certnz

Quarterly Report:
Data Landscape

Q3

1 July – 30 September
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 July – 30 September 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 https://www.cert.govt.nz/about/quarterly-report/

2. Incidents and referrals

Incident summary

Between 1 July and 30 September 2018, 870 incidents were reported to CERT NZ. This is up 18% from the previous quarter (736).

Of the 870 incidents reported:

- 711 were responded to directly by CERT NZ, up 16% from the 615 in Q2 2018
- 18% (157) were referred to NZ Police, up 40% from last quarter.

Table 1: Incident partner referrals

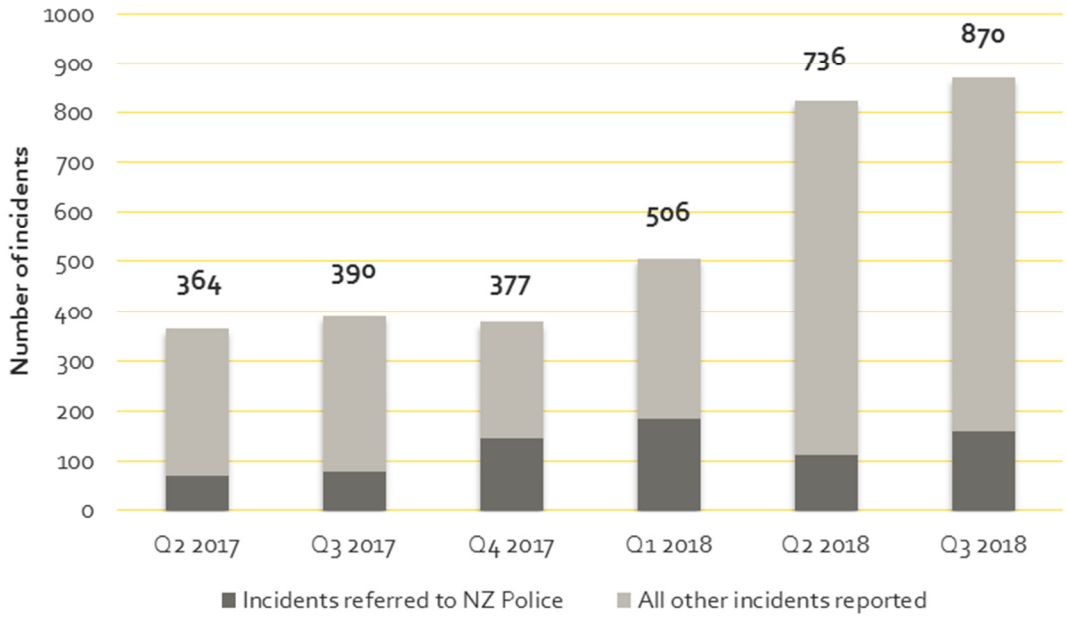
870 incidents reported	
711	responded to directly by CERT NZ
157	referred to NZ Police
1	referred to Netsafe
0	referred to National Cyber Security Centre
1	referred to Department of Internal Affairs

Another 135 events were automatically directed to other agencies and not recorded as an incident by CERT NZ. Our online reporting tool does this when an incident is immediately identifiable as being outside CERT NZ's scope and best dealt with by an agency with the right expertise, for example cyber bullying, spam and online child abuse.

Incidents per quarter

The total number of incidents reported to date is 3243.

Figure 1: Number of incidents reported by quarter



3. Reporting by incident category

Breakdown by category

There has been a 90% increase in scam and fraud incidents, up from 104 in Q2 2018, to 198 in Q3.

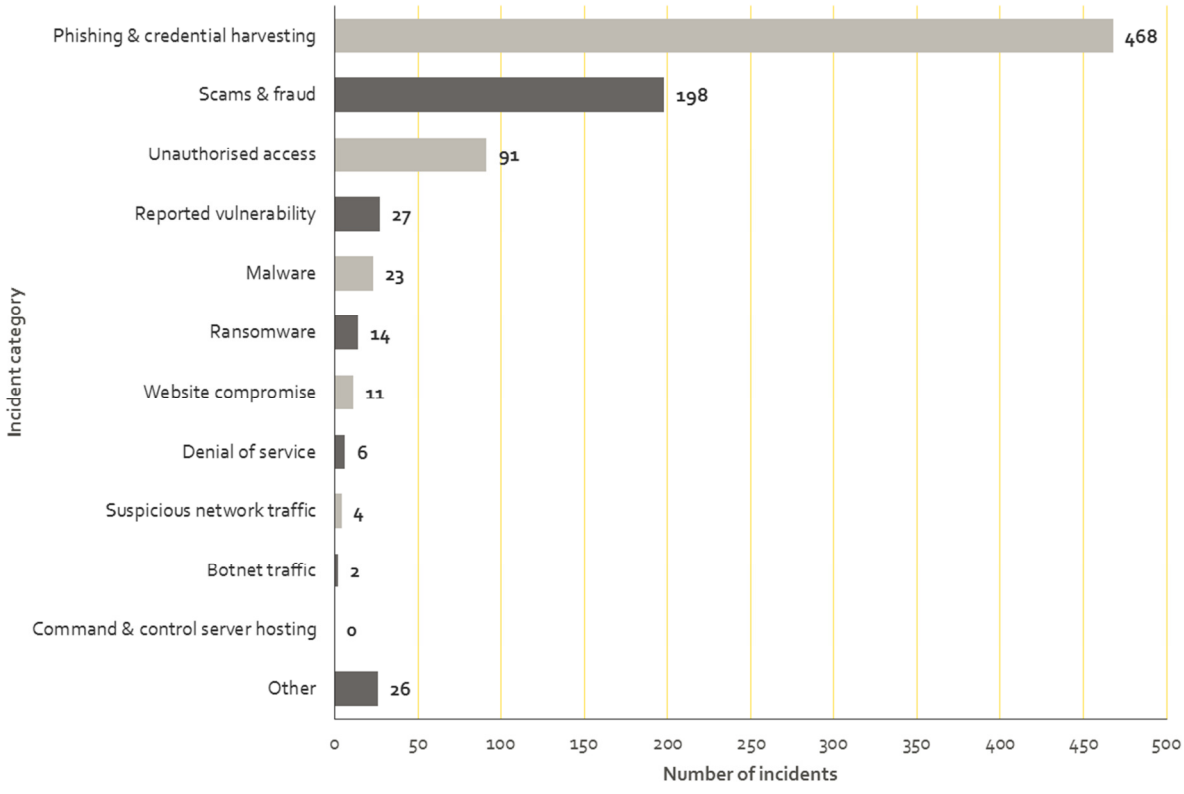
Webcam blackmail and payment scams made the largest contribution to this increase. The payment scams are mainly scammers using fake invoice emails, or compromising email accounts to change bank account details in invoices, to divert money to accounts controlled by the scammers.

Phishing and credential harvesting reports have been steady this quarter with a 3% increase from 455 in Q2 2018. Compared to the last quarter, other notable increases in the categories of reports are:

- a 28% increase in unauthorised access incidents from 71 to 91
- a 283% increase in malware reports from 6 to 23.

Read CERT NZ's Quarterly Report: Highlights for more information.

Figure 2: Breakdown by incident category

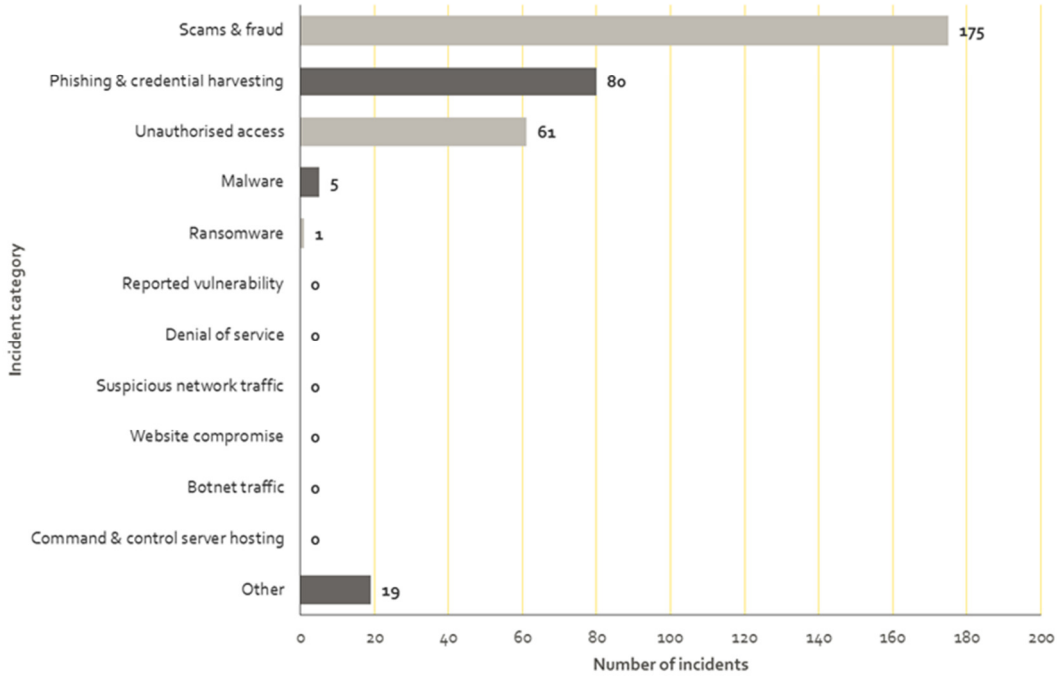


Breakdown of incidents about individuals

341 (39%) of incidents reported were about individuals, up 49% from 229 last quarter.

The webcam blackmail scam[1] made a significant contribution to this increase, with scam and fraud reports about individuals increasing 88% compared to last quarter.

Figure 3: Breakdown of incidents about individuals

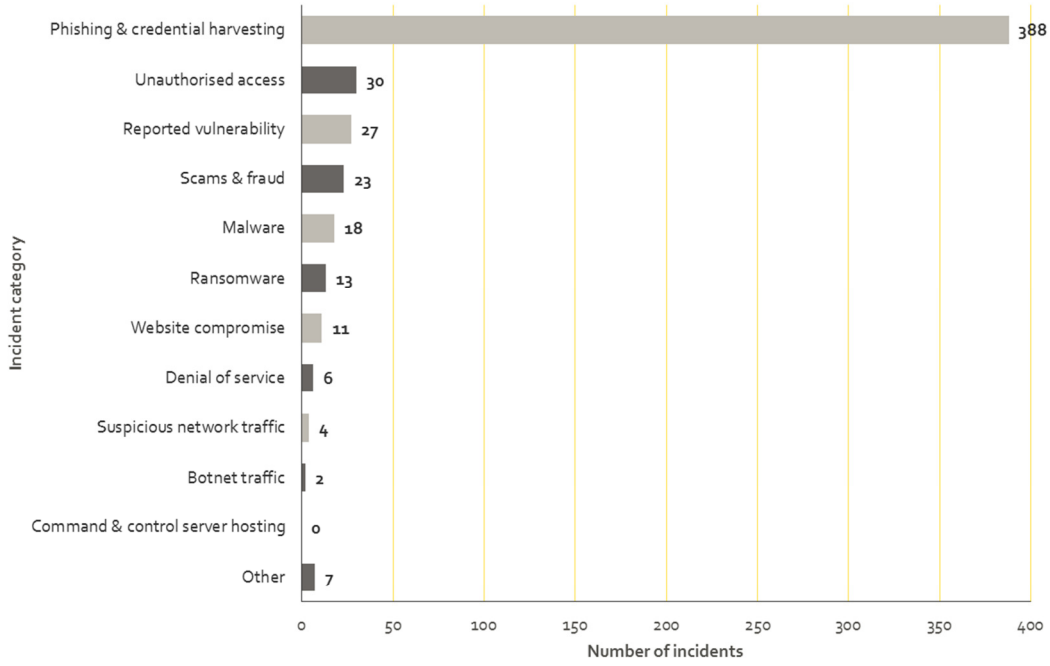


[1] https://www.cert.govt.nz/businesses-and-individuals/recent-threats/webcam-and-password-blackmail-scam/

Breakdown of incidents about organisations

529 (61%) of incidents reported were about organisations, up 4% from 507 last quarter.

Figure 4: Breakdown of incidents about organisations

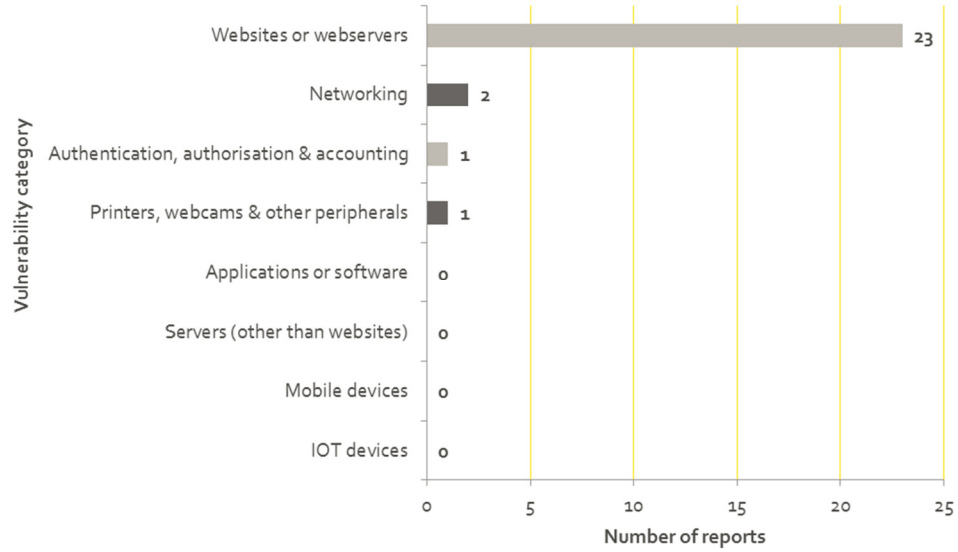


Breakdown of reported vulnerabilities

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.

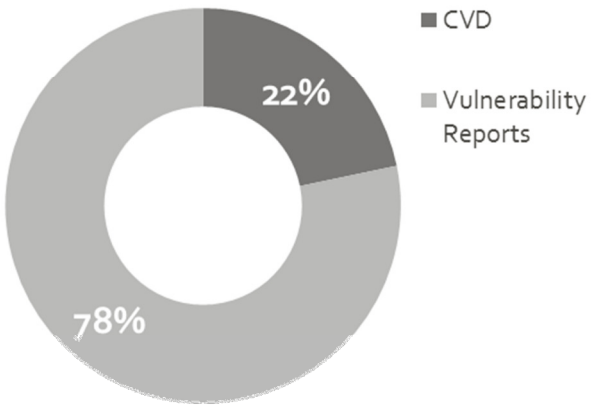
This quarter CERT NZ received 27 reported vulnerabilities. Consistent with Q1 and Q2 2018, the largest reported category is websites or webservers making up 85%.

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 six vulnerability reports this quarter using the CVD policy[2]. The proportion of CVD reports to vulnerability reports in Q3 remains the same as for Q1 and Q2 combined.

Figure 6: Proportion of coordinated vulnerability disclosures



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

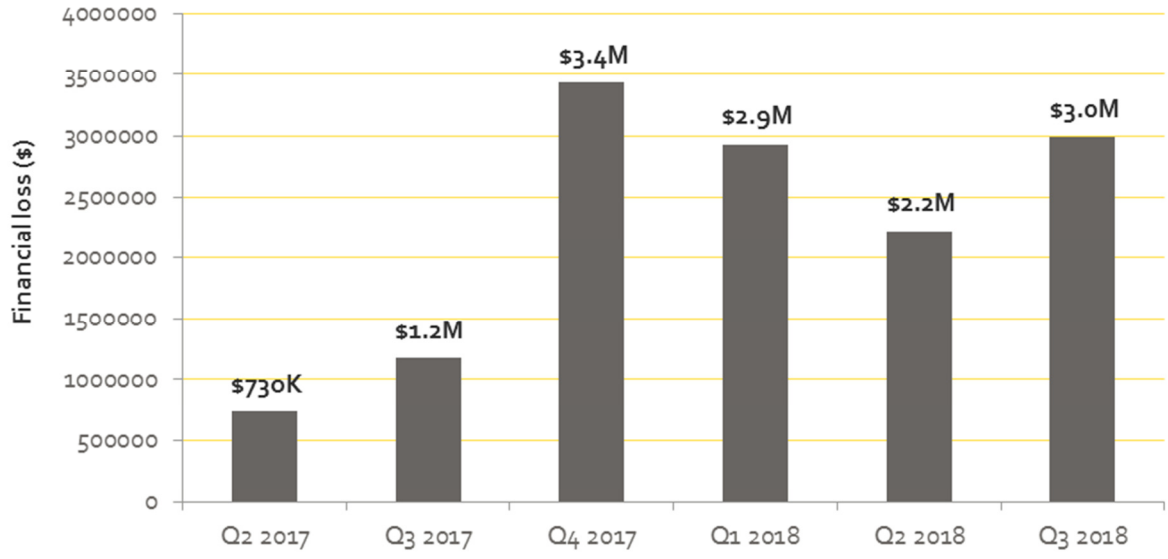
4. Impacts

Total financial losses

Direct financial losses increased by 35% to $2,993,518 this quarter.

Half of the financial losses reported were due to personal and business emails being compromised (this includes cases of invoice scams covered on our website[3]). The reports showed that attackers used a range of techniques from 'spoofing' email addresses to trick recipients into thinking it was from a legitimate source, to full takeover of email accounts to do things like change bank details in invoices.

Figure 7: Direct financial losses per quarter



[3] https://www.cert.govt.nz/businesses-and-individuals/recent-threats/invoice-scams-affecting-new-zealand-businesses/

Distribution of financial loss

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

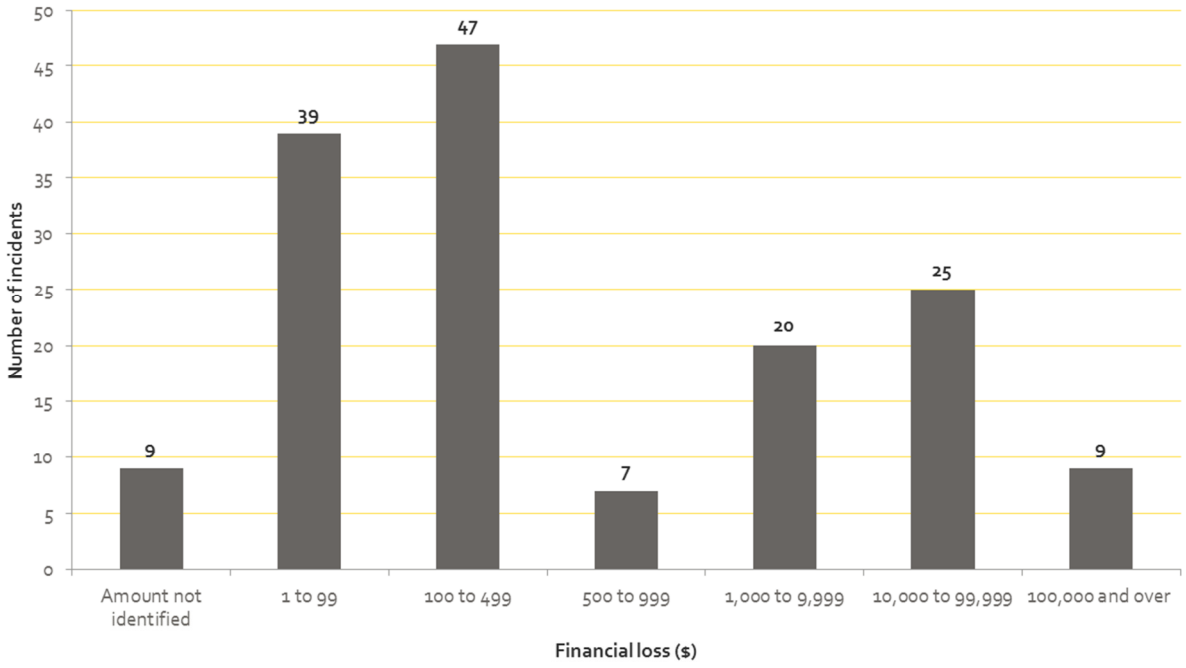
- organisations reported $1,377,563 (46% of all direct financial loss)
- individuals reported $1,615,955 (54% of all direct financial loss).

During this quarter, nine incidents involved losses of $100,000 or more, a total of $2,061,008. Of these nine incidents:

- seven involved scams and fraud, including three invoice scams affecting businesses
- two involved unauthorised access.

The percentage of incidents reporting direct financial loss this quarter was 18% (156). This is a 50% increase in the number of incidents reporting direct financial loss in Q2 2018.

Figure 8: Distribution of direct financial loss



Types of loss

Of the incidents reported this quarter, 27% (234) reported some type of loss (not just financial). This is up from the 21% (157) of incidents that reported some type of loss last quarter. Note that some reports include multiple types of loss.

Of the 341 incidents reported about individuals, 47% (161) involved some type of loss. Of the 529 incidents reported about organisations, 14% (73) involved some type of loss.

Losses experienced are broken down by type as follows:

Table 2: Types of loss

18% **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 recovery, such as needing to contract IT security services or investing in new security systems after an incident (Q2 2018: 14%).

1% **Reputational loss:**

Damage to the reputation of an individual or organisation as a result of being the victim of an incident (Q2 2018: 2%).

5% **Data loss:**

Loss or unauthorised copying of data, business records, personal records and intellectual property (Q2 2018: 5%).

1% **Technical damage:**

Impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation (Q2 2018: 2%).

4% **Operational impacts:**

The time, staff and resources that need to be spent on recovering from an incident, taking people away from normal business operations (Q2 2018: 2%).

2% **Other:**

Includes types of loss not covered in the other categories (Q2 2018: 1%).

5. Demographics

Reporting by sector

Of the 529 incidents reported about organisations, the three sectors with the most reports were:

- finance and insurances services 333 (63%)
- technology 33 (6%)
- professional, scientific, technical, administrative and support services 25 (5%)

Figure 9: Reports about organisations; breakdown by sector

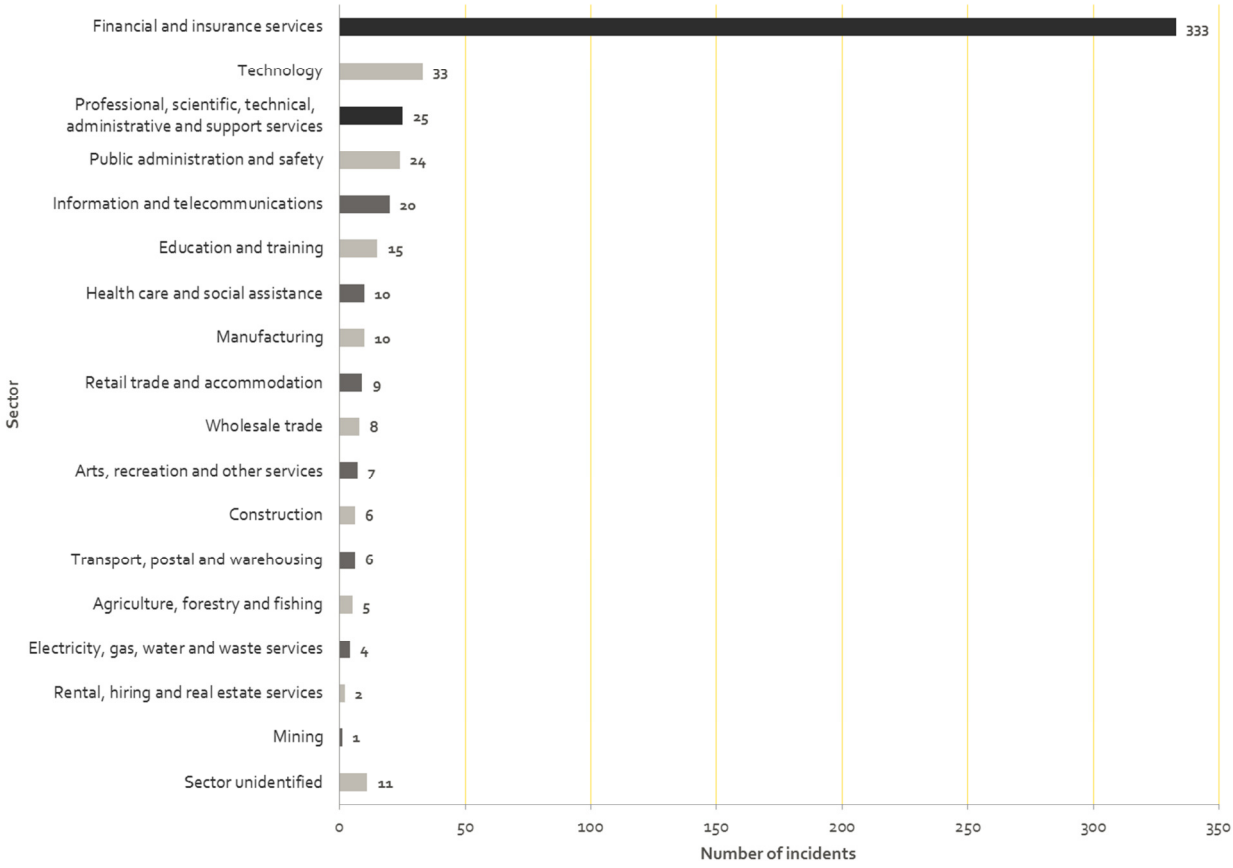
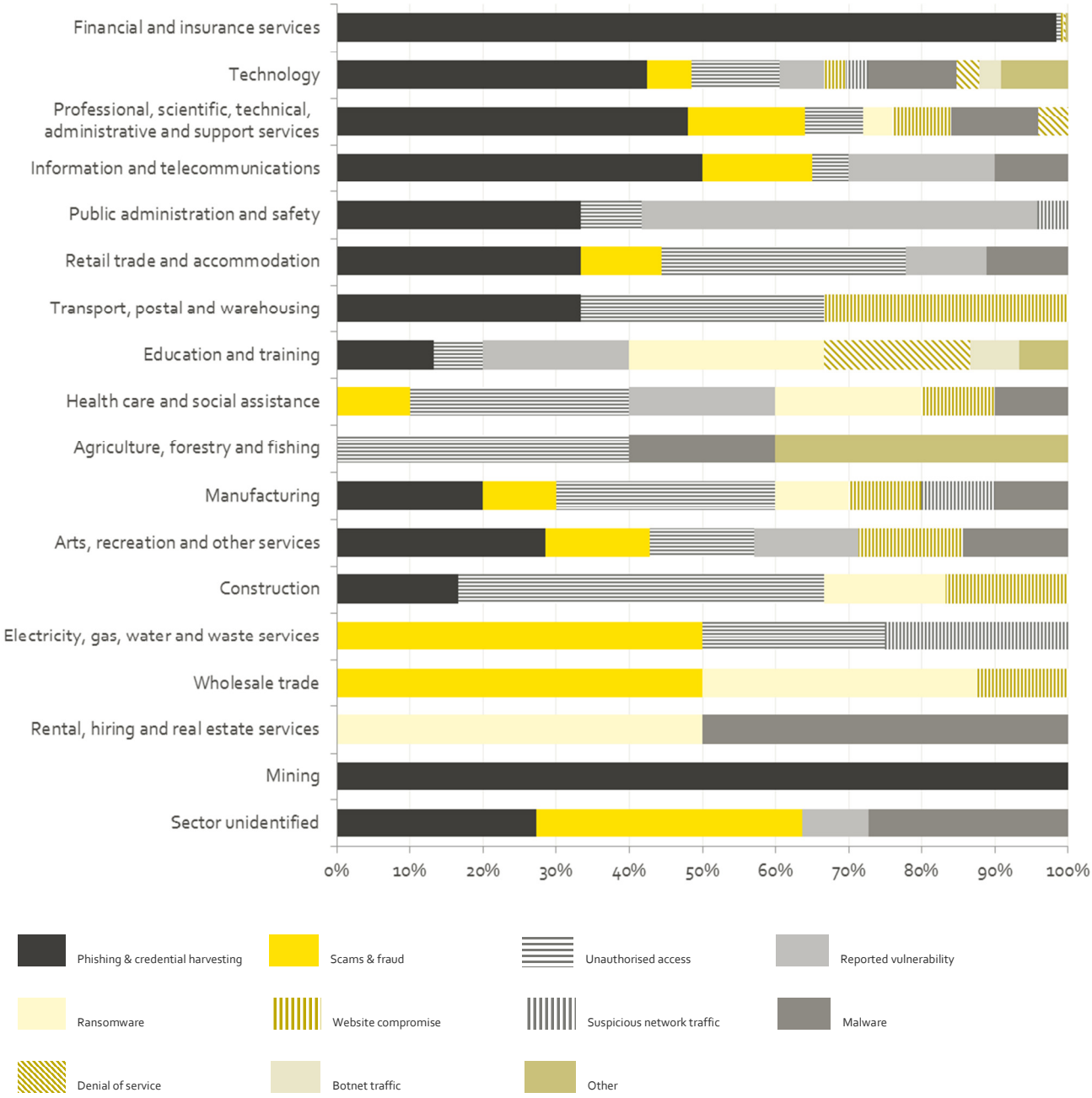


Figure 10: Breakdown by sector and incident category

A broad range of sectors have been affected by phishing and credential harvesting, scams and fraud, unauthorised access, ransomware, malware and website compromise.

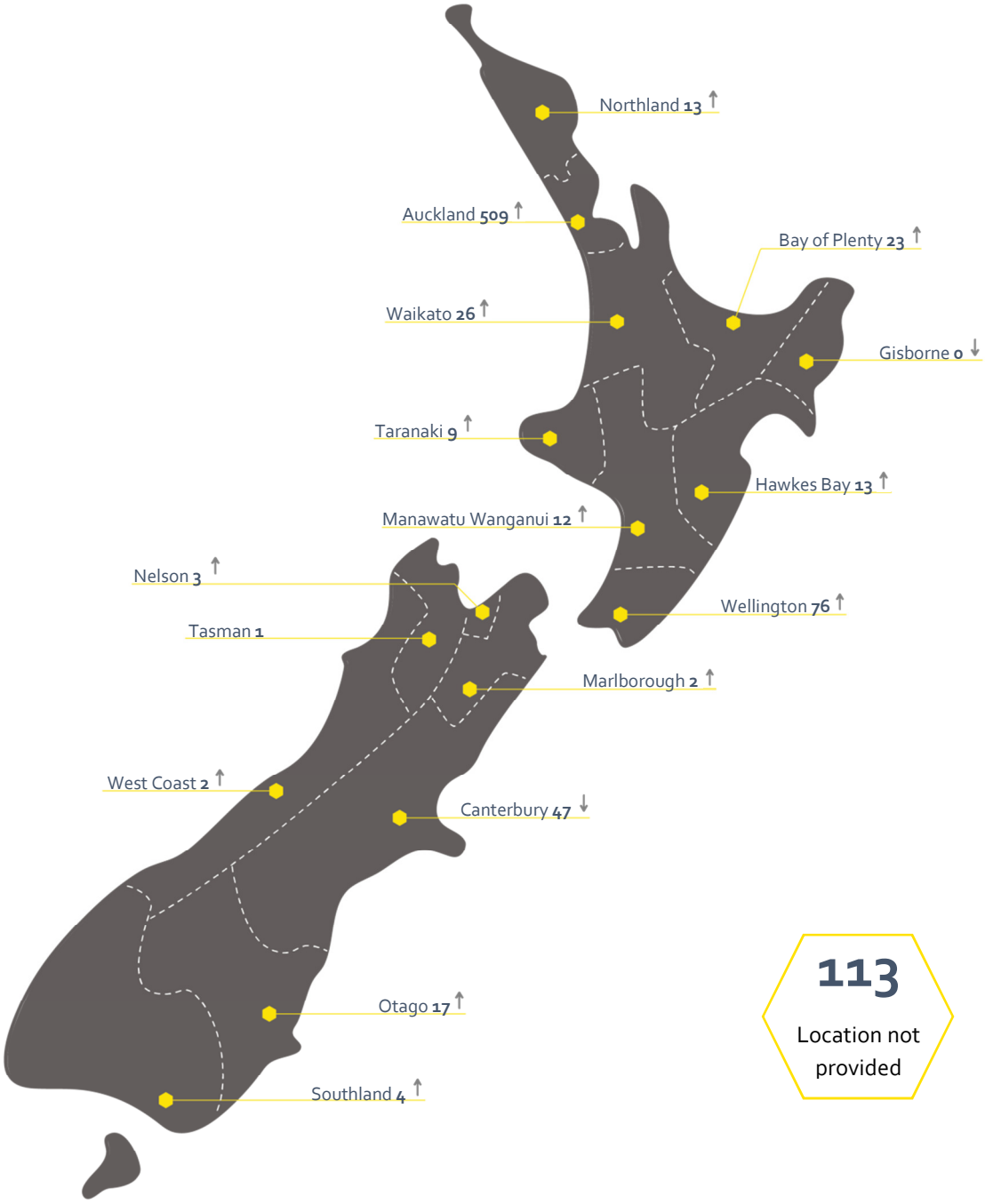


Reporting by region

Incidents reported increased across every region in New Zealand compared to last quarter, except for:

- Gisborne and Canterbury, where they decreased
- Tasman, where they were steady.

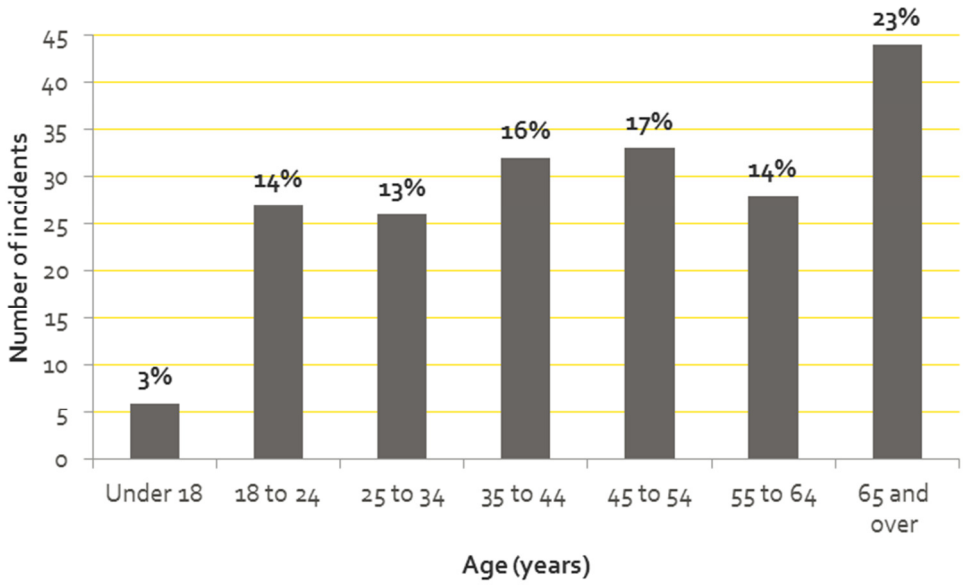
Figure 11: Breakdown by region



Reporting by age

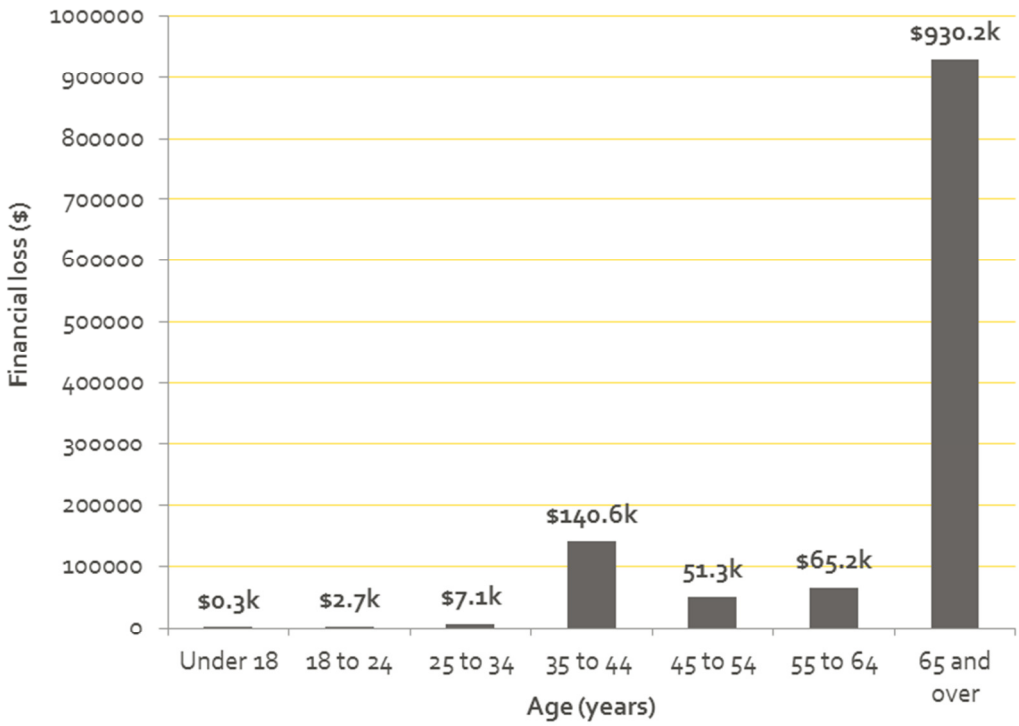
Of the 341 incidents reported about individuals, 57% provided a date of birth. Of these, the age range with the most incidents reported was 65 years and over (23%: 44 incidents). The spread of affected age ranges remains consistent with previous quarters.

Figure 12: Reports about individuals: breakdown by age



The 65-years-and-over age range experienced the highest value of direct financial loss with 78% of the value of direct financial losses reported (by individuals who provided their age).

Figure 13: Distribution of direct financial loss reported by age



For the 82 incidents about individuals with a date of birth and loss amount provided, the average loss was$14,441 and the median loss was $215.

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
$345	$2,680	$7,059	$140,605	$51,336	$65,216	$930,200

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 as 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 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 - over time we will refine these categories to a more granular level 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 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).

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, 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.

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.

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.

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.

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.

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 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.

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

Vulnerability categories we use

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

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.

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.

IOT devices - 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 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.