your organisation is another matter. Here are some key lessons we've learnt.

Get buy-in, use stick and carrot: You want the DBPR to be a living and actively-used document, so invest time and energy in communicating its importance and benefit for your organisation. Communications issued by your most senior

---

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

Deep Dive:
Into the Breach

" When a data breach occurs, a quick and effective response can have a positive impact on people's perceptions of an organisation's trustworthiness. That is why being prepared for a data breach is important for all organisations that handle personal information **"**

executives will draw staff attention to the DBRP's role in ensuring the organisation meets its legal requirements. This alone may not be enough to drive proactive use of the DBRP. For that, promote the DBRP not just as a compliance vehicle, but as a tool that supports your business to build great outcomes for customers, especially by protecting their privacy.

Build supporting infrastructure around the DBRP: In many organisations, the creation of a DBRP will bring a more structured and rigorous process for identifying potential data breaches than previously has been in place. It's likely there will be an immediate spike in potential incidents being reported – you'll need teams and processes to support the organisation using the DBRP and appropriate systems to log, triage and action incidents. Systems should also be capable of drawing out trends and insights from the data you are logging (more on this later).

Assemble an effective response team: The data breach response team is central to the effective execution of the data breach response plan. The aforementioned OAIC guide describes how to compose such a team, with key roles including legal and compliance staff, cyber security and forensics teams, HR support (for breaches due to staff action) and communications experts. In our experience,

INCIDENT MANAGEMENT BEST PRACTICE

- Commence remedial action at the earliest opportunity
- Minimise risk of harm to individuals and the organisation
- Preserve evidence to maintain integrity of the fact find process
- Maintain legal privilege and confidentiality.
- Engage relevant business units for support
- Maintain records of decisions and reasoning
- Apply escalation protocols and continue to assess impact as investigations continue

staff that have a deep understanding of the organisation are vital to the response team, particularly to assess and understand the parties and data involved in an incident, in order to determine seriousness and accountabilities. Finally, the members of the data breach response team will differ for specific incidents depending on the organisation and the circumstances of the incident. It may not even be necessary to involve a broad response team for certain incidents. The key is to have a variety of expertise available on an on-call basis.

Codenames and war rooms: Having implemented a data breach response plan, ideally you'll be having more regular and open conversations about potential data breaches

and how to respond to them. This is a positive outcome, but needs to be managed with discretion. Devise codenames for incidents – better that staff are heard discussing "MOONSTONE" than "the incident where customer files were lost by staff on the bus". Allocate dedicated physical space (war room) for response teams to meet.

GETTING THE MOST VALUE FROM YOUR DBRP
Effective implementation of the DBRP will include the collection and reporting of data that can be analysed to inform a better understanding of your organisation's privacy culture, and drive strategic improvements.

After a few months of the NDB scheme, we've seen how data that results from having a DBRP in place provides key insights, including:

- **Hotspots in your business** – By collecting data on potential incidents over time, an improved understanding of data management practices right across the organisation develops. Privacy and security teams can better understand teams or business units that may be particular hotspots and target accordingly.

- **Patterns of behaviour** – Breaches can take many forms – from loss of physical files, to data

theft through cyber-attack, to staff inadvertently emailing documents to the wrong person. In Australia, for example, the OAIC's first quarterly report[xxxii] indicated human error was the cause of the largest number of eligible data breaches. Your own data may similarly illuminate particular practices, patterns or points-in-time that lead to higher number of data incidents.

- **Informing policy, technology and training needs** – building on the last point, data from the DBRP can drive changes to policies or workplace technologies, or lead to new staff training programs, in order to address known hotspots and improve the organisation's privacy posture. Having a regular spot on the agenda of senior forums in your organisation where these insights can be shared will help drive these changes.

DBRP TOP DO'S AND DON'TS
DO – have clear accountabilities in your breach response team

DO – invest in a platform to log incidents and identify trends

DO – get exec support for the plan

DON'T – be unprepared for spike in reported incidents

DON'T – discuss incidents indiscreetly. Use codenames and war rooms

DON'T – leave business unsupported in executing DBRP. Training and OCM are key

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

Better Practice

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

Some help meeting new data protection regulations?

For: CISOs, legal practitioners, regulatory and compliance teams

The Office of the Privacy Commissioner (OAIC) has published a technology guide[xlii], which outlines how businesses can comply with their privacy obligations in relation to emerging and existing technologies. In a similar vein, for organisations that are subject to GDPR, the UK's Information Commissioner's Office has issued guidance on technical security outcomes[xliii] expected under the new European regulation.

Updated NIST Cyber Security Framework

For: CISOs and cyber security strategy teams

NIST has released an update to its Cybersecurity Framework[xliv], a widely used tool to guide organisations' cyber security strategy and investments. NIST recommends customising the framework according to your organisation's individual needs.
What's changed? This version includes expanded sections on using the framework to perform self-assessments of cyber security risk and for supply chain risk management.

DDoS resilience

For: CISOs and network administrators

Organisations today cannot avoid being targeted by distributed denial-of-service (DDoS) attacks, says the Australian Cyber Security Centre. But it notes that there are measures they can implement to prepare and reduce the impact should such an attack occur. The centre has published this guide[xlv] with tips on preparing for, responding to and avoiding DDoS attacks.

The threat that "keeps IT security staff awake at night"

For: CISOs and security teams

CERT Australia minces no words, describing insider threat as "the hardest to mitigate, detect and prosecute". In this new guide[xlvi], it recommends a multi-faceted approach to mitigating insider threat that goes beyond technology. Network monitoring, application whitelisting and strong access controls are among a strong baseline of technical controls recommended. Beyond that, CERT highlights the importance of cultural factors and staff education.

Horizon Scan
Upcoming events of interest

2018 Oct 19

Melbourne
OWASP AppSec Day

Commonwealth Bank's Digital Protection Group will again be the principal (Diamond) sponsor of AppSecDay, the annual application security conference organise by the Open Web Application Security Project (OWASP). AppSecDay provides a forum for software developers, testers, DevOps engineers and security professionals to improve the security of their apps. The event features talks andhands-on technical workshops led by prominent Australian developers and security professionals.

2018 Oct 25-27

UCSA Events Centre, Christchurch, New Zealand
Christchurch Hacking Conference

CHCon is a conference for security professionals and hackers in Christchurch, NZ. Training will be run on Thursday 25th October, and presentations on Friday 26th and Saturday 27th. Badge and locksport challenges will be run throughout the main event.
https://2018.chcon.nz/

2018 Nov 16-17

Michael Fowler Centre, Wellington, Aotearoa
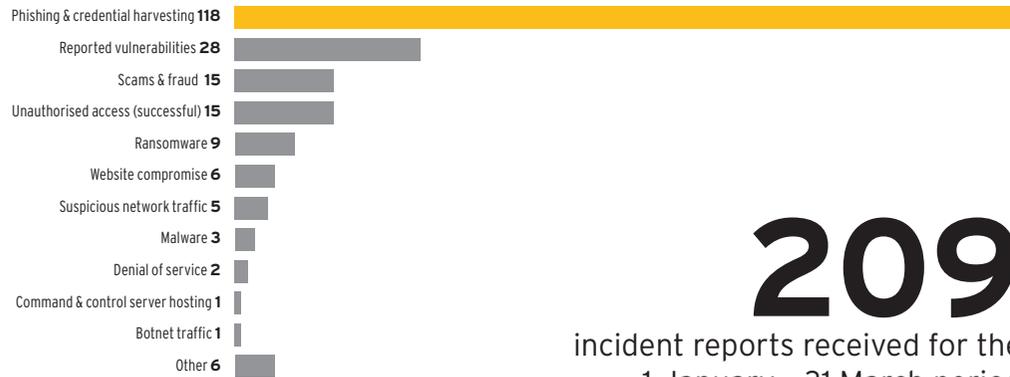### Kiwicon 2038

After a brief hiatus, KIWICON is back for 2018 with a distinctly cyberpunk vibe. KIWICON is the principle gathering of New Zealand and Asia-Pacific's cyber security researchers, practitioners and policymakers.

Incident Report

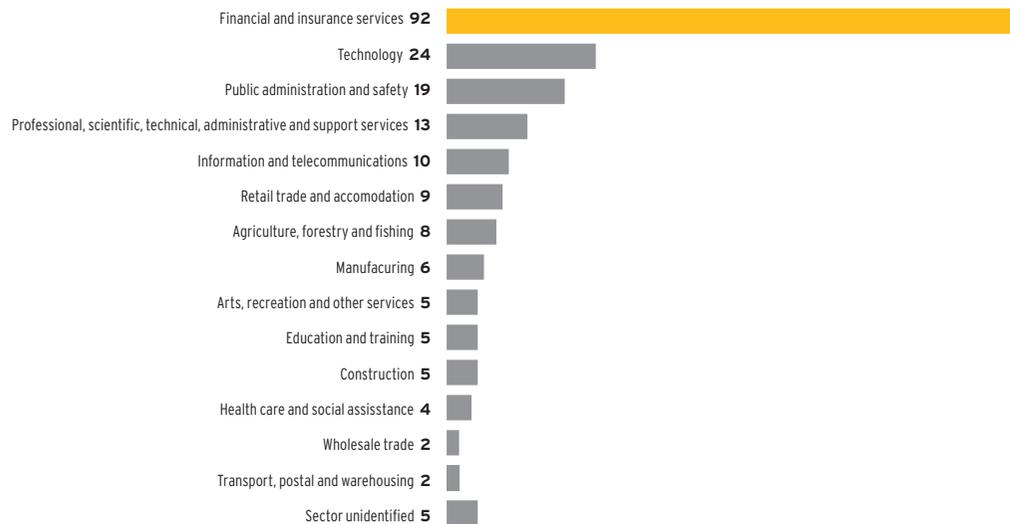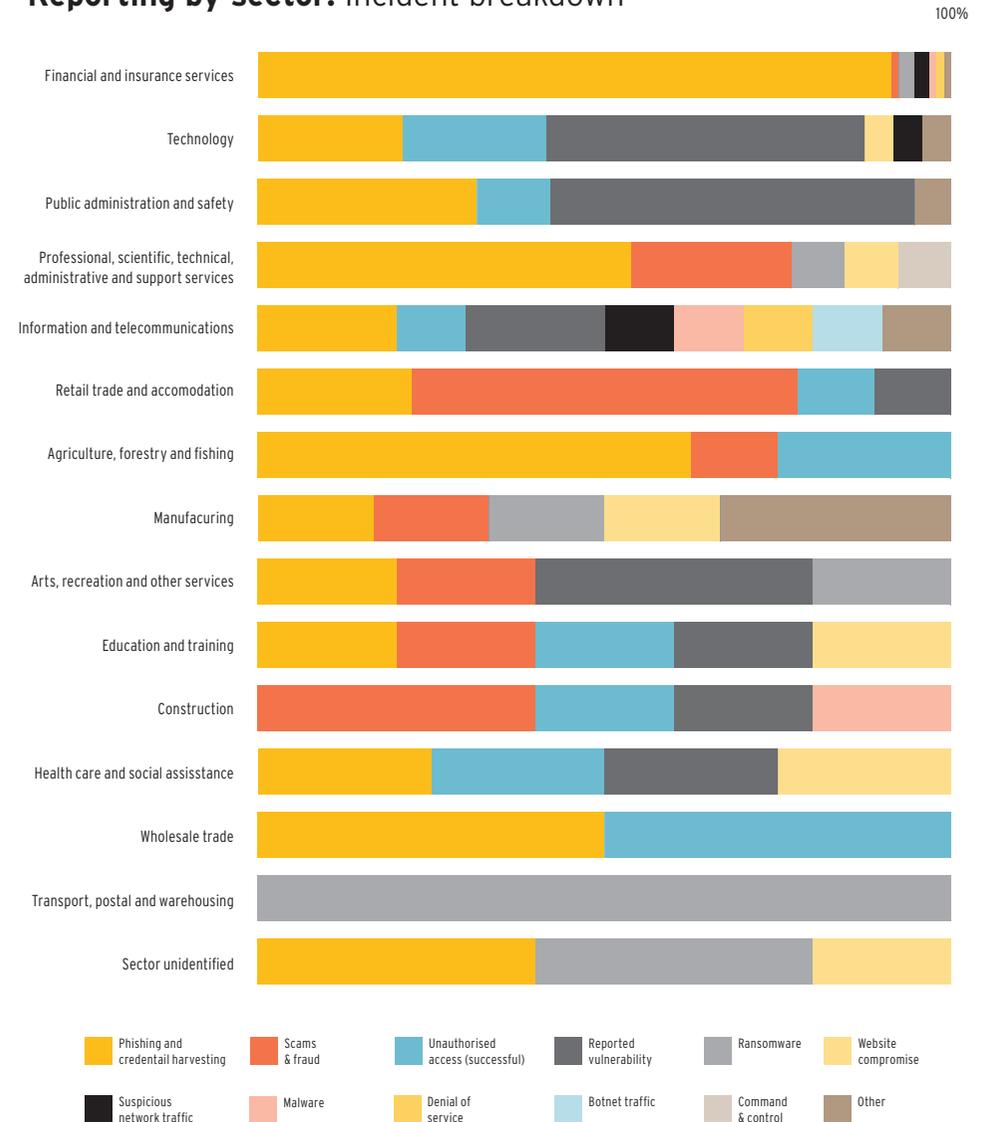*CERT NZ's cyber security incident organisation statistics from around the country[xxvii]*

certnz

Reporting by category

Category	Count
Phishing & credential harvesting	118
Reported vulnerabilities	28
Scams & fraud	15
Unauthorised access (successful)	15
Ransomware	9
Website compromise	6
Suspicious network traffic	5
Malware	3
Denial of service	2
Command & control server hosting	1
Botnet traffic	1
Other	6

209

incident reports received for the
1 January – 31 March period

Reporting by sector

Sector	Count
Financial and insurance services	92
Technology	24
Public administration and safety	19
Professional, scientific, technical, administrative and support services	13
Information and telecommunications	10
Retail trade and accomodation	9
Agriculture, forestry and fishing	8
Manufacuring	6
Arts, recreation and other services	5
Education and training	5
Construction	5
Health care and social assisstance	4
Wholesale trade	2
Transport, postal and warehousing	2
Sector unidentified	5

Reporting by sector: Incident breakdown

100%

Sectors (top to bottom):
Financial and insurance services; Technology; Public administration and safety; Professional, scientific, technical, administrative and support services; Information and telecommunications; Retail trade and accomodation; Agriculture, forestry and fishing; Manufacuring; Arts, recreation and other services; Education and training; Construction; Health care and social assisstance; Wholesale trade; Transport, postal and warehousing; Sector unidentified

Legend:
- Phishing and credentail harvesting
- Scams & fraud
- Unauthorised access (successful)
- Reported vulnerability
- Ransomware
- Website compromise
- Suspicious network traffic
- Malware
- Denial of service
- Botnet traffic
- Command & control
- Other

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

Endnotes

i https://www.accc.gov.au/system/files/F1240_Targeting%20scams%20report.PDF
ii https://www.oaic.gov.au/media-and-speeches/news/notifiable-data-breaches-first-quarterly-report-released
iii https://www.itnews.com.au/news/dla-piper-paid-15000-hours-of-it-overtime-after-notpetya-attack-490495
iv http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
v https://www.carbonblack.com/wp-content/uploads/2018/06/Cryptocurrency_Gold_Rush_on_the_Dark_Web_Carbon_Black_Report_June_2018.pdf
vi https://www.bdo.com.au/BDO_AU/media/bdo/PDF/CyberSecurityReport_20172018FINAL.pdf
vii http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
viii https://gdpr-info.eu/art-33-gdpr/
ix http://minister.homeaffairs.gov.au/angustaylor/Pages/australian-government-attribution-of-cyber-incident-to-russia.aspx
x https://www.us-cert.gov/ncas/alerts/TA18-106A
xi https://www.ic3.gov/media/2018/180525.aspx
xii https://www.ic3.gov/media/2018/180525.aspx
xiii https://badpackets.net/large-cryptojacking-campaign-targeting-vulnerable-drupal-websites/
xiv https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-arbitrary-code-execution_2018-046/
xv https://groups.drupal.org/security/faq-2018-002
xvi https://www.owasp.org/
xvii https://www.accc.gov.au/system/files/F1240_Targeting%20scams%20report.PDF
xviii https://www.inforisktoday.com/in-australia-email-compromise-scams-hit-real-estate-a-11049
xix http://www.abc.net.au/news/2017-10-25/scam-targets-conveyancing-clients-in-sa/9086172
xx https://www.itnews.com.au/news/pexa-beefs-up-security-controls-after-home-sale-fraud-495437
xxi https://www.commbank.com.au/content/dam/commbank/assets/business/can/business-insights/signals/signals-email-payment-fraud-march-2018.pdf
xxii https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html
xxiii https://www.troyhunt.com/life-is-about-to-get-harder-for-websites-without-https/
xxiv https://www.asa.org.uk/rulings/barclays-bank-plc-a17-409277.html
xxv https://developers.google.com/web/fundamentals/security/encrypt-in-transit/why-https
xxvi https://www.bankinfosecurity.com/eu-claims-kaspersky-lab-software-confirmed-as-malicious-a-11080
xxvii https://www.cert.govt.nz
xxviii https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf
xxix https://www.privacy.org.nz/privacy-for-agencies/gdpr-resources/
xxx https://www.asb.co.nz/content/dam/asb/documents/reports/signals/asb-signals-2017-q4.pdf
xxxi https://www.privacy.org.nz/data-breaches/data-safety-toolkit/ /
xxxii https://www.oaic.gov.au/media-and-speeches/news/notifiable-data-breaches-first-quarterly-report-released
xlii https://www.privacy.org.nz/privacy-for-agencies/technology-guidance/
xliii https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes
xliv https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
xlv https://asd.gov.au/publications/protect/preparing-for-responding-to-ddos-attacks.htm
xlvi https://www.cert.gov.au/news/insider-threat-beyond-technical-controls

Editorial Panel

Contributors

Lucy Mannering
Portfolio Manager Digital Trust & Privacy, Commonwealth Bank

Luke Hopewell
Manager, Cyber Outreach

Martha McKeen
Senior Manager, Cyber Outreach

Reviewers

Yuval Illuz
Chief Information Security and Trust Officer

Kevin Cleary
Cyber Intelligence Researcher

Ryan Cotterell
Head of Information Security, ASB

Malcolm Allen
Information Security Consultant, ASB

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

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

CONFIDENCE IN OUR ASSESSMENTS

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

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

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

ASB