certnz

Quarterly Report: Data Landscape

Q4 2019

1 October – 31 December, 2019

New Zealand Government

Contents

1. Introduction

The CERT NZ Quarterly Report: Data Landscape for Q4 2019 provides a standardised set of results and graphs for the quarter, and an analysis of the latest trends. Analytical comment is provided where meaningful or interesting trends were identified.

The report covers the quarter from 1 October – 31 December 2019, and is supplemented by the:

- CERT NZ Quarterly Report: Highlights Q4 2019, providing an overview of the cyber security incidents reported this quarter
- 2019 Report Summary, providing and overview of what we've seen and done in 2019.

All three documents can be found on our website at: https://www.cert.govt.nz/about/quarterly-report/

2. Incidents and referrals

Incident summary

Between 1 October and 31 December 2019, 1197 incidents were reported to CERT NZ.

Of the 1197 incidents reported:

- 1000 (84%) were responded to directly by CERT NZ
- 196 (16%) were referred to New Zealand Police
- 1 (0.1%) was referred to the Department of Internal Affairs (DIA).

This is broadly consistent with Q2 and Q3 2019, except for the single incident reported to the DIA, which represents a significant drop from the 24 referred to DIA in Q3 2019.

Table 1: Incident partner referrals

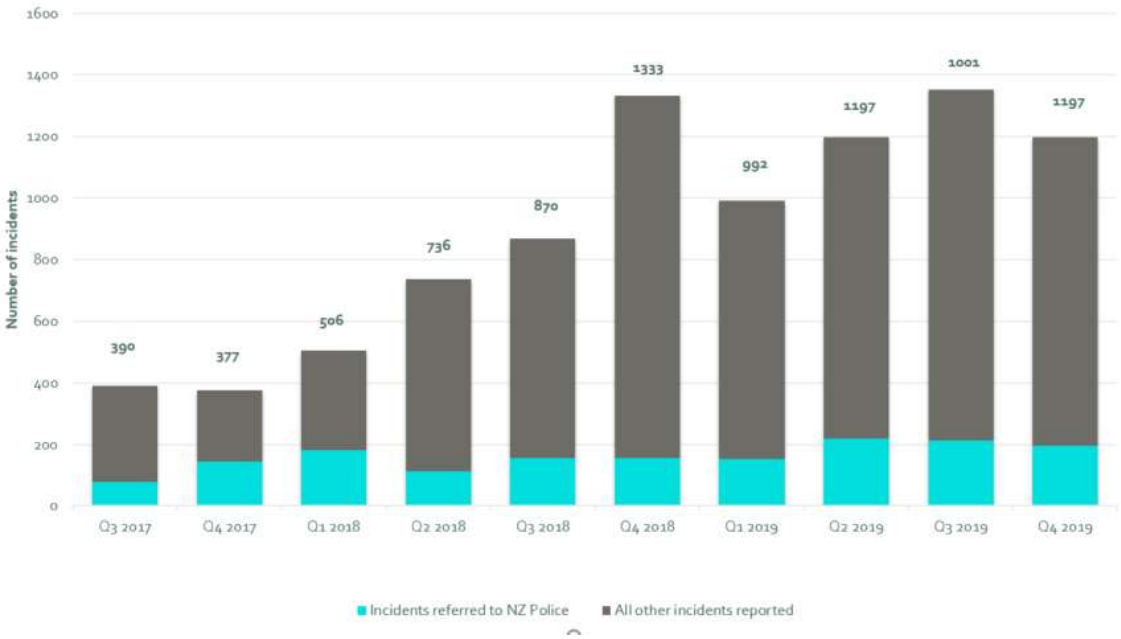
1197 incidents reported	
1000	responded to directly by CERT NZ
196	referred to NZ Police
0	referred to Netsafe
0	referred to National Cyber Security Centre
1	referred to Department of Internal Affairs

Another 218 events were automatically directed to other agencies and not recorded as incidents by CERT NZ. When an incident concerns an issue immediately identifiable as being outside CERT NZ's scope – such as cyber bullying, spam and online child abuse – our online reporting tool directs it to the agency with the necessary expertise to deal with it.

Incidents per quarter

The total number of incidents reported over the year 1 January – 31 December 2019 is 4,740.

Figure 1: Number of incidents reported by quarter



3. Reporting by incident category

Breakdown by category

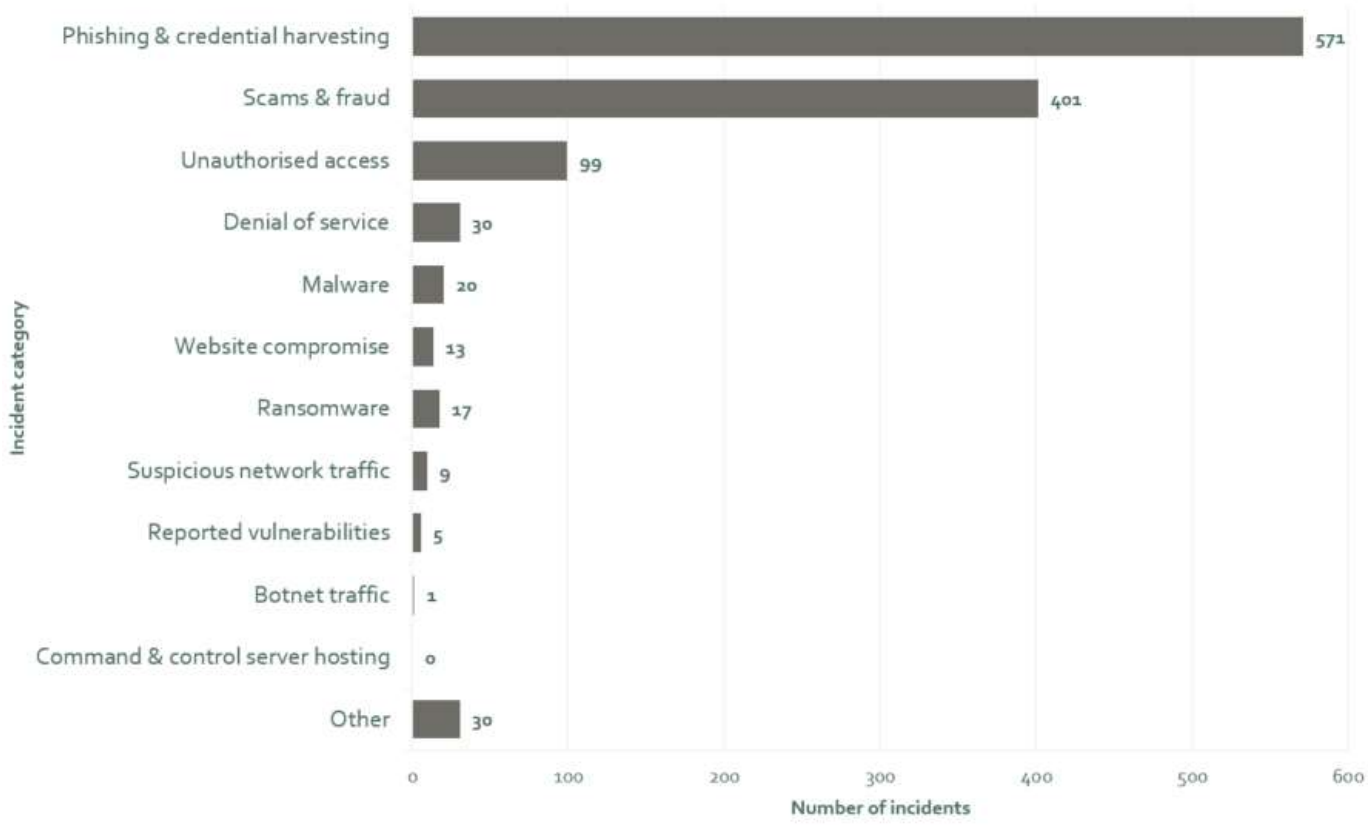
We received 401 reports of scam and fraud incidents, a significant 27% decrease compared to Q3. Reports of phishing and credential harvesting increased 11% on Q3, against a backdrop of lower reporting volumes during Q4.

Notable incident category trends in Q4 include:

- a return to the historical mean of fewer than 10 reports of suspicious network traffic, after peaking in Q2 with 65 incidents reported
- a significant variation in vulnerability reports from quarter to quarter, with just five incidents in Q4, down from 31 in Q2
- an increase in denial of service reports with an average of 22 reported per quarter in 2019, compared with an average of four per quarter reported in 2018.

For more information about the incident reports received, read CERT NZ Quarterly Report: Highlights Q4 2019 on https://www.cert.govt.nz/about/quarterly-report/

Figure 2: Breakdown by incident category



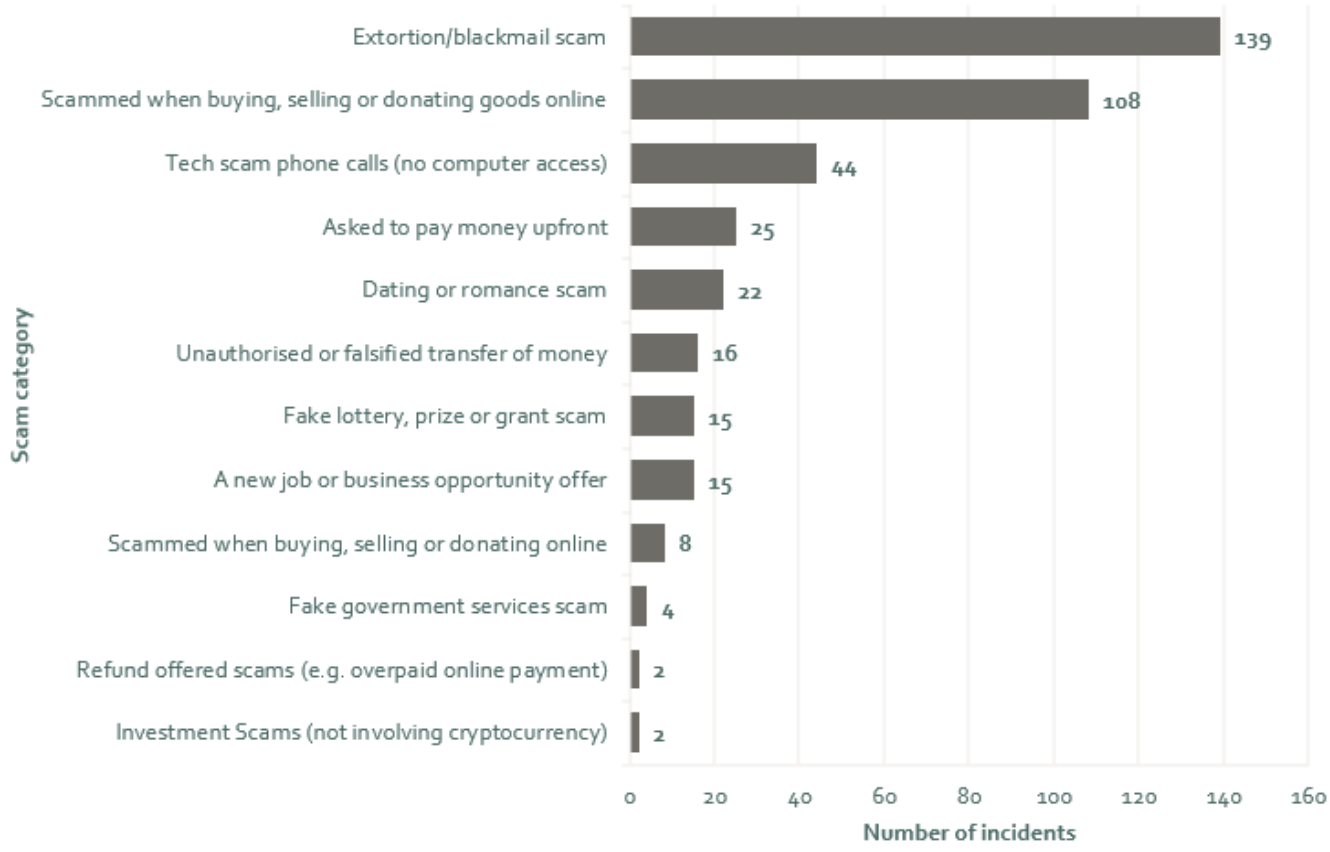
Breakdown of scam and fraud incidents

Of the incidents reported this quarter, 401 (34%) were about scams and fraud. The scam and fraud category consistently accounts for the majority of incident reports received. In Q1 2019, CERT NZ began breaking down scam reports in to sub-categories, to gain further insights into the types of online scams and fraud affecting New Zealanders. The graph below shows the number of reports per sub-category.

As scams and fraud are mostly targeted at financial gain, they account for the highest value of financial losses, with $3,620,000 (77%) of reported losses this quarter. Financial losses can range from small amounts (as with buying or selling online) through to significant amounts (as with investment scams).

Read CERT NZ's Q4 2019 Quarterly Report: Highlights on https://www.cert.govt.nz/about/quarterly-report/ for more information about the incident reports received in this category.

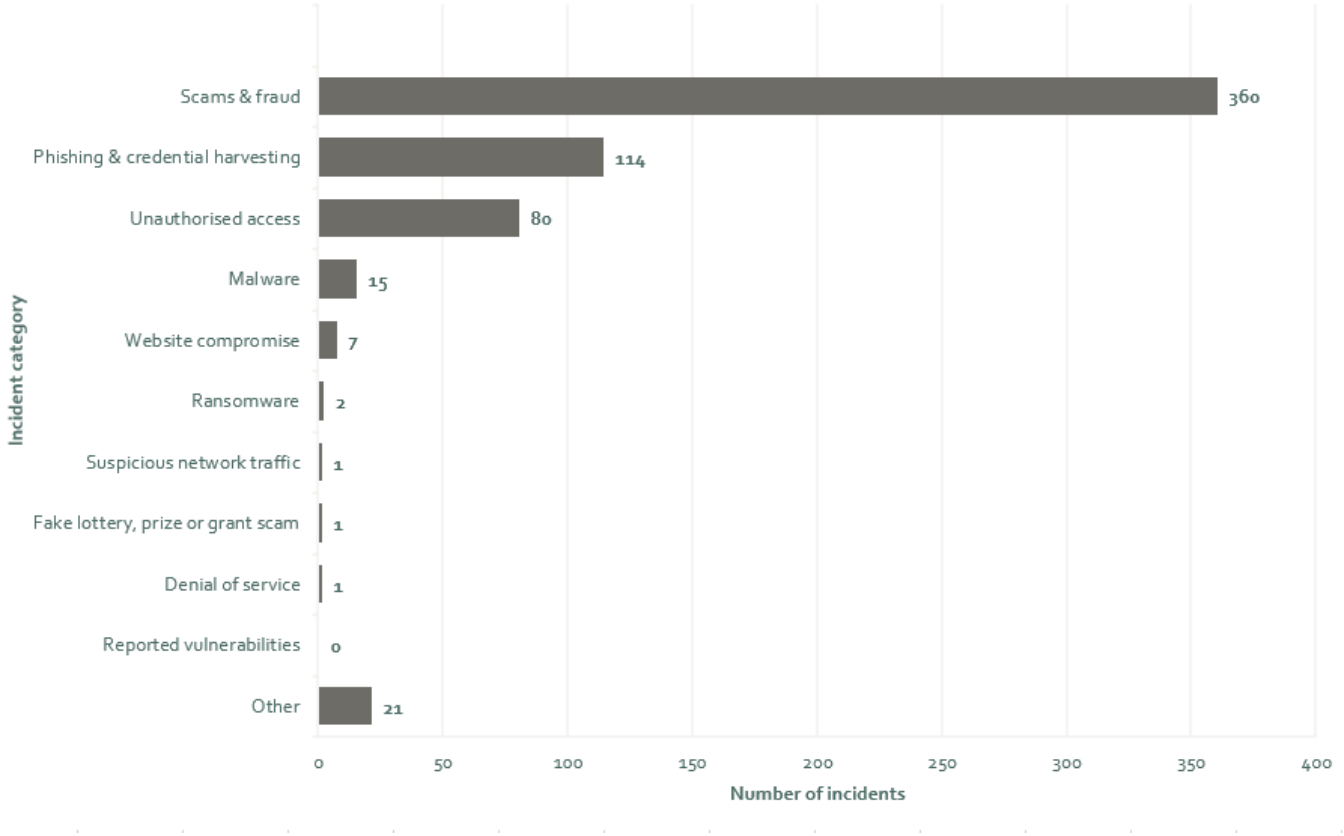
Figure 3: Breakdown of scam and fraud categories



Breakdown of incidents affecting individuals

In Q4, 602 reports (50%) were about incidents affecting individuals, down from 792 (58%) in Q3. This significant decrease in the reporting of incidents affecting individuals is linked to the decrease in the volume of scams and fraud reports, down from 506 in Q3 to 360 in Q4.

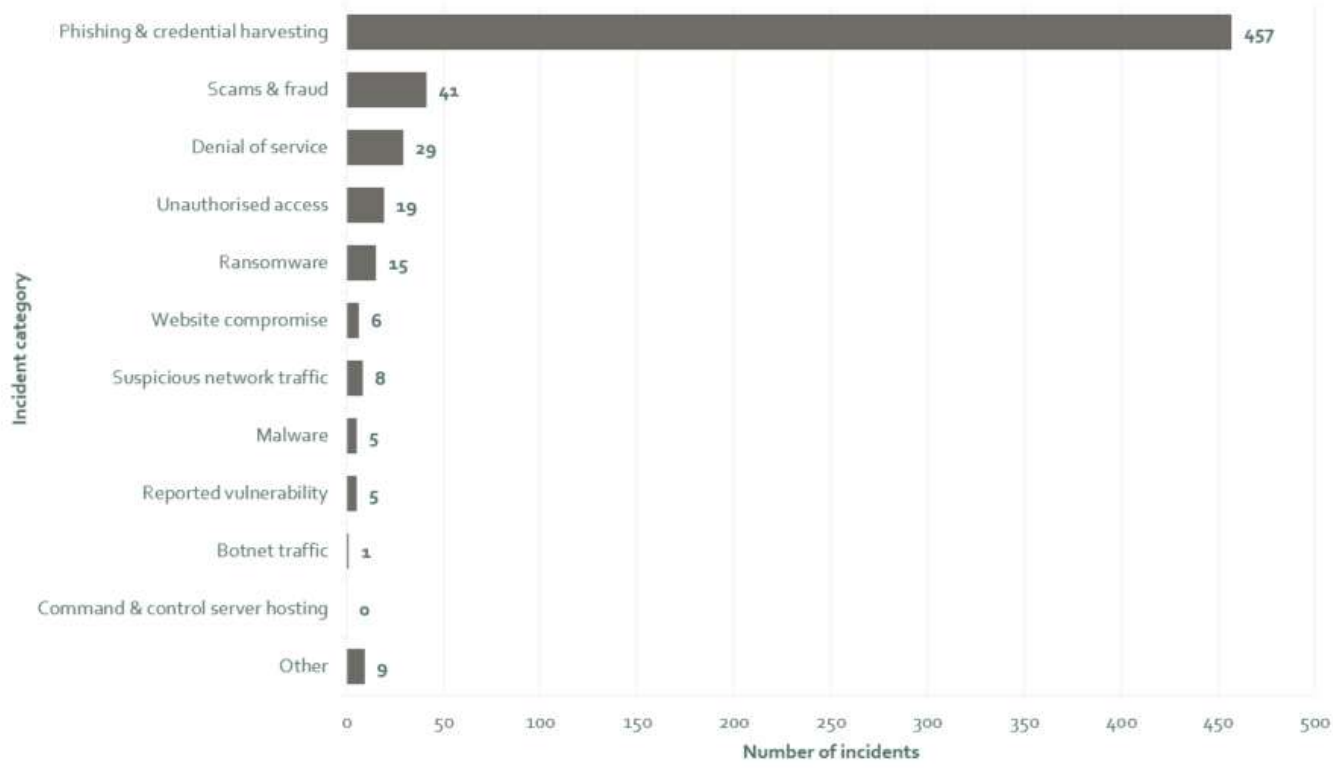
Figure 4: Breakdown of incidents affecting individuals



Breakdown of incidents affecting organisations

Half the reports (595) received in Q4 were about incidents affecting organisations, compared with 42% (562) in Q3. Significantly, Q4 saw a 30% increase in reports of phishing and credential harvesting incidents from organisations, from 352 in Q3 to 457 this quarter.

Figure 5: Breakdown of incidents affecting organisations

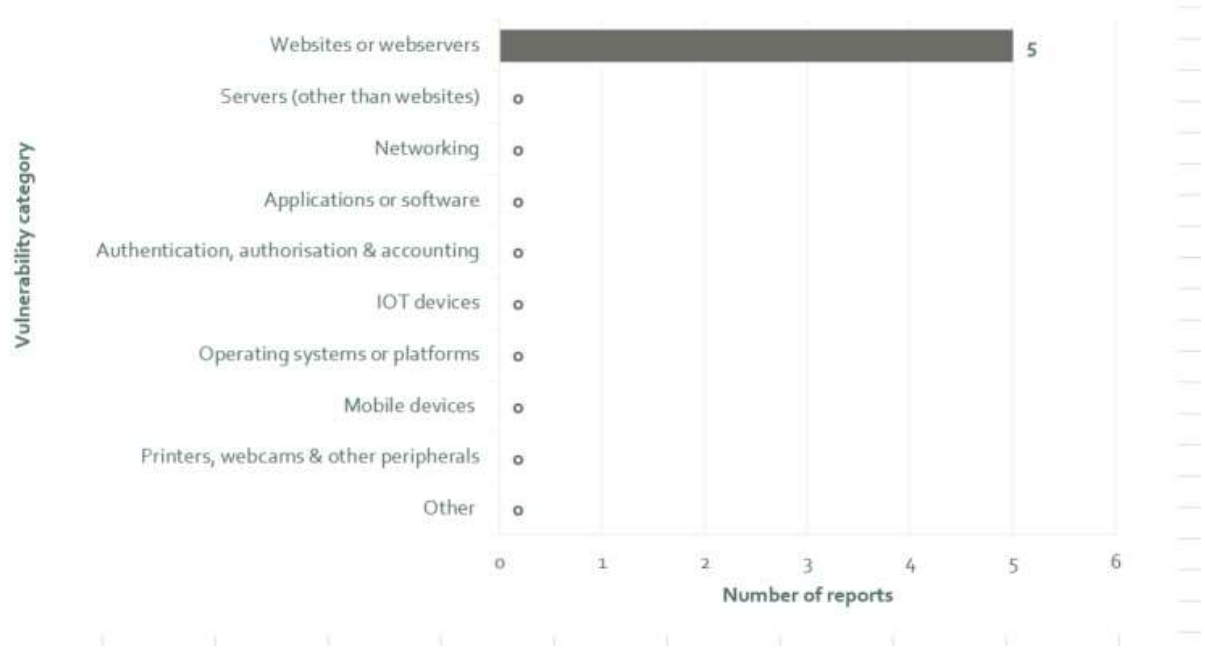


Breakdown of reported vulnerabilities

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

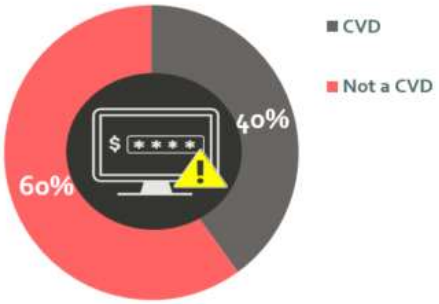
CERT NZ received five vulnerability reports, down from nine in Q3.

Figure 6: 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 two vulnerability reports using the CVD policy[1], making up 40% of the vulnerability reports received in Q4.

Figure 7: Proportion of coordinated vulnerability disclosures

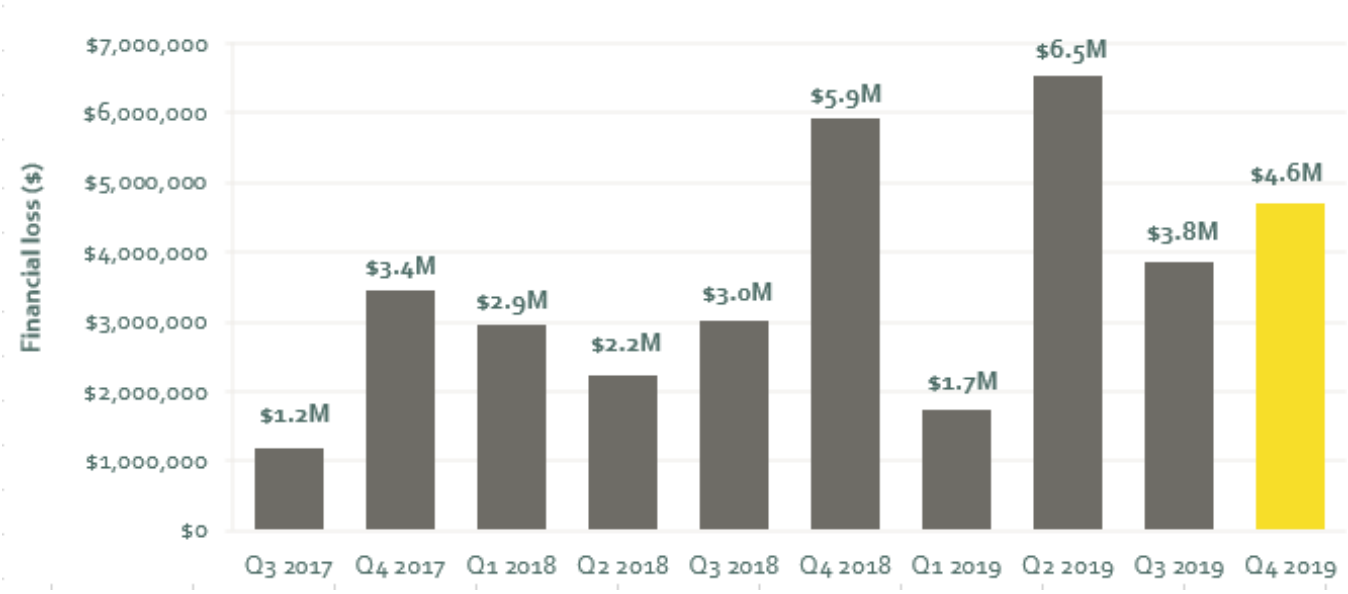


4. Impacts

Direct financial loss

Direct financial losses totalled $4,678,140 this quarter. This is a 22% decrease compared to Q4 2018.

Figure 8: Direct financial losses per quarter



Distribution of direct financial losses

The difference in direct financial losses between reports affecting individuals and those affecting organisations was:

- organisations reported financial losses to the value of $4,089,123 (87% of all direct financial losses)
- individuals reported financial losses to the value of $589,012 (13% of all direct financial losses)

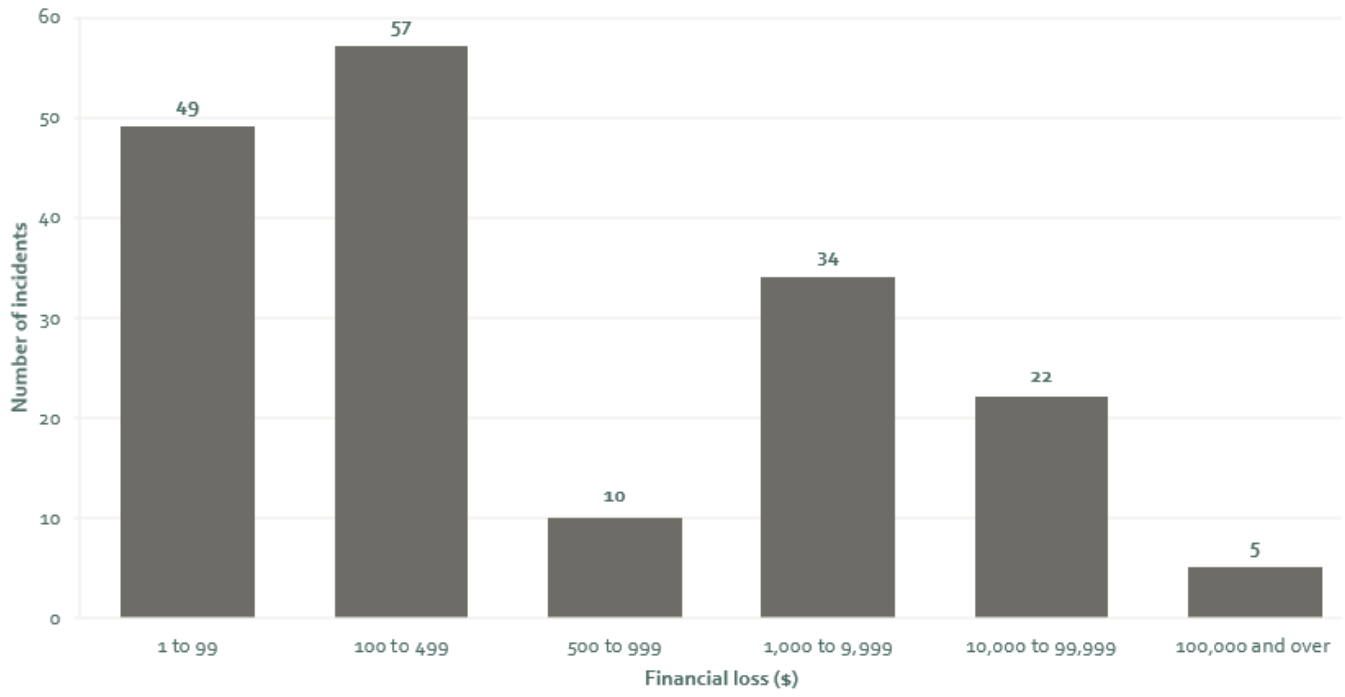
For reports affecting individuals where a date of birth and loss amount was provided, the average amount lost from reported incidents was $3,635, and the average age was 41.

Five incidents reported this quarter involved losses of $100,000 or more, and totalled $3,876,958. Of these five incidents:

- two involved victims being asked to pay money upfront, through the issuing of fake invoices and suchlike
- two involved phishing and credential harvesting, through the unauthorised changing of business payment/invoice details
- one involved unauthorised or falsified transfer of money.

In addition, two reports concerned incidents relating to SIM swap attacks, involving losses in the tens of thousands. CERT NZ has only received one other report of fraud via SIM swap attack this year. Read CERT NZ's Q4 2019 Quarterly Report: Highlights on https://www.cert.govt.nz/about/quarterly-report/ for more information about SIM swap attacks. Similarly to Q3, 15% (177) of all incidents in Q4 reported direct financial loss.

Figure 9: Distribution of direct financial losses



Types of loss

250 (21%) reports received this quarter involved incidents where some type of loss (not only financial) occurred.

Of the 602 reports of incidents affecting individuals, 226 (38%) involved some type of loss. Of the 595 reports of incidents affecting organisations, 24 (4%) involved some type of loss.

Reported losses are broken down by type, as follows:

Table 2: Types of loss

15% **Financial loss**

This not only includes money lost as a direct result of the incident, but also includes the cost of recovery, like the cost of contracting IT security services or investing in new security systems following an incident (Q3 2019: 15%).

1% **Reputational loss**

Damage to the reputation of an individual or organisation as a result of the incident (Q3 2019: 1%).

3% **Data loss**

Loss or unauthorised copying of data, business records, personal records and intellectual property (Q3 2019: 4%).

0% **Technical damage**

Impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation (Q3 2019: 0%).

1% **Operational impacts**

The time, staff and resources spent on recovering from an incident, taking people away from normal business operations (Q3 2019: 0%).

3% **Other**

Includes types of loss not covered in the other categories (Q3 2019: 1%).

5. Demographics

Reporting by sector

Reports from the finance and insurance sector accounted for 58% of the 595 reports about incidents affecting organisations.

Figure 10: Reports by sector

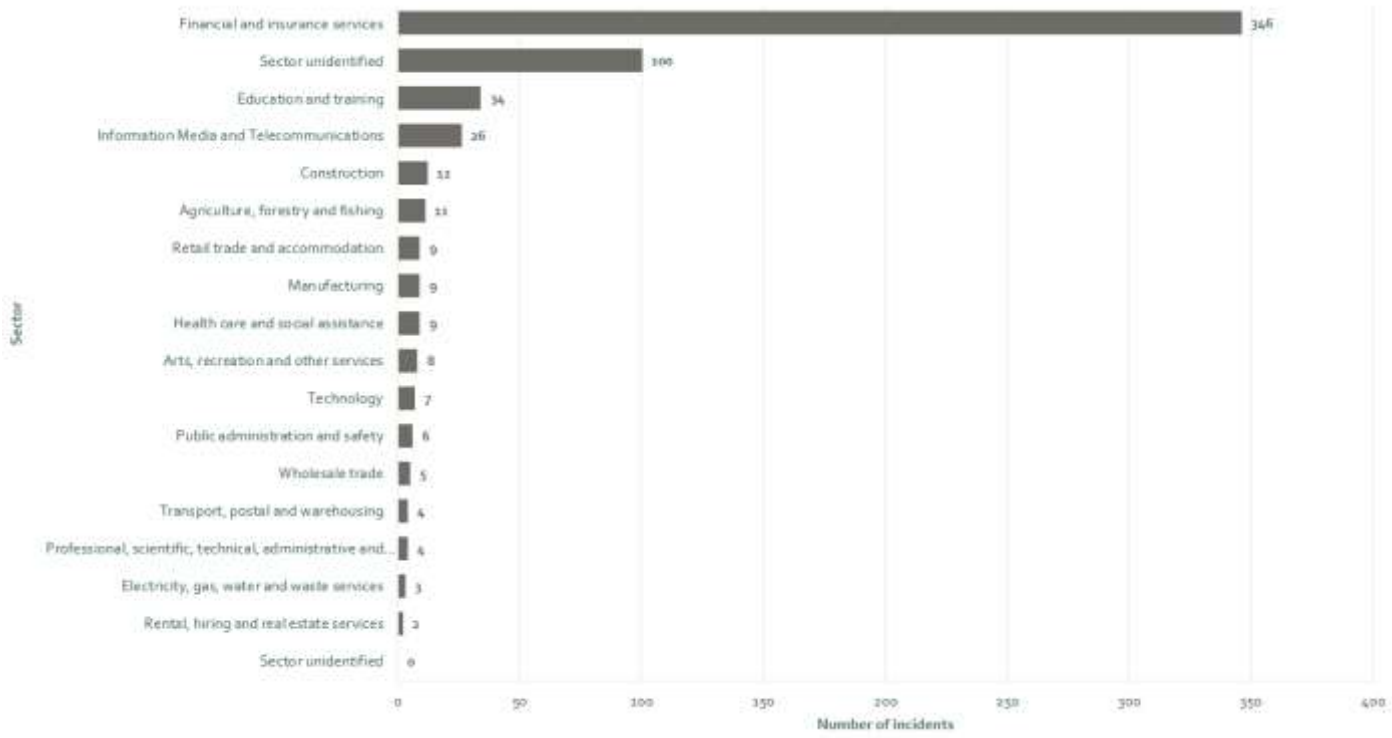
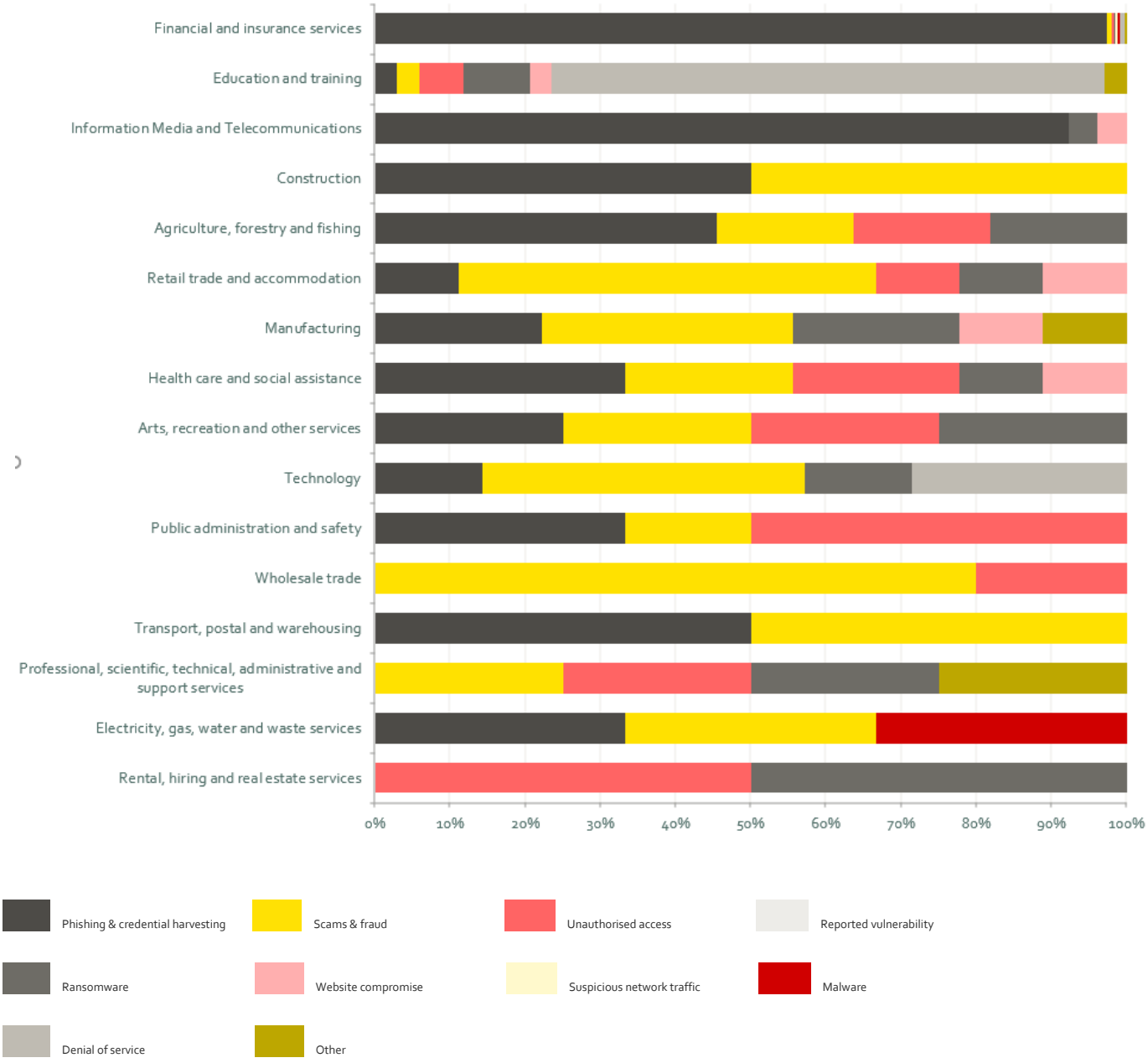


Figure 11: Breakdown by sector and incident category

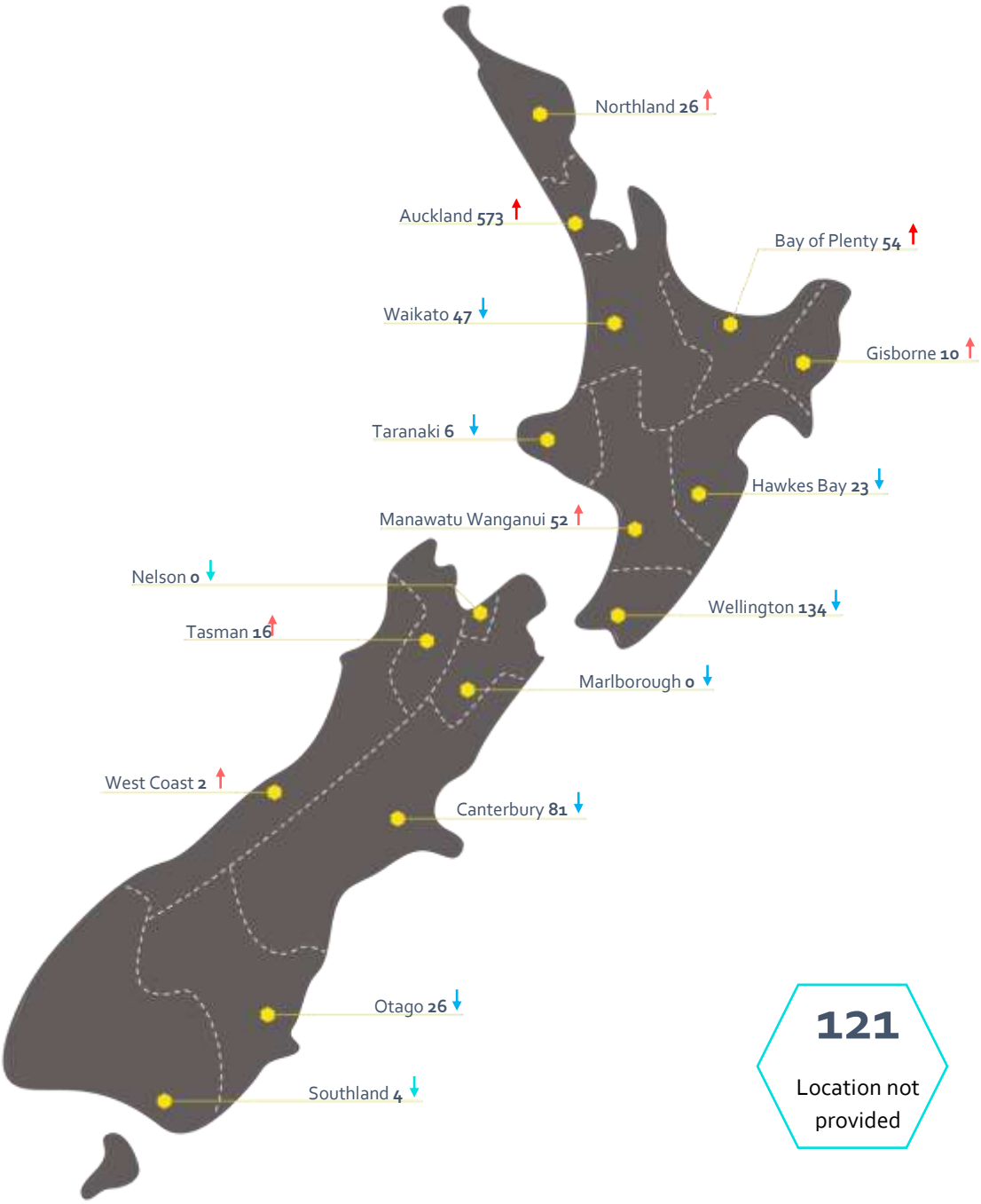
The education and training sector reported 25 (83%) denial of service incidents during Q4. 337 (97%) of the incidents reported by the financial and insurance sector were for phishing and credential harvesting.



Reporting by region

Auckland experienced the largest increase in reported incidents, from 553 in Q3 to 573 in Q4. In comparison, Wellington experienced the largest decrease in incidents, dropping from 196 in Q3 to 134 in Q4.

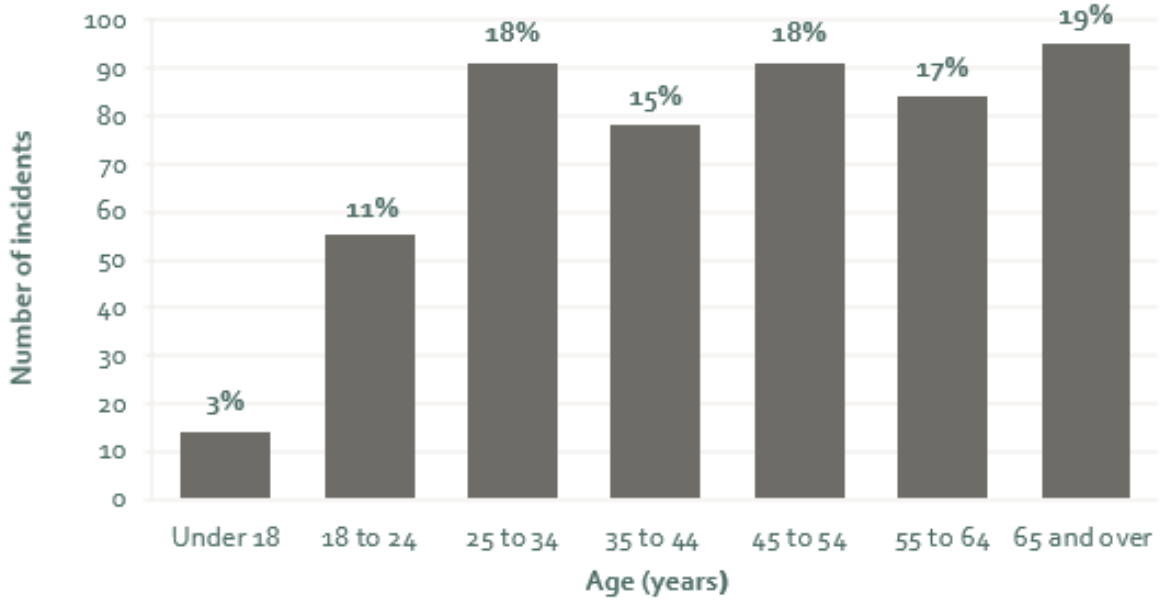
Figure 12: Breakdown of reports by region


Northland 26
Auckland 573
Bay of Plenty 54
Waikato 47
Gisborne 10
Taranaki 6
Hawkes Bay 23
Manawatu Wanganui 52
Nelson 0
Wellington 134
Tasman 16
Marlborough 0
West Coast 2
Canterbury 81
Otago 26
Southland 4
121
Location not provided

Reporting by age

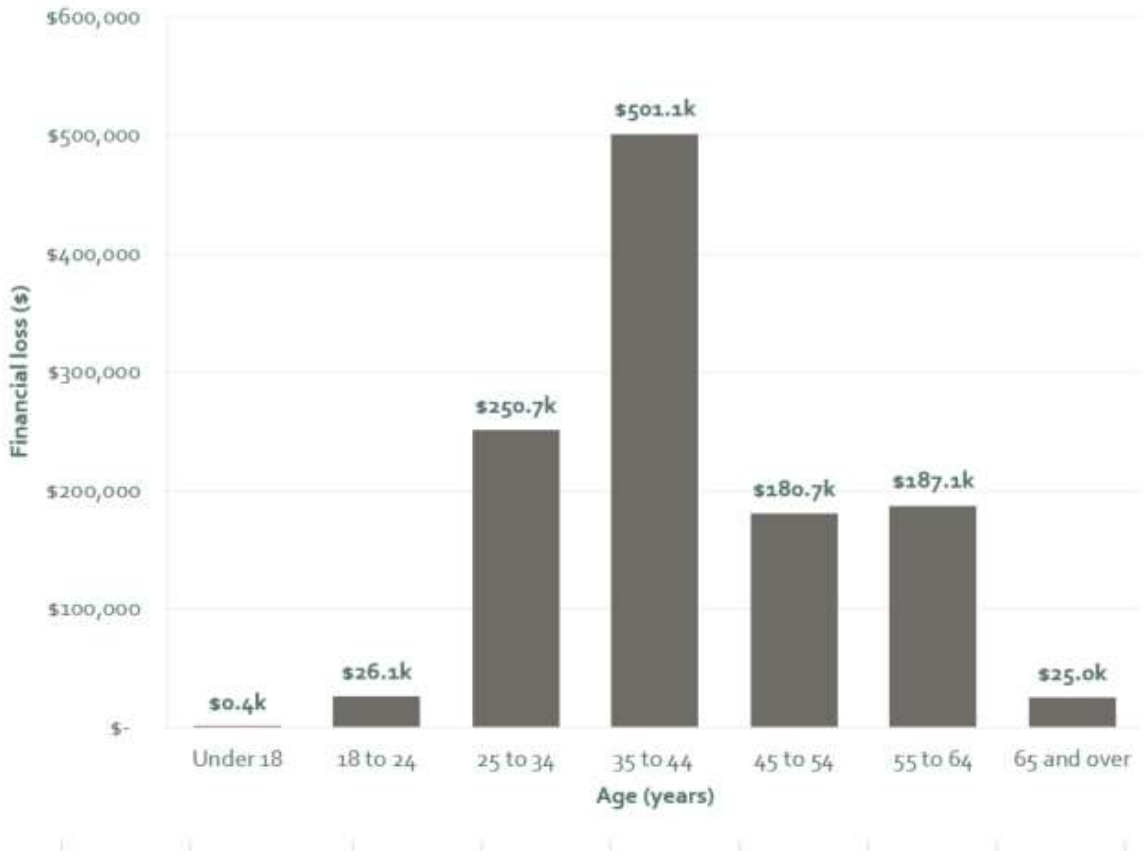
Of the 602 reports of incidents affecting individuals, 508 (84%) provided their date of birth.

Figure 13: Incidents affecting individuals – breakdown by age



New Zealanders in the 35 – 44 age group, experienced the largest direct financial loss in Q4, accounting for 43% of the total of direct financial losses.

Figure 14: Distribution of direct financial losses reported by age



Of the 177 reports of incidents affecting New Zealand individuals where a date of birth and loss amount was provided, the average loss was $7,604 and the median loss was $294.

Table 3: Distribution of direct financial losses reported by age

Under 18	18 - 24	25 -34	35 - 44	45 - 54	55 - 64	65 and over
$410	$26,064	$250,726	$501,090	$180,689	$187,120	$25,018

6. About CERT NZ

CERT NZ is New Zealand's Computer Emergency Response Team, and works to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. CERT NZ provides trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand. See www.cert.govt.nz for more information.

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 are comfortable in providing, often about very sensitive incidents.

Sometimes CERT NZ may ask for additional information about an incident to gain a better understanding, or if 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 as published on our website, and this report is subject to the CERT NZ standard disclaimer.

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

Our regional 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. 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 the best next steps to take.

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. These will be refined as the data set grows.

The **incident** report categories are:

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.

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

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

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.

Phishing and credential harvesting . Types of email, text or website attacks designed to convince users they are genuine, when 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.

Ransomware. A common malware variant with a specific purpose. If installed (usually by tricking a user into doing so, or by 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.

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

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

Suspicious network traffic. Detected attempts to find insecure points or vulnerabilities in networks, infrastructure or computers. Attackers 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.

Unauthorised access . Successful unauthorised access can enable an attacker to conduct a wide range of malicious activities on a network, infrastructure or computer. These activities generally fall under one of the three impact categories:

- compromise of the confidentiality of information
- improper modification affecting the integrity of a system
- degradation or denial of access or service affecting its availability.

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

Vulnerability categories we use

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

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

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 arising from human-introduced errors, misconfiguration or unintentional circumvention of security controls.

IoT devices. Internet of Things devices are internet-connected devices used to perform distributed functions over a network.

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

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.

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.

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

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 can also arise from misconfiguration or failures in security management.

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.