certnz

Quarterly Report:
Data Landscape

Q2

1 April – 30 June
2018

New Zealand Government

/// Contents

1. Introduction

This document provides a standardised set of results and graphs for the quarter, and easily digestible analysis of the latest trends. Analytical comment is provided where meaningful or interesting trends were identified.

This report covers the quarter from 1 April 2018 – 30 June 2018.

This document, the CERT NZ Quarterly Report: Data Landscape, is supplemented by the CERT NZ Quarterly Report: Highlights which summarises key observations and focus areas that our data is demonstrating.

You can find both on our website at www.cert.govt.nz/about/quarterly-report/.

2. Incidents and referrals

Incident summary

Between 1 April and 30 June 2018, 736 incidents were reported to CERT NZ. This is up 45% from the 506 incidents reported in the previous quarter.

Table 1: Incident partner referrals

736 incidents reported	
615	responded to directly by CERT NZ
112	referred to NZ Police
9	referred to Netsafe
0	referred to National Cyber Security Centre
0	referred to Department of Internal Affairs

Of the 736 incidents reported:

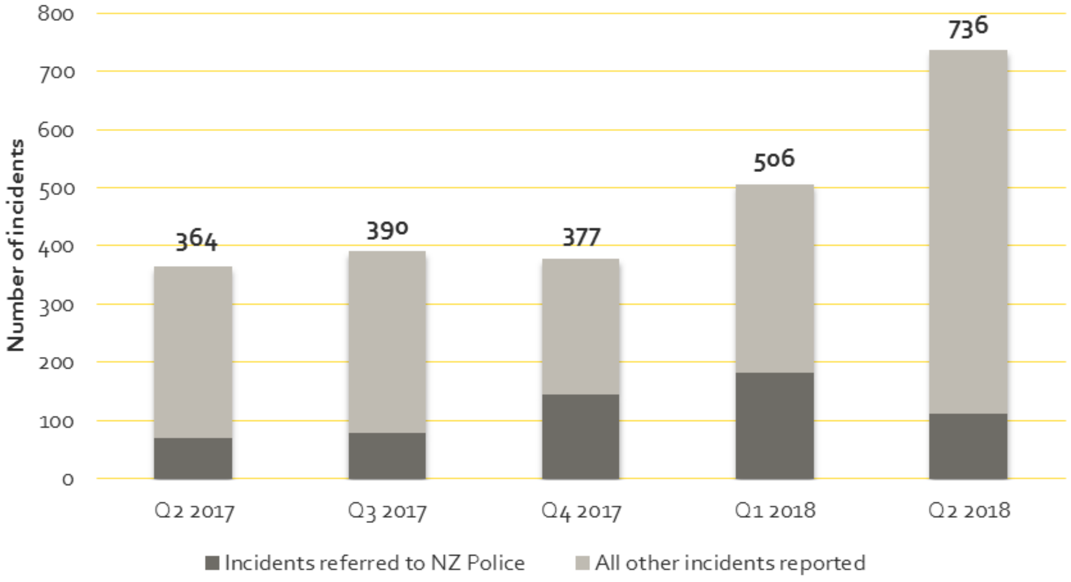
- 615 (84%) were responded to directly by CERT NZ, almost double the number from last quarter
- 112 (15%) were referred to NZ Police, down 38% from last quarter

Another 94 events were automatically directed to other agencies and weren't recorded as an incident by CERT NZ. Our online reporting tool does this when it is immediately identifiable as being outside CERT NZ's scope and best dealt with by an agency with the right expertise, e.g. cyber bullying, spam, online child abuse.

Incidents per quarter

The total number of incidents reported to date is 2,373.

Figure 1: Number of incidents reported by quarter



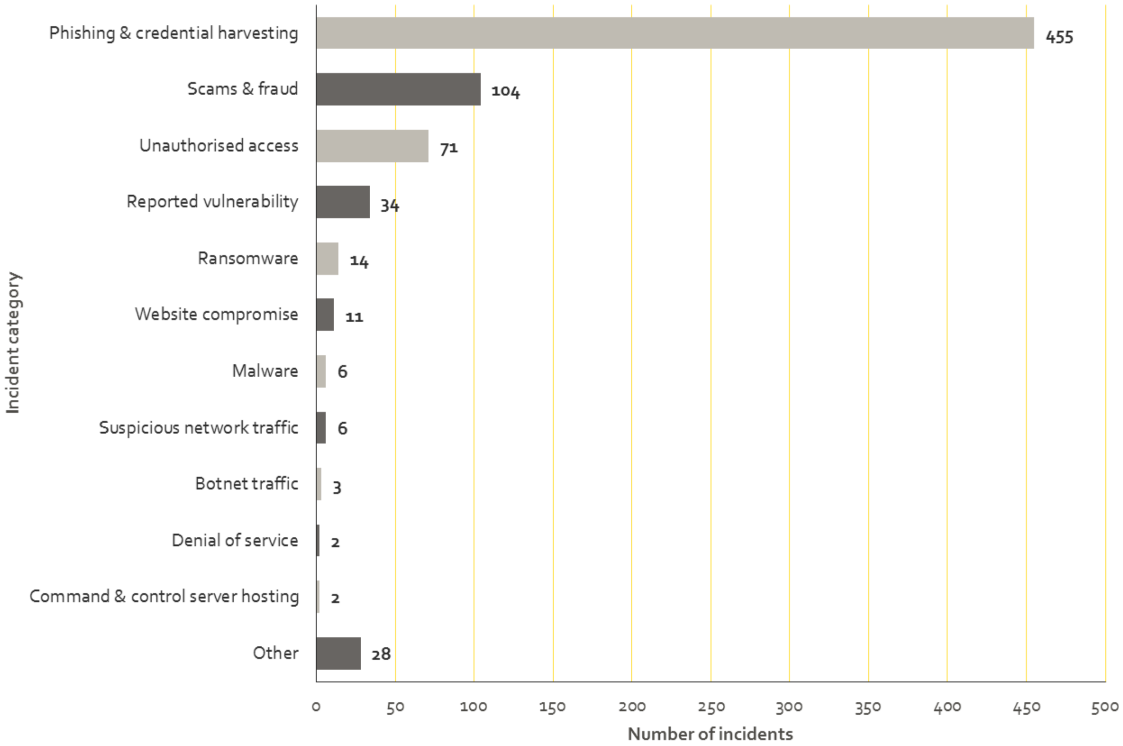
3. Reporting by incident category

Breakdown by category

Phishing & credential harvesting reports have increased again by over 132% from last quarter. This increase continues to come largely from cooperation with New Zealand-based banks and financial services organisations.

Scam & fraud reports are down 38% from last quarter. The number of vulnerability reports is similar to last quarter (35 in Q1 2018)

Figure 2: Breakdown by incident category

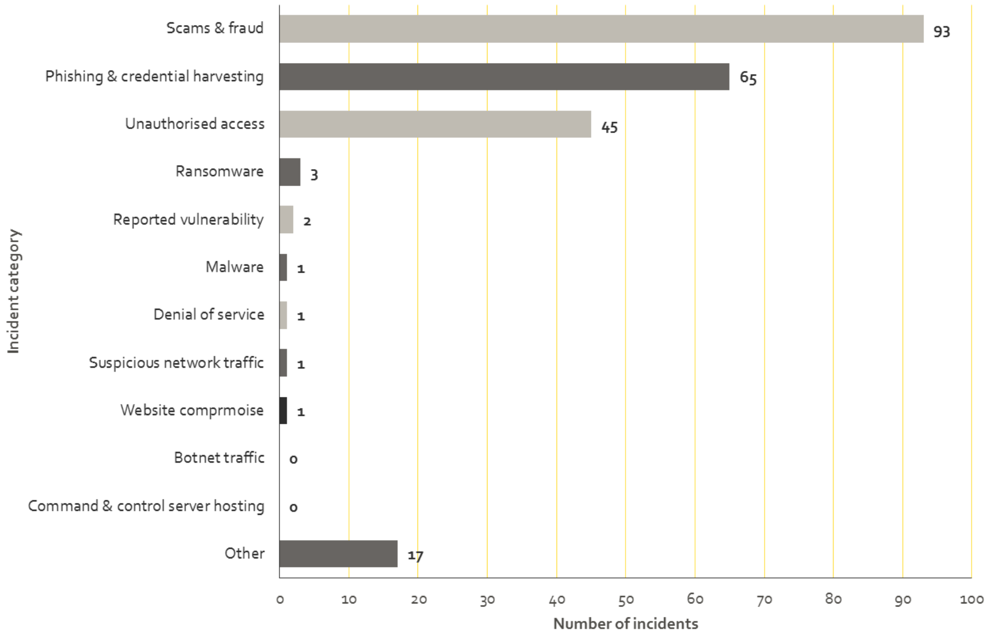


337 (74%) of the phishing & credential harvesting reports are about the financial sector with 118 (26%) about other sectors or individuals. Of the 337 about the finance sector, 95% (321) used a New Zealand brand.

Breakdown of incidents about individuals

This quarter there were 229 incident reports about individuals, 31% of all incident reports received. This is a 23% decrease from the 297 received in Q1 2018.

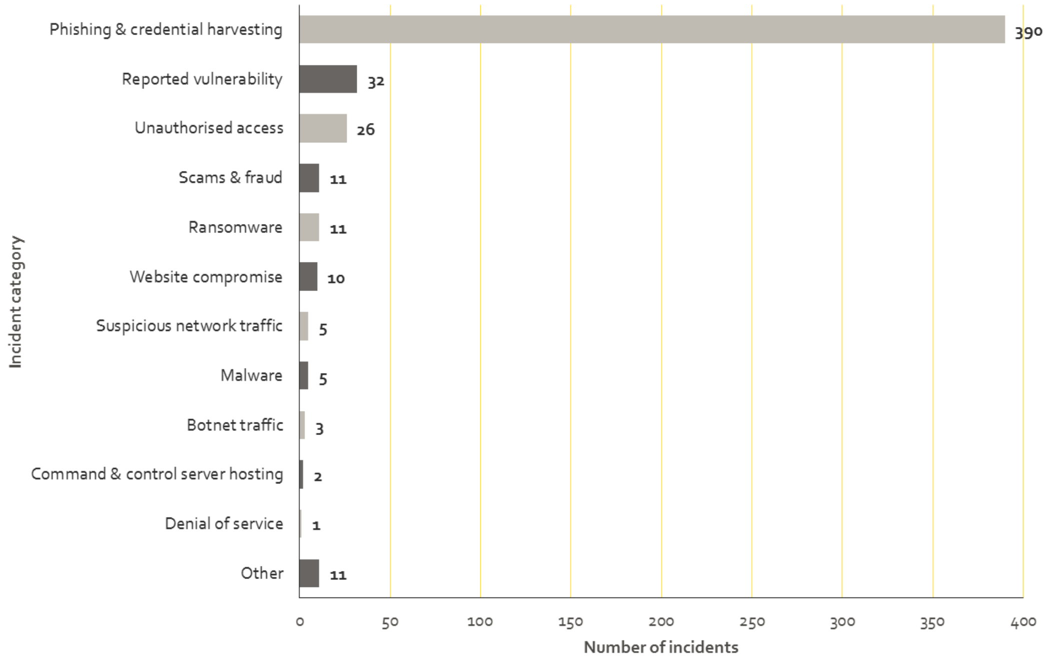
Figure 3: Breakdown of incidents about individuals



Breakdown of incidents about organisations

There were 507 incident reports about organisations, 69% of all incident reports received. This is a 143% increase from the 209 received in Q1 2018.

Figure 4: Breakdown of incidents about organisations



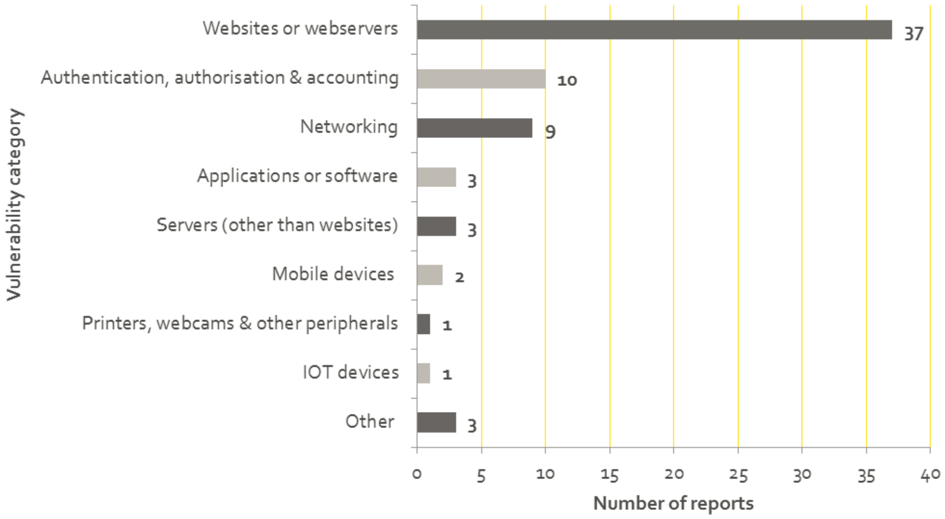
Breakdown of reported vulnerabilities – Q1 & Q2

A vulnerability is a weakness in software, hardware, or an online service that can be exploited to access information or damage a system. Early discovery of vulnerabilities means they can be addressed to prevent future incidents.

In response to requests, this quarter we have broken down vulnerability reports by category in Figure 5. The data used covers both Q1 and Q2 2018. We use broad vulnerability categories to group these reports - over time we will refine these categories to a more granular level as the data set grows. A full list of the vulnerability categories can be found at the end of this document.

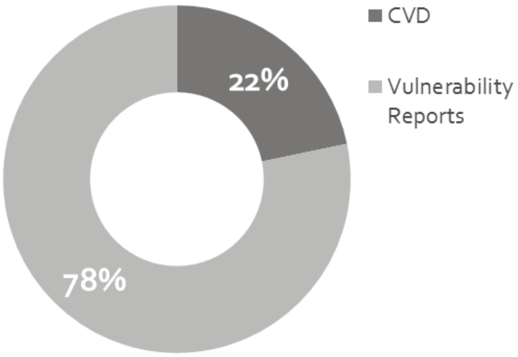
Of the 69 vulnerability reports received 1 January -30 June 2018, 54% related to website applications and servers, 14% to authentication, authorisation and accounting and 13% to networking.

Figure 5: Breakdown of reported vulnerabilities



Some vulnerability reports come under CERT NZ's Coordinated Vulnerability Disclosure (CVD) policy. This is used when the person reporting the vulnerability doesn't want, or has been unable to, contact the vendor directly themselves. CERT NZ received 15 vulnerability reports using the CVD policy 1 January -30 June2018[1].

Figure 6: Breakdown of vulnerability reports 1-30 June 2018



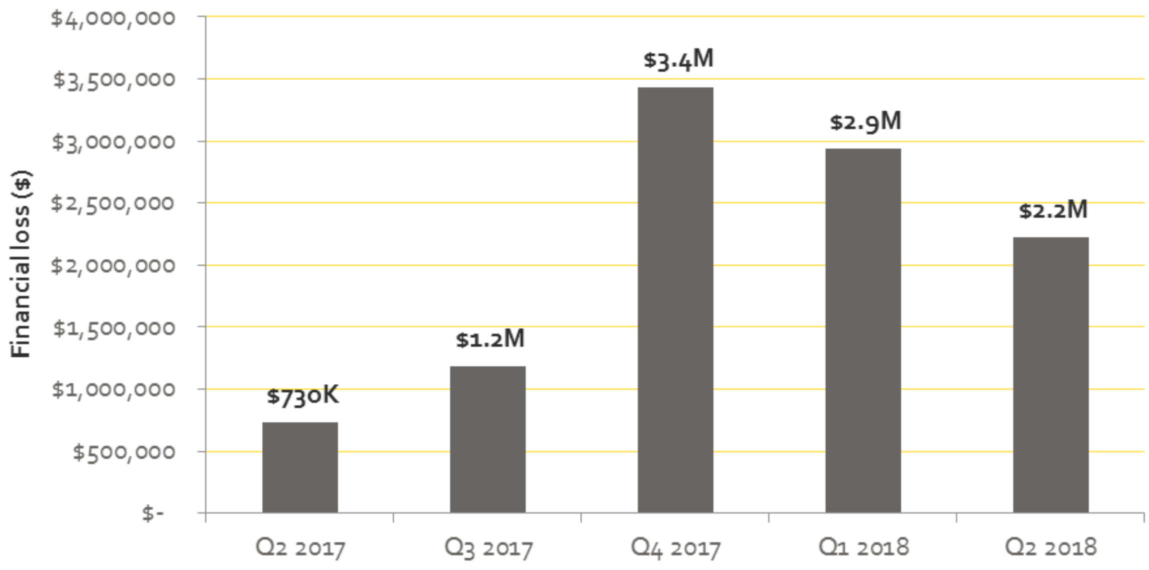
[1] https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/

4. Impacts

Total financial losses

This quarter, direct financial losses totalled $2,221,593. This is down by 24% from the last quarter.

Figure 7: Direct financial losses per quarter



Distribution of financial loss

The spread of direct financial loss between reports about individuals, and those about organisations was:

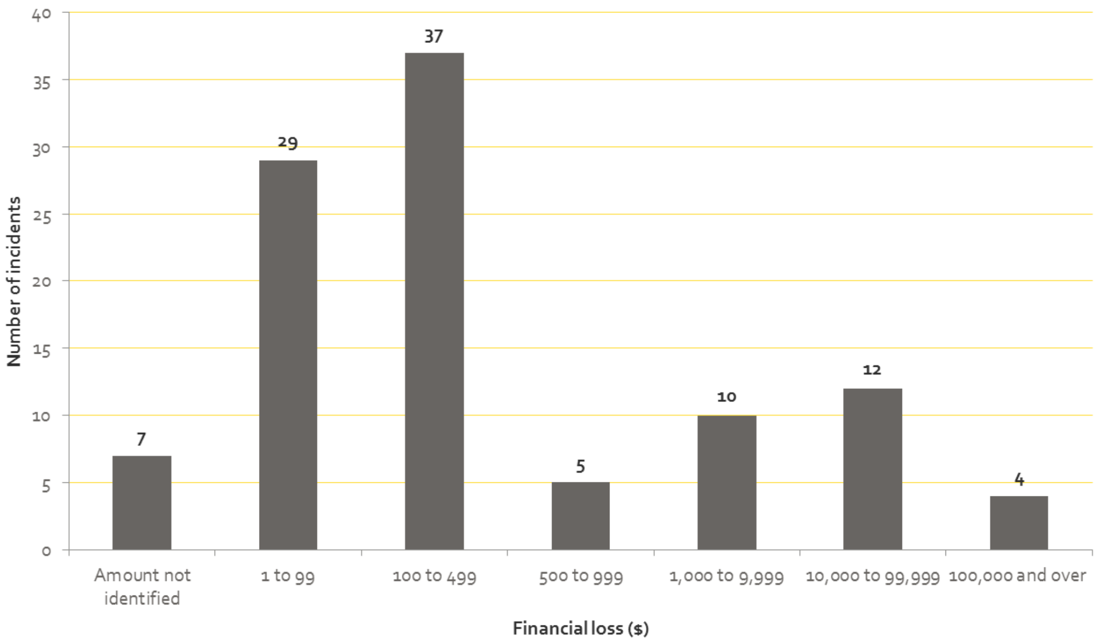
- organisations reported $1,522,767 (69% of all direct financial loss)
- individuals reported $698,826 (31% of all direct financial loss)

During this quarter, four incidents involved losses of $100,000 or more, totalling $1,710,000. These four incidents made up almost 77% of all reported financial losses. Of these four incidents:

- 2 involved scams & fraud
- 1 involved phishing and credential harvesting
- 1 involved unauthorised access.

Altogether 104 incidents reported a direct financial loss this quarter, down 38% from Q1 2018 (167).

Figure 8: Distribution of direct financial loss



68% of incidents reporting loss are for amounts below $500.

Types of loss

Of the incidents reported this quarter, 21% (157) reported some type of loss (not just financial losses).This is a down from the 45% (226) of incident that reported some type of loss last quarter. Note that some reports include multiple types of loss.

Of the 229 incidents reported about individuals, 49% (113) involved some type of loss. Of the 507 incidents reported about organisations, 9% (44) involved some type of loss.

Losses experienced are broken down by type as follows:

Table 2: Types of loss

14%	**Financial loss:**	The direct financial costs of an incident. This could be money lost as a result of an incident, but can also include the costs of recovering, such as needing to contract IT security services or investing in new security systems after an incident (Q1 2018: 33%).
2%	**Reputational loss:**	Damage to the reputation of an individual or organisation as a result of being the victim of an incident (Q1 2018: 2%).
5%	**Data loss:**	Loss or unauthorised copying of data, business records, personal records and intellectual property (Q1 2018: 6%).
2%	**Technical damage:**	Impacts on services like e-mail, phone systems or websites, resulting in disruption to a business or organisation (Q1 2018: 3%).
2%	**Operational impacts:**	The time, staff and resources that need to be spent on recovering from an incident, taking people away from normal business operations (Q1 2018: 3%).
1%	**Other:**	Includes types of loss not covered in the other categories (Q1 2018: 4%).

5. Demographics

Reporting by sector

Of the 507 incidents reported about organisations, the three sectors with the most reports were:

- Financial and insurances services with 350 (69%)
- Technology with 38 (7%)
- Professional, scientific, technical, administrative and support services and information and telecommunications both with 21 (4%).

The increased number of phishing reports from New Zealand banks and financial services organisations is contributing to the increase in reports for this sector.

Figure 9: Reports about organisations; breakdown by sector

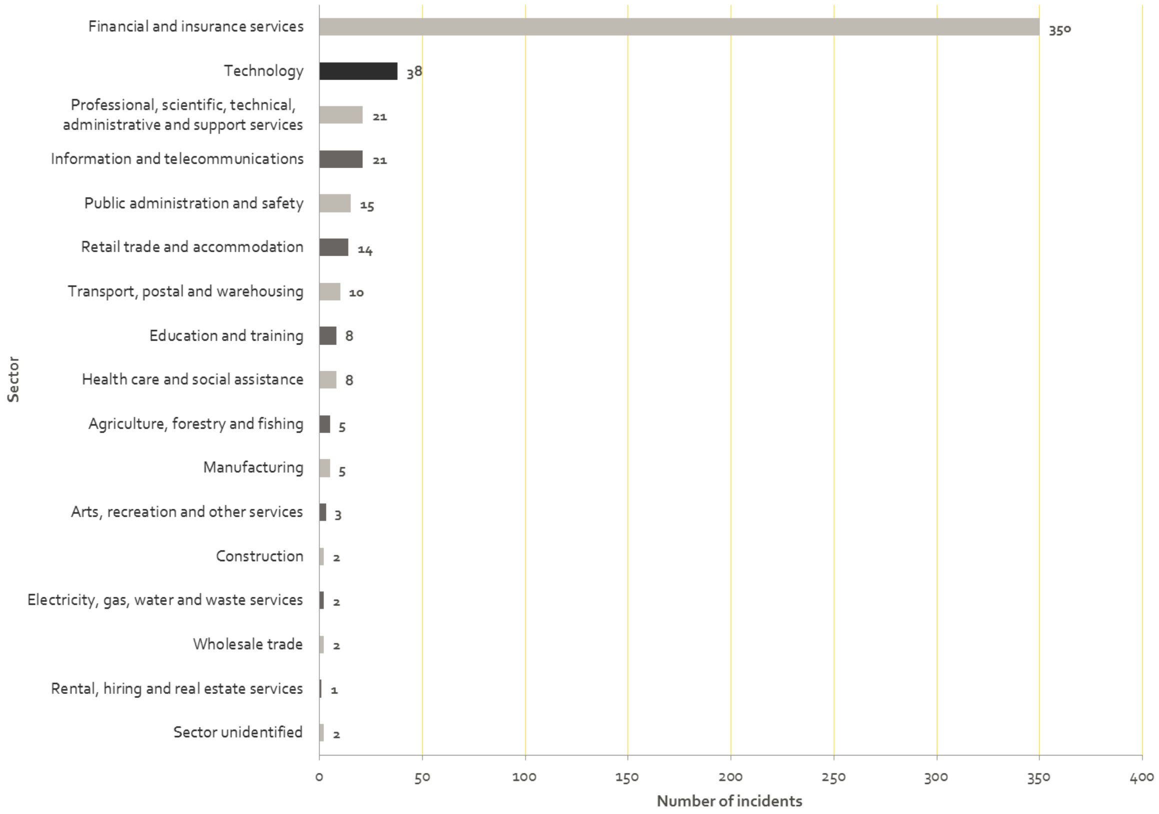
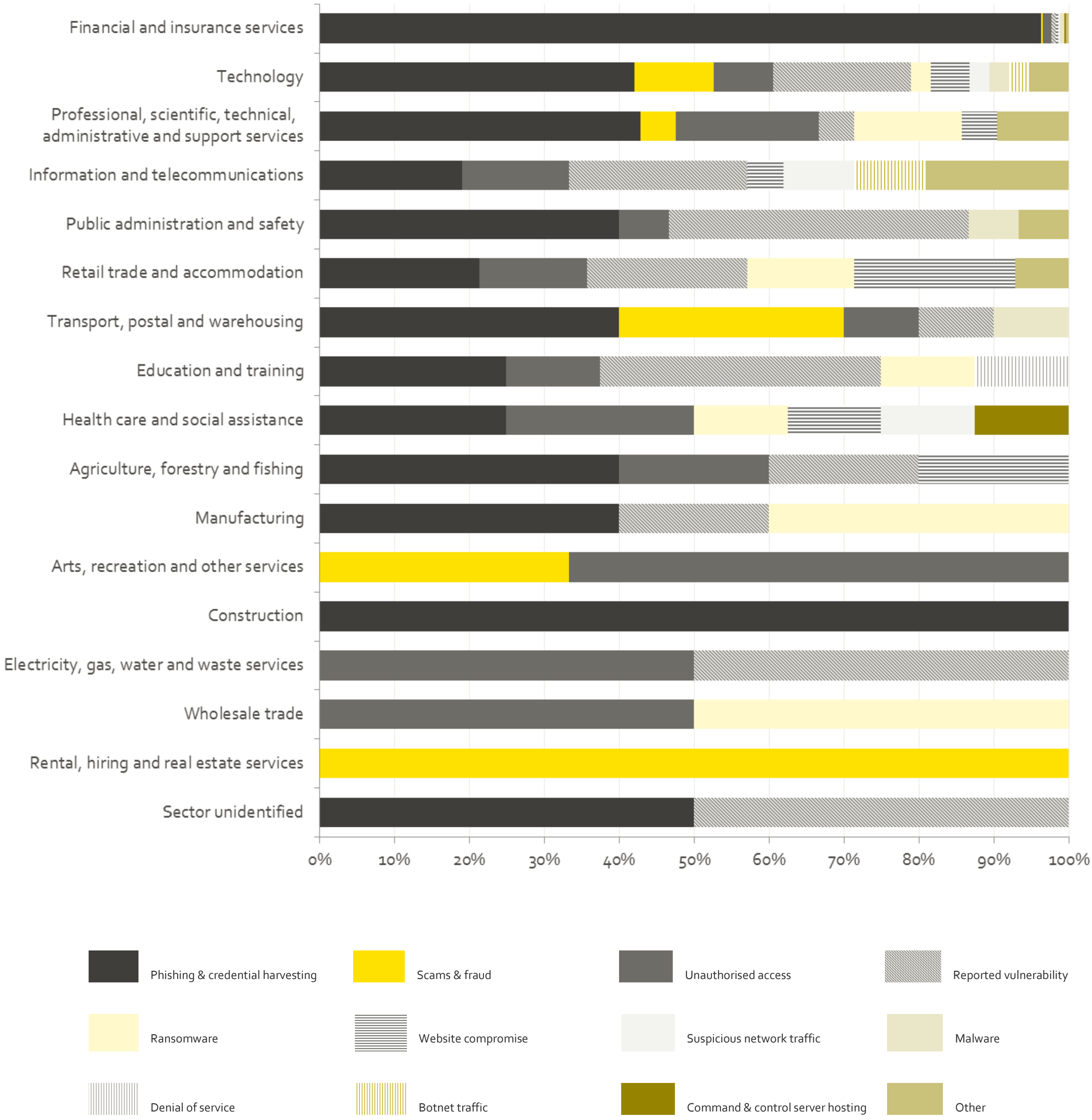


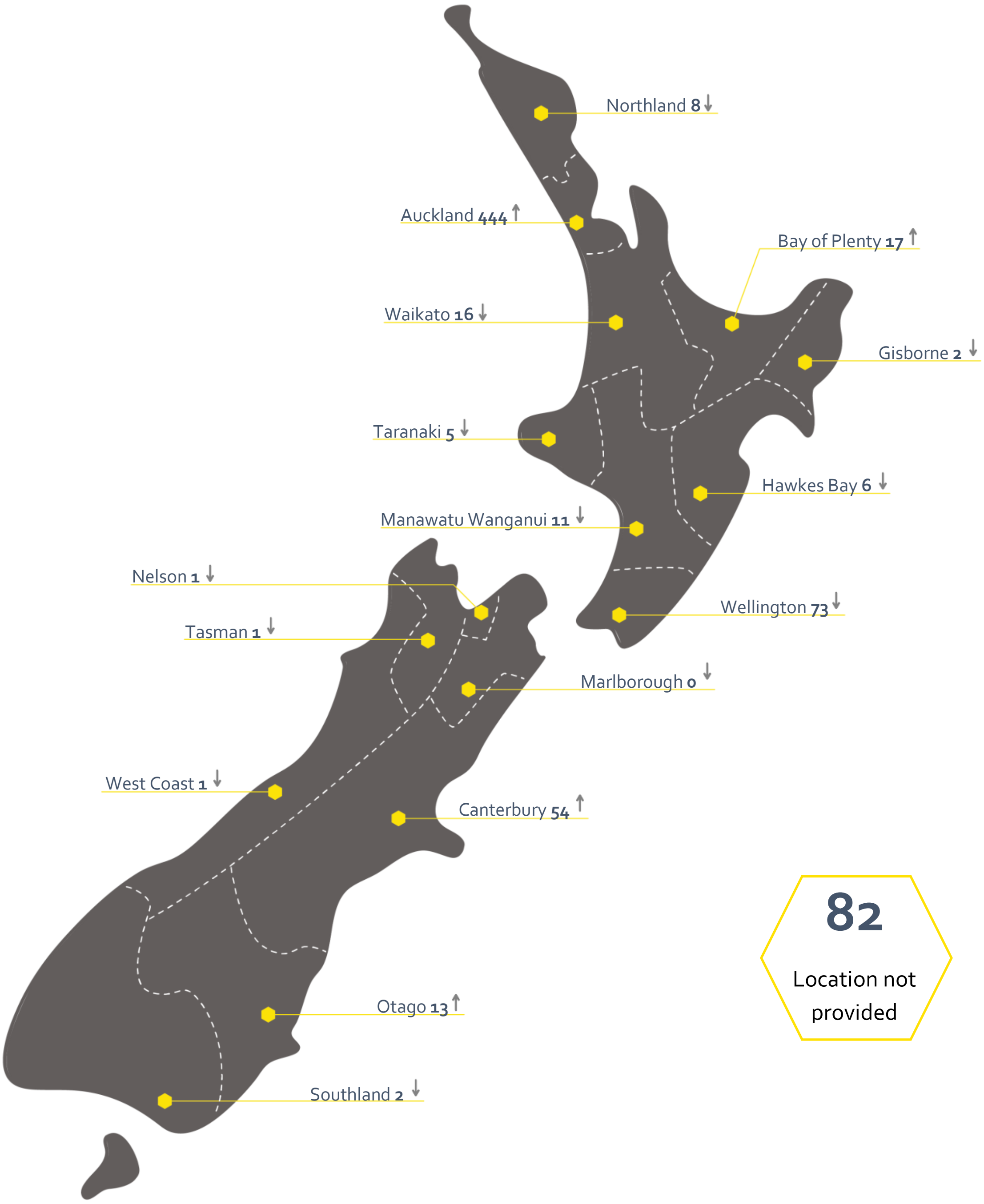
Figure 10: Breakdown by sector and incident category



Reporting by region

Incidents reported in Auckland increased by 56%, Bay of Plenty increased by 18%, Canterbury increased by 15%, and Otago increased by 8%. The number of incidents where a location was not provided includes reports for locations outside New Zealand.

Figure 11: Breakdown by region



82

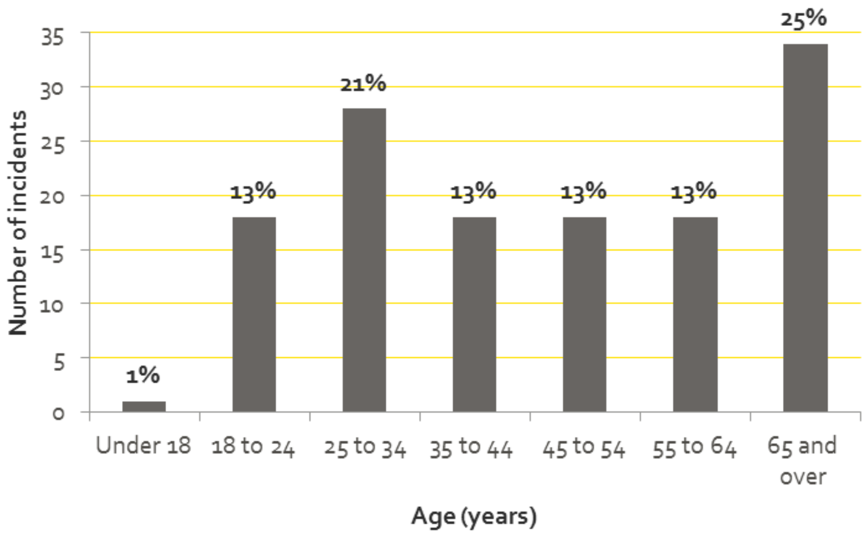
Location not provided

Reporting by age

Of the 229 incidents reported about individuals, 59% provided their date of birth. The 65 and over age range represents a quarter of these reports.

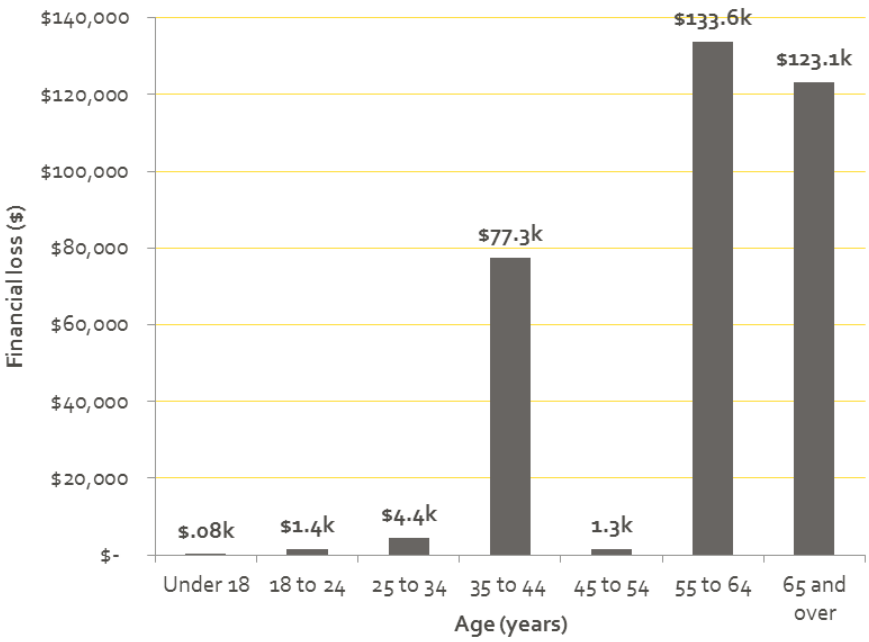
The spread of affected age ranges is broadly similar to the last quarter.

Figure 12: Reports about individuals; breakdown by age



The loss amounts for all age groups are down on last quarter except for those aged 35-44. The losses for those aged 55 and over represents 75% of the value of direct losses reported by individuals[2]. This is consistent with the trend seen in Q1 2018.

Figure 13: Distribution of direct financial loss reported by age



[2] Where a date of birth was provided

For the 60 incidents about individuals with a date of birth and loss amount provided, the average loss was $2528 and the median low was $145.

Table 3: Distribution of direct financial loss reported by age

Under 18	18 - 24	25 -34	35 - 44	45 - 54	55 - 64	65 and over
$80	$1,413	$4,390	$77,336	$1,358	$133,619	$123,147

6. About CERT NZ

CERT NZ is a specialist cyber security unit and part of the Ministry of Business, Innovation and Employment (MBIE). We gather information on cyber security threats and incidents in New Zealand and overseas, advising organisations of all sizes and the public on how to avoid and manage cyber security risks.

A word about our information

Reporting quarters are based on the calendar year, 1 January to 31 December.

Incidents are reported to CERT NZ by individuals and organisations. They choose how much or little information they feel comfortable providing, often about very sensitive incidents.

Sometimes CERT NZ may ask for additional information about an incident to gain a better understanding, or we might need to do technical investigations. Before sharing specific details about an incident, CERT NZ will seek the reporting party's consent.

CERT NZ is not always able to verify the information we receive, though we endeavour to do so, particularly when dealing with significant cyber security incidents.

All information provided to CERT NZ is treated in accordance with our Privacy and Information statement published on our website and this report is subject to the CERT NZ standard disclaimer.

The sectors we use are based on the Stats NZ New Zealand Industry Standard Industry Output Categories.

Our region reporting uses the sixteen regions of the Local Government Act 1974.

Age is calculated from the date of birth provided and the date we received the incident report from an individual. The reporting by age data does not include reported vulnerabilities, as those are from individuals proactively reporting issues, rather than having been affected by them.

Reporting an incident to CERT NZ

Anyone can report a cyber security incident to CERT NZ, from IT professionals and security personnel to members of the public, businesses and government agencies. We also receive incident notifications from our international CERT counterparts when they identify affected New Zealand organisations in their investigations.

To report a cyber security incident, go to our website www.cert.govt.nz or call our freephone number 0800 CERT NZ (0800 2378 69). Your report will be received by an expert who can advise you on next steps.

With your permission, we may refer incidents to our partners such as the National Cyber Security Centre for national security threats, NZ Police for cybercrime, the Department of Internal Affairs for unsolicited electronic mail (spam), and Netsafe for cyberbullying.

Incident categories we use

We use broad categories to group incident reports - over time we will refine these categories to a more granular level as the data set grows.

The **incident** report categories are:

Malware - Short for malicious software. Malware is designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Commonly includes computer viruses, worms, Trojan horses, spyware and adware.

Ransomware - A common malware variant, with a specific purpose. If installed (usually by tricking a user into doing so, or exploiting a vulnerability) ransomware encrypts the contents of the hard drive of the computer it is installed on, and demands the user pay a ransom to recover the files.

Phishing and credential harvesting - Types of email, text or website attacks designed to convince users they are genuine, but they are not. They often use social engineering techniques to convince users of their authenticity and trick people into giving up information, credentials or money.

Unauthorised access (successful) - Successful unauthorised access can enable an attacker to conduct a wide range of malicious activities on a network, infrastructure or computer. These activities are generally categorised by the three types of impact:

- Compromise of confidentiality of information
- Improper modification affecting the integrity of a system
- Degradation or denial of access or service affecting its availability

Scams and fraud - Computer enabled fraud that is designed to trick users into giving up money. This includes phone calls or internet pop-up adverts designed to trick users into installing fake software on their computers.

Denial of service (DoS) - An attack on a service, network or system from a single source that floods it with so many requests that they become overwhelmed and are either stopped completely or operate at a significantly reduced rate. Assaults from multiple sources are referred to as Distributed Denial of Service attacks (DDoS).

Website compromise - The compromise, defacement or exploitation of websites by attackers for malicious purposes, such as spreading malware to unsuspecting visitors.

Botnet traffic - Botnets are networks of infected computers or devices that can be remotely controlled as a group without their owners' knowledge and are often used to perform malicious activities such as sending spam, or launching Distributed Denial of Service attacks.

Suspicious network traffic - Detected attempts to find insecure points or vulnerabilities in networks, infrastructure or computers. Threat actors typically conduct a range of reconnaissance activities before conducting an attack, which are sometimes detected by security systems and can provide early warning for defenders.

C & C server hosting - a system used as a command-and-control point by a botnet.

Reported vulnerabilities - Weaknesses or vulnerabilities in software, hardware or online service, which can be exploited to cause damage or gain access to information. They are reported to CERT NZ under our Coordinated Vulnerability Disclosure (CVD) service.

Vulnerability categories we use

The **vulnerability** report categories we currently use are:

Websites or webservers - Includes vulnerabilities in websites themselves, or the infrastructure they run on. An example would be unpatched websites or webservers which would potentially give an attacker the ability to compromise a website.

Servers (other than websites) - Other kinds of enterprise servers organisations would typically use, such as mail, application and proxy servers. Vulnerabilities can be found in the hardware or firmware, and also arise from misconfiguration or failures in security management.

Networking - Covers vulnerabilities in network equipment, such as routers, gateways and firewalls, or the software and tools used to manage networks. This also includes vulnerabilities which may exist in routing, which could expose network traffic to compromise.

Applications or software - Vulnerabilities discovered in software products which could be exploited by a potential attacker. They are relatively common and when discovered are typically patched or mitigated through controls.

Operating systems or platforms - Low level software which provides, or supports, the basic operating environment of a computer.

PCs and laptops - Desktop and laptop computer hardware.

Mobile devices - Includes phones, handheld devices, hardware and mobile operating systems.

Printers, webcams and other peripherals - Hardware components used to support PC or laptop functions.

IOT devices - Internet connected devices used to perform distributed functions over a network.

Authentication, authorisation and accounting – common terminology for controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to account for services. Vulnerabilities, if exploited to disrupt these functions, would have considerable impacts on the security of a network, system or device.

Human introduced - Vulnerabilities which arise from human introduced errors, misconfiguration or unintentional circumvention of security controls.