certnz

Quarterly Report:
Data Landscape

Q1

1 January – 31 March
2018

/// 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 January 2018 – 31 March 2018.

This quarter we have produced two new reporting documents: this document, the CERT NZ Quarterly Report: Data Landscape, provides graphs and information about the incident reports we received. It 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 https://www.cert.govt.nz/about/quarterly-report/.

2. Incidents and referrals

Incident summary

Between 1 January and 31 March 2018, 506 incidents were reported to CERT NZ. This is up 34% from the previous quarter (from 377).

Of the 506 incidents reported, nearly 36% (182) were referred to NZ Police, up 26% from last quarter.

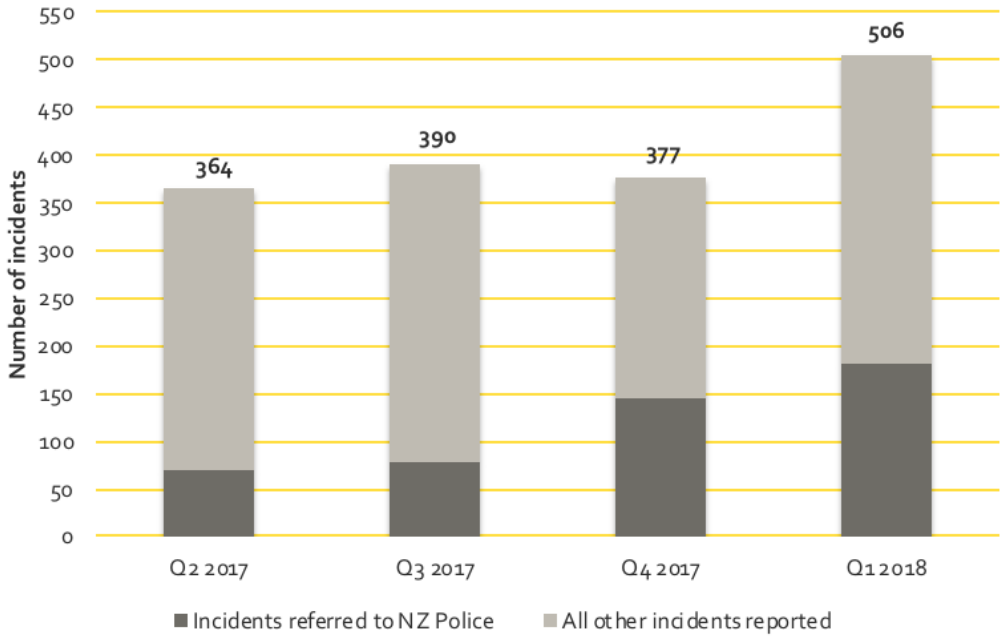
Table 1: Incident partner referrals

506 incidents reported	
318	responded to directly by CERT NZ
182	referred to NZ Police
5	referred to Netsafe
0	referred to National Cyber Security Centre
1	referred to Department of Internal Affairs

Another 67 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

Figure 1: Number of incidents reported by quarter



3. Reporting by incident category

Breakdown by category

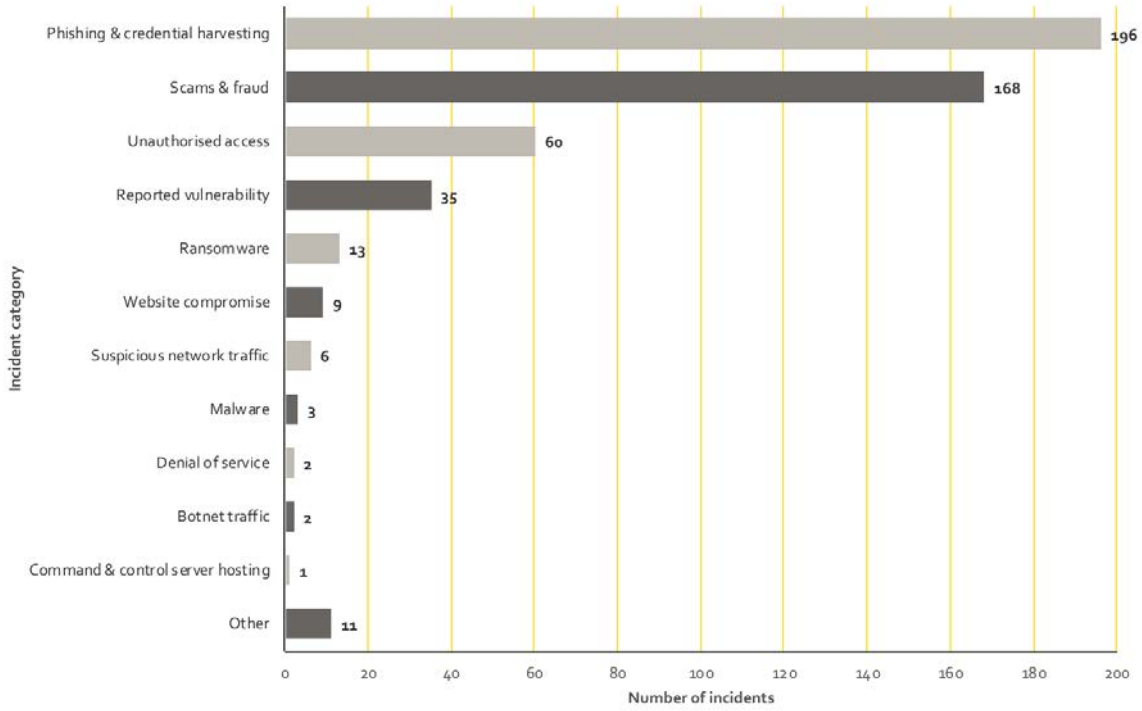
Phishing & credential harvesting reports increased by over 50% from last quarter to 196. Increased cooperation with New Zealand based banks and financial services organisations has contributed to the jump. CERT NZ's Quarterly Report: Highlights has more information on what CERT NZ is doing to disrupt phishing activity in New Zealand.

Scam & fraud reports continue to grow, up 21% from last quarter to 168, reflecting the prevalence of these in the community.

Compared to the last quarter, changes in the types of incidents reported include a:

- 67% increase in unauthorised access incidents from 36 to 60
- 133% increase in vulnerability reports from 15 to 35
- a decrease in malware reports from 29 to 3.

Figure 2: Breakdown by incident category

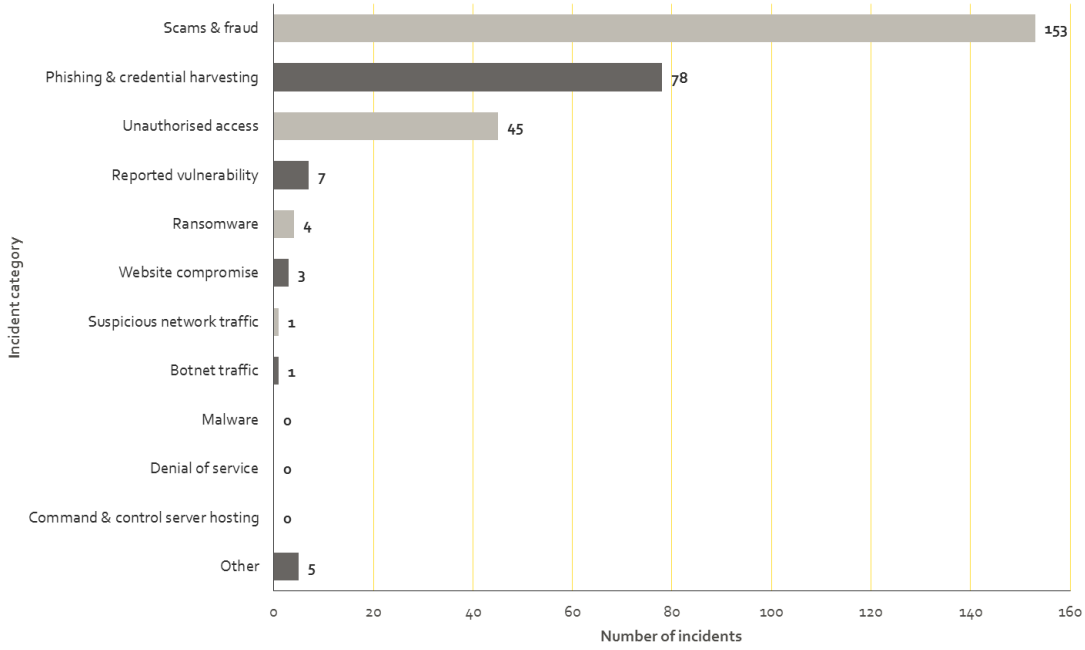


CERT NZ's Q1 2018 Quarterly Report: Highlights available on www.cert.govt.nz provides more information about the vulnerability reports received.

Breakdown of incidents about individuals

297 (59%) of incidents reported were about individuals.

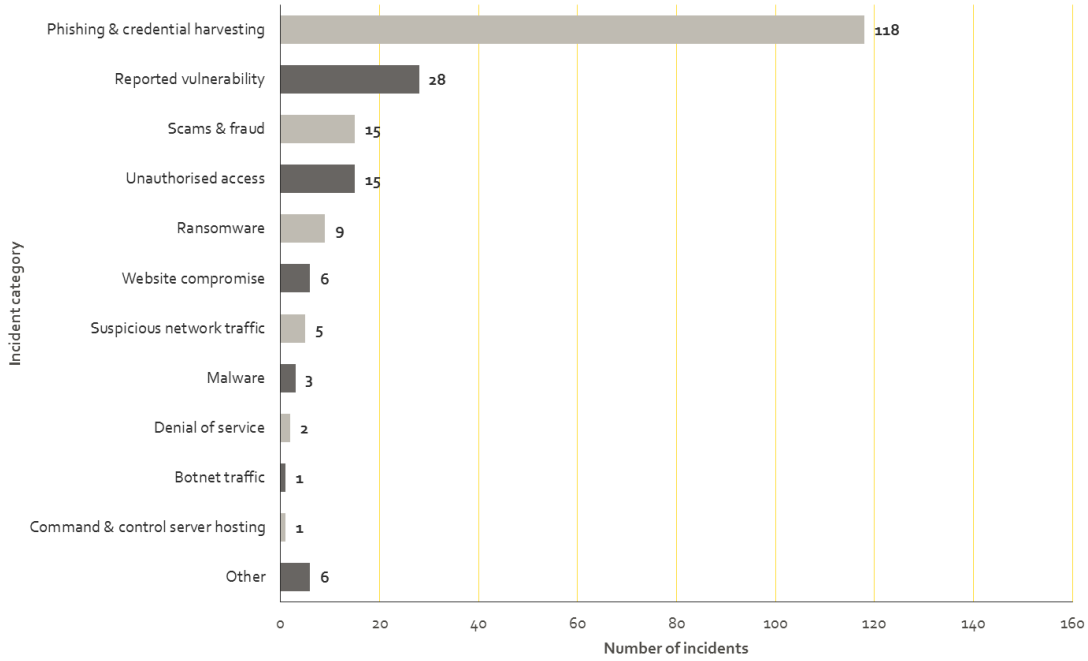
Figure 3: Breakdown of incidents about individuals



Breakdown of incidents about organisations

209 (41%) incidents reported were about organisations.

Figure 4: Breakdown of incidents about organisations

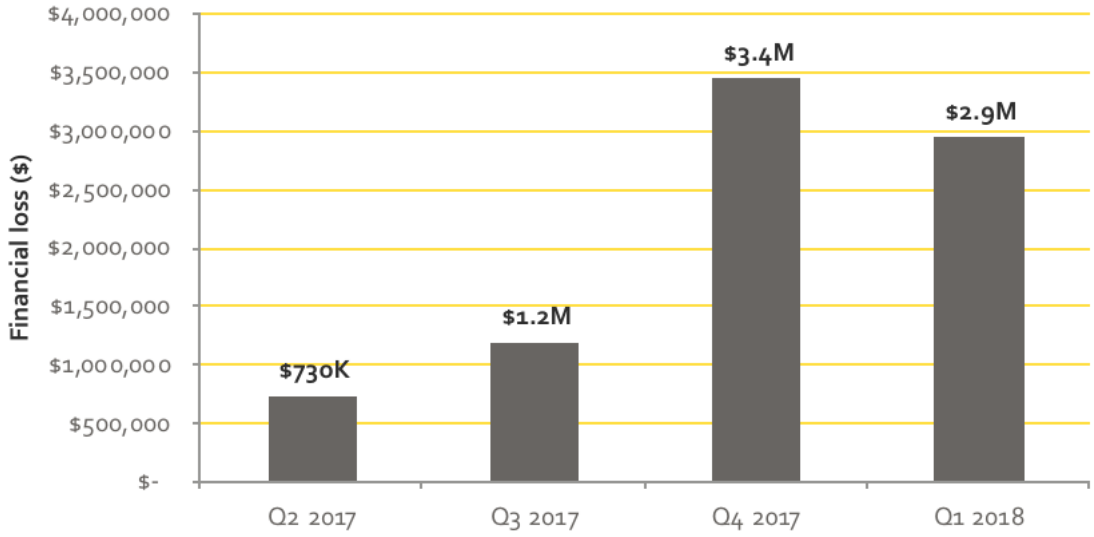


4. Impacts

Total financial losses

In this quarter, direct financial losses totaled $2,936,962. This is already more than half of the total financial losses reported in 2017 of $5.3million.

Figure 5: Direct financial losses per quarter



Distribution of financial loss

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

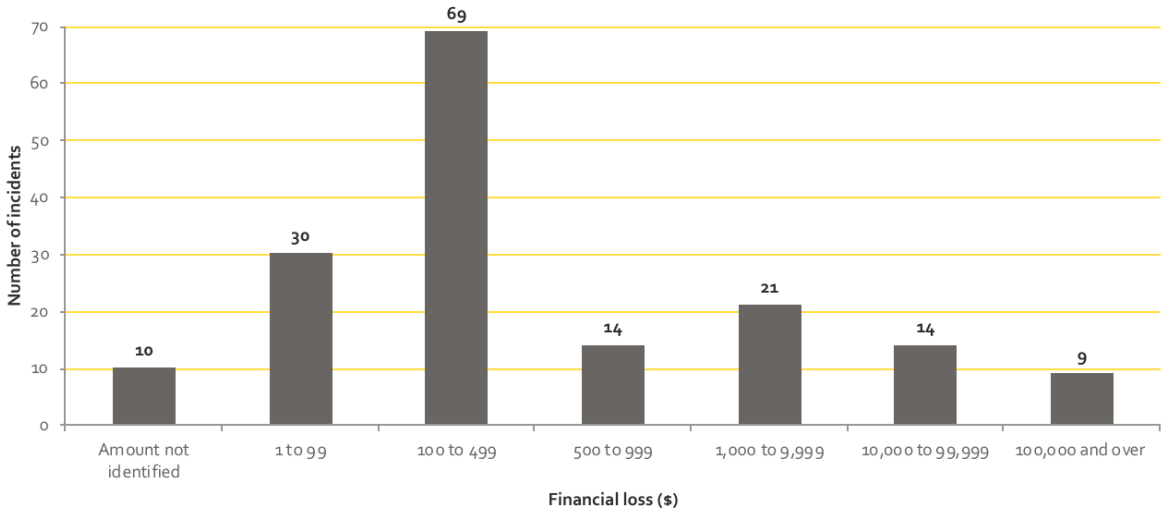
- organisations reported $728,318 (25% of all direct financial loss)
- individuals reported $2,208,644 (75% of all direct financial loss)

During this quarter, nine incidents involved losses of $100,000 or more, a total of $2,387,671. Of these nine incidents:

- 8 involved scams & fraud, including 4 invoice scams affecting businesses
- 1 involved unauthorised access.

The percentage of incidents reporting direct financial loss was 33% (167), about the same as last quarter (34%).

Figure 6: Distribution of direct financial loss



Types of loss

Overall, 45% of incidents reported some type of loss. Note that some reports include multiple types of loss.

Of the 297 incidents reported about individuals, 60% (177) involved some type of loss. Of the 209 incidents reported about organisations, 23% (49) involved some type of loss.

Losses experienced are broken down by type as follows:

Table 2: Types of loss

33% **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 (Q4 2017: 34%).

2% **Reputational loss:**

Damage to the reputation of an individual or organisation as a result of being the victim of an incident (Q4 2017: 1%).

6% **Data loss:**

Loss or unauthorised copying of data, business records, personal records and intellectual property (Q4 2017: 4%).

3% **Technical damage:**

Impacts on services like e-mail, phone systems or websites, resulting in disruption to a business or organisation (Q4 2017: 1%).

3% **Operational impacts:**

The time, staff and resources that need to be spent on recovering from an incident, taking people away from normal business operations (Q4 2017: 2%).

4% **Other:**

Includes types of loss not covered in the other categories (Q4 2017: 6%).

5. Demographics

Reporting by sector

Of the 209 incidents reported about organisations, the three sectors with the most reports were:

- Finance and insurances services 92 (44%)
- Technology 24 (11%)
- Public administration and safety 19 (9%)

Figure 7: Reports about organisations; breakdown by sector

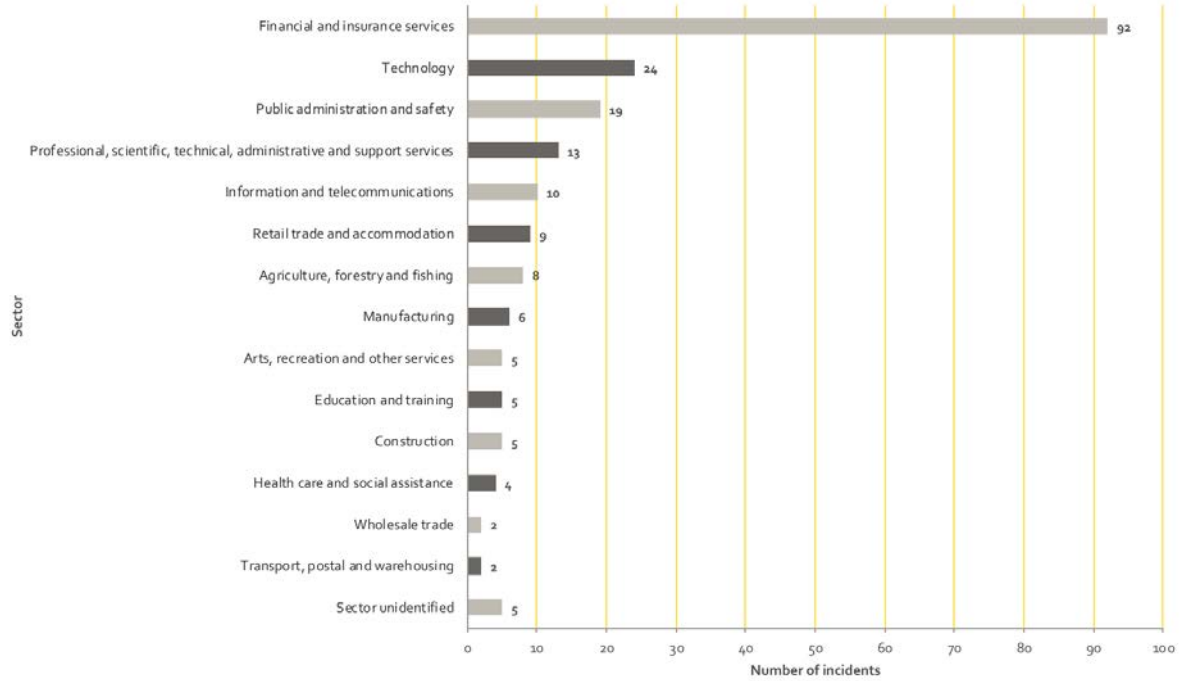
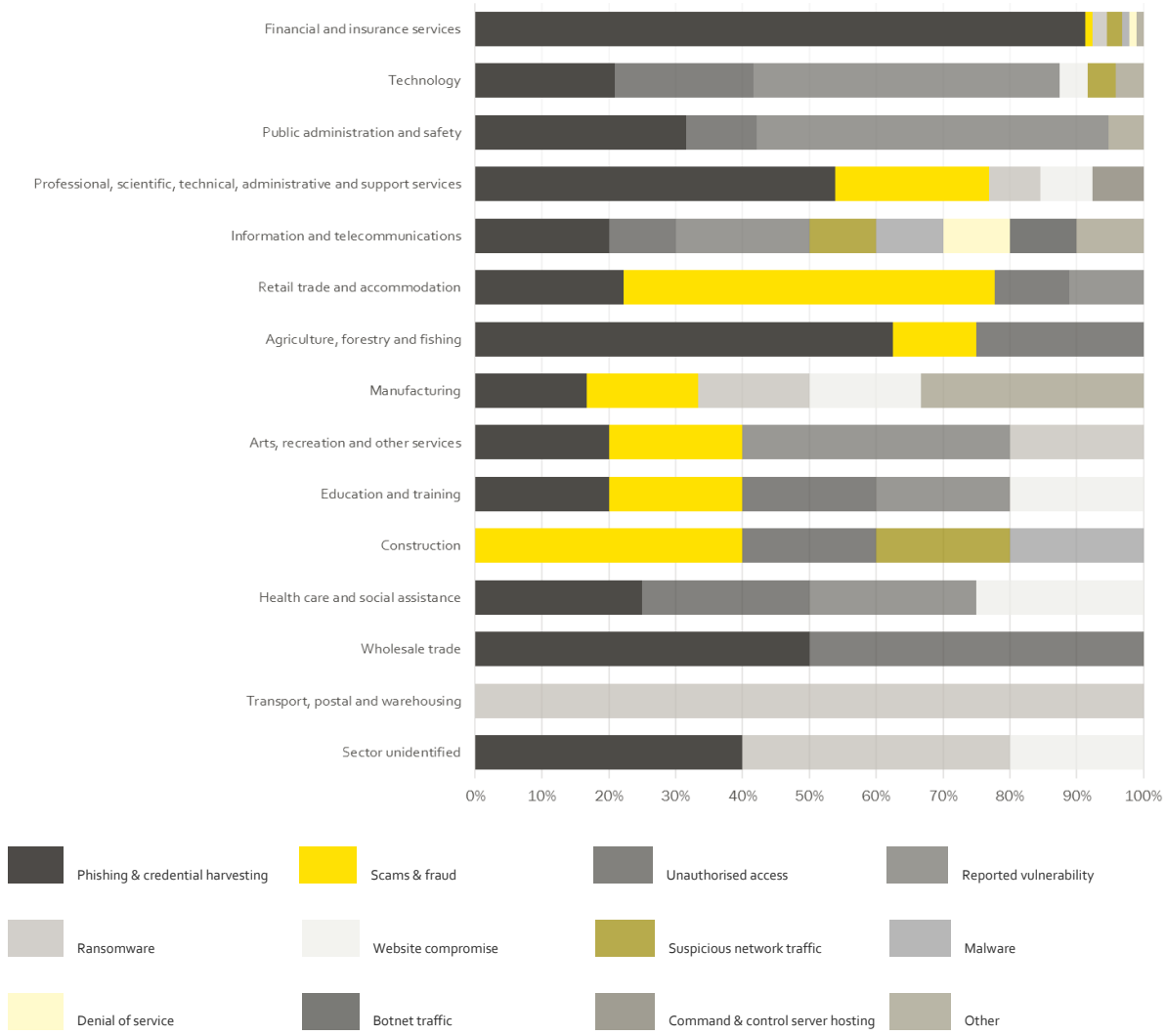


Figure 8: Breakdown by sector and incident category



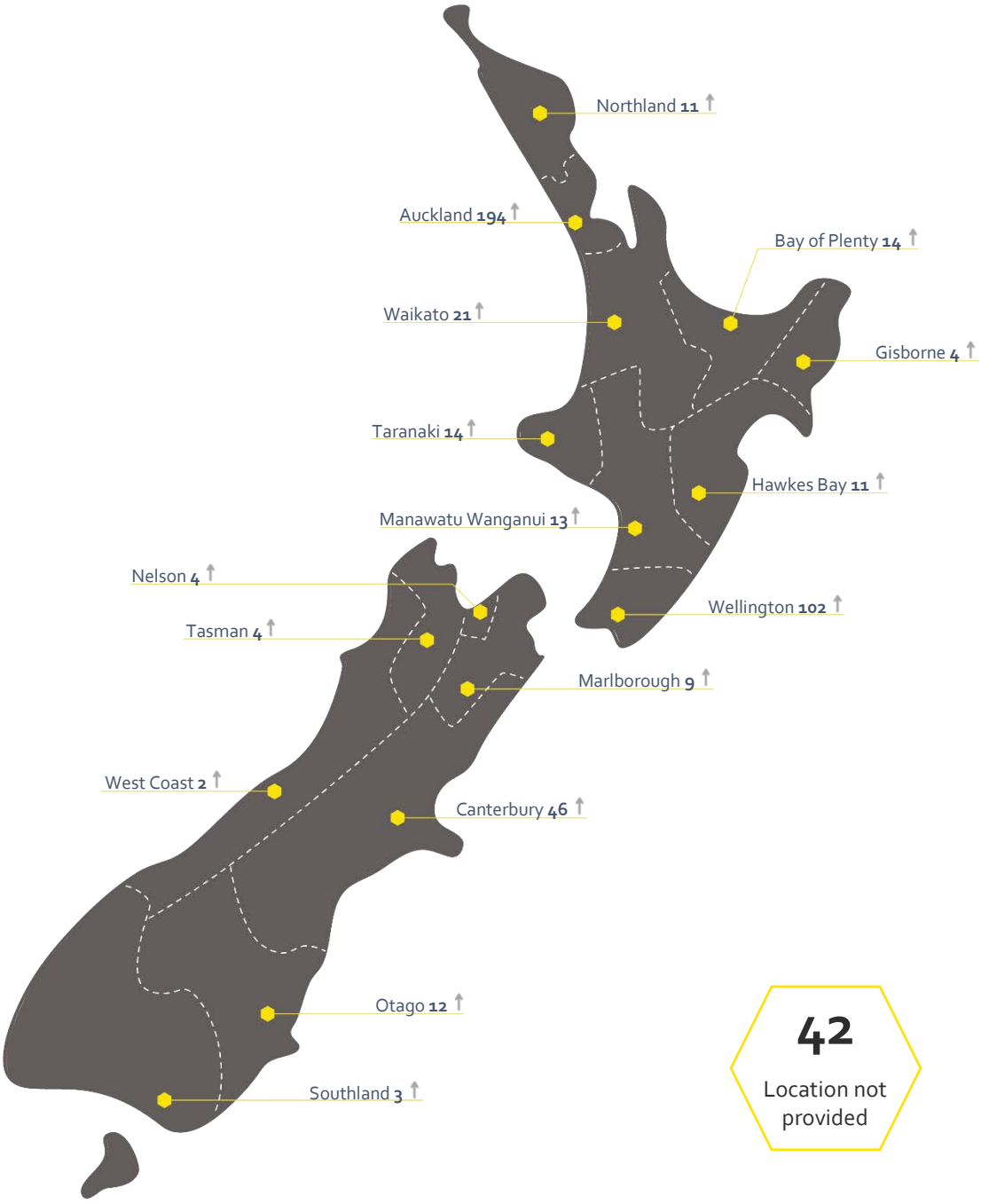
All sectors have reported phishing other than construction and transport, and postal and warehousing.

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

Reporting by region

Incidents reported increased across every region in New Zealand compared to last quarter.

Figure 9: Breakdown by region

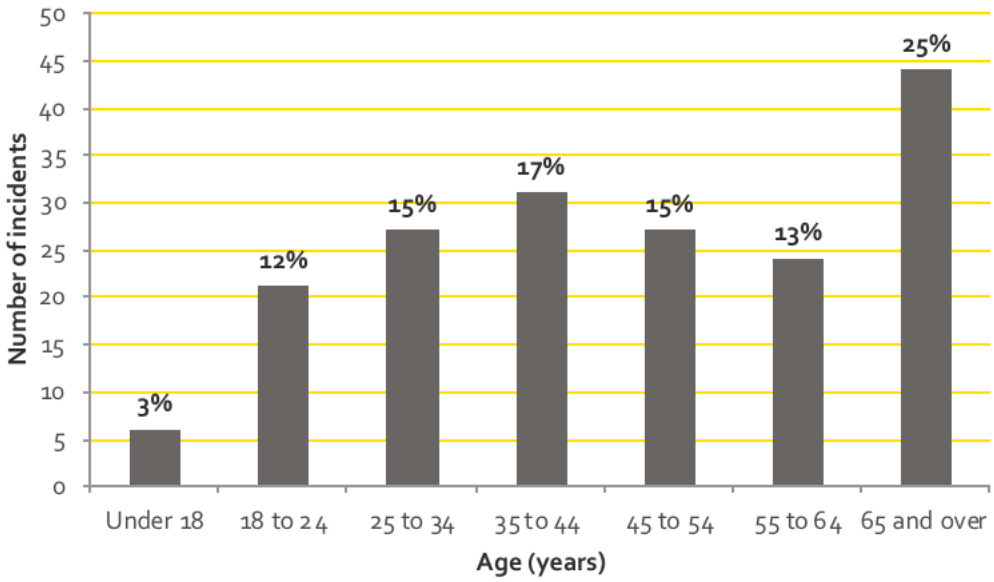


Reporting by age

Of the 297 incidents reported about individuals, 61% provided their date of birth. Of these, the age range with the most incidents reported was 65 years and over (25% : 44 incidents).

The spread of affected age ranges overall shows that New Zealanders of all ages are being targeted by cyber security threats.

Figure 10: Reports about individuals; breakdown by age



Whilst all age groups experienced incidents, those 55 and over experienced the highest value of direct financial loss. Nearly 90% of the value of direct financial losses reported by individuals who provided their age came from people who were 55 or over.

Figure 11: Distribution of direct financial loss reported by age

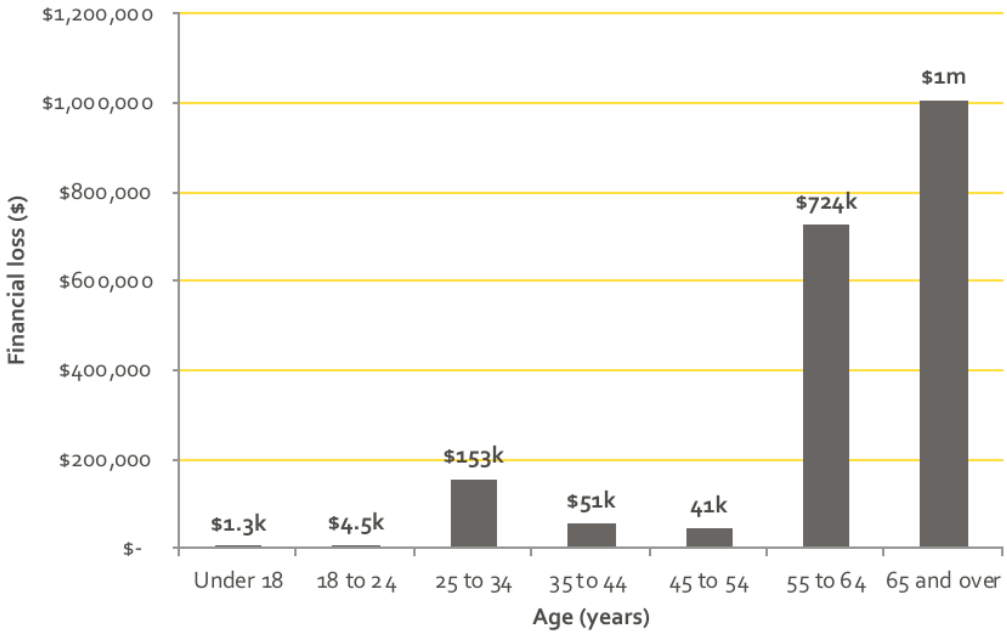


Table 3: Distribution of direct financial loss reported by age

Under 18	18 - 24	25 -34	35 - 44	45 - 54	55 - 64	65 and over
$1,365	$4,511	$153,784	$51,891	$41,309	$724,552	$1,005,147

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 Department of Internal Affairs for unsolicited electronic mail (spam), the National Cyber Security Centre for national security threats, Netsafe for cyberbullying, and NZ Police for cybercrime.

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 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.