



# Quarterly Report: Data Landscape



1 October – 31 December  
2018



# Contents

<b>1. Introduction</b>	<b>2</b>
<b>2. Incidents and referrals</b>	<b>2</b>
Incident summary	2
Incidents per quarter	3
<b>3. Reporting by incident category</b>	<b>4</b>
Breakdown by category	4
Breakdown of incidents about individuals	5
Breakdown of incidents about organisations	6
Breakdown of reported vulnerabilities	7
<b>4. Impacts</b>	<b>8</b>
Total financial losses	8
Distribution of financial loss	9
Types of loss	10
<b>5. Demographics</b>	<b>11</b>
Reporting by sector	11
Reporting by region	13
Reporting by age	14
<b>6. About CERT NZ</b>	<b>16</b>
A word about our information	16
Reporting an incident to CERT NZ	16
Incident categories we use	17
Vulnerability categories we use	18

# 1. Introduction

This document provides a standardised set of results and graphs for the quarter, and an 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 October 2018 – 31 December 2018.

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

You can find both documents on our website at <https://www.cert.govt.nz/about/quarterly-report/>

## 2. Incidents and referrals

### Incident summary

Between 1 October and 31 December 2018, 1333 incidents were reported to CERT NZ. This is up 53% from the previous quarter (from 870).

Of the 1333 incidents reported:

- 1174 were responded to directly by CERT NZ, up 65% from the 711 in Q3 2018
- 12% (157) were referred to NZ Police, the same as last quarter.

**Table 1: Incident partner referrals**

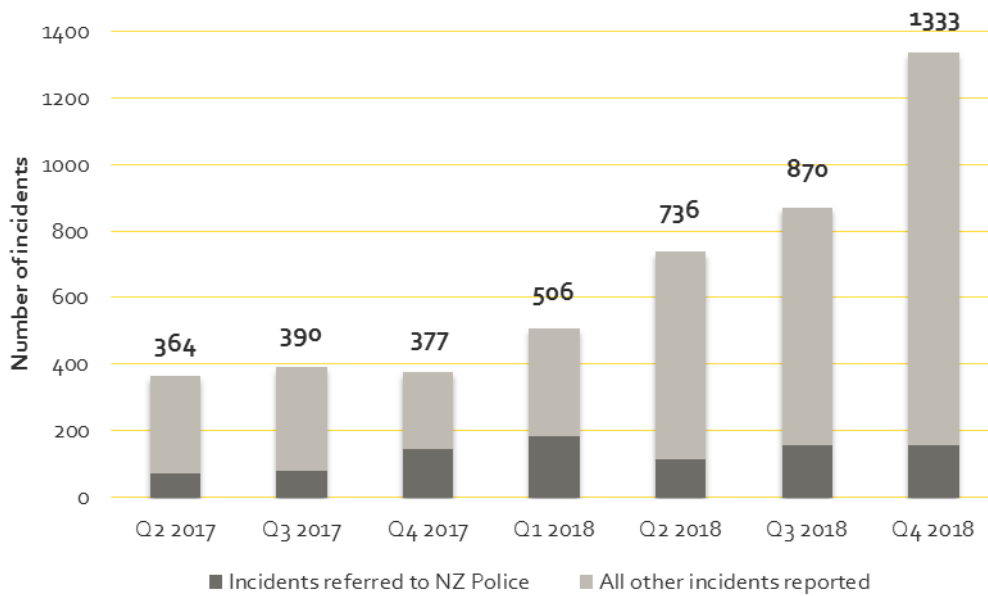
1333 incidents reported	
1174	responded to directly by CERT NZ
157	referred to NZ Police
1	referred to Netsafe
0	referred to National Cyber Security Centre
1	referred to Department of Internal Affairs

Another 124 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 4576. A total of 3445 reports were received in 2018, more than triple the number (1131) received in 2017.

**Figure 1: Number of incidents reported by quarter**



## 3. Reporting by incident category

### Breakdown by category

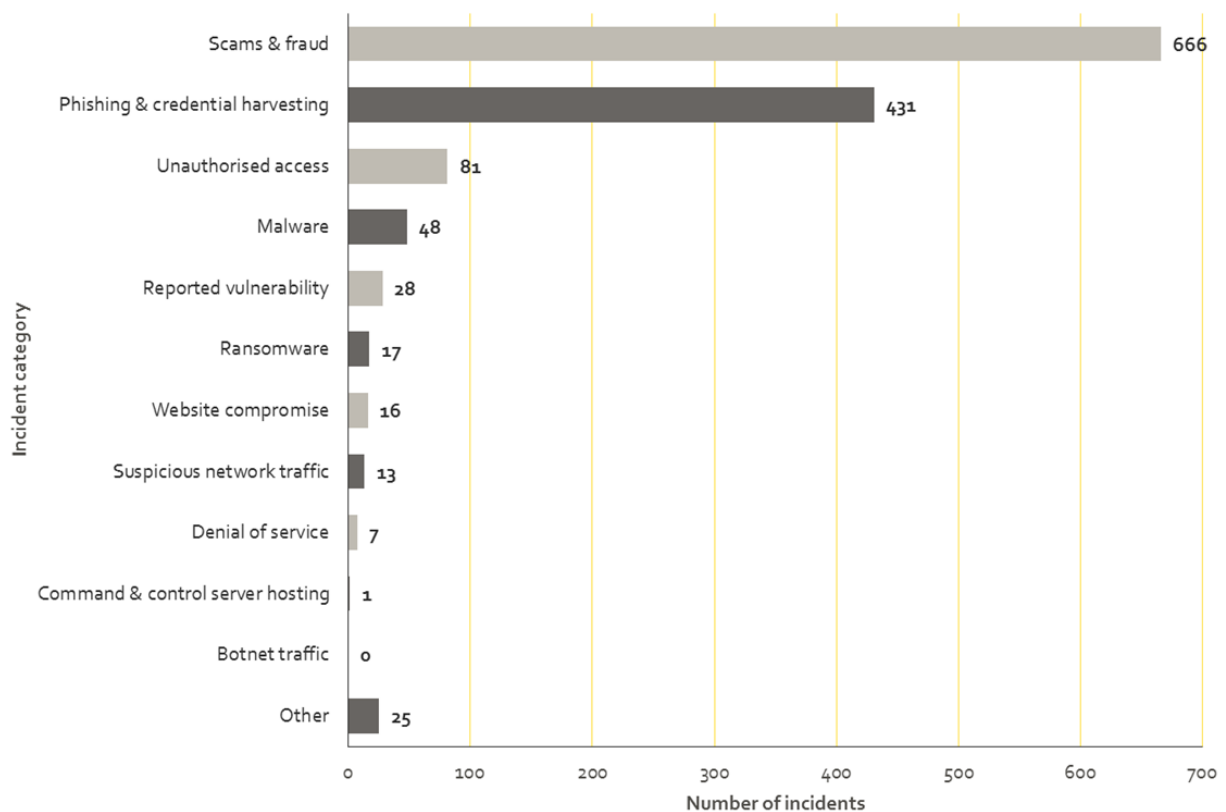
Scam and fraud incidents increased again this quarter with over triple the 198 received last quarter. A surge in email extortion scams and other variants was behind the increase. Phishing and credential harvesting reports are down from the 468 received last quarter. They still make up 32% of all incident reports received. This quarter has seen:

- over double the number of malware reports, up 109% from the 23 last quarter to 48 this quarter
- a 45% increase in website compromise from 11 to 16
- an 11% decrease in unauthorised access reports from 91 to 81.

Some categories have remained consistently low through Q4 and throughout 2018, such as botnet traffic, command and control server hosting, and denial of service reports. Each category accounted for less than 1% of reports. However, it is not possible at this time to assess whether it is because these incidents aren't happening in New Zealand as frequently, or whether they are just not being reported to CERT NZ currently.

Read CERT NZ's Q4 2018 Quarterly Report: Highlights on [www.cert.govt.nz](http://www.cert.govt.nz) for more information about the incident reports received.

**Figure 2: Breakdown by incident category**

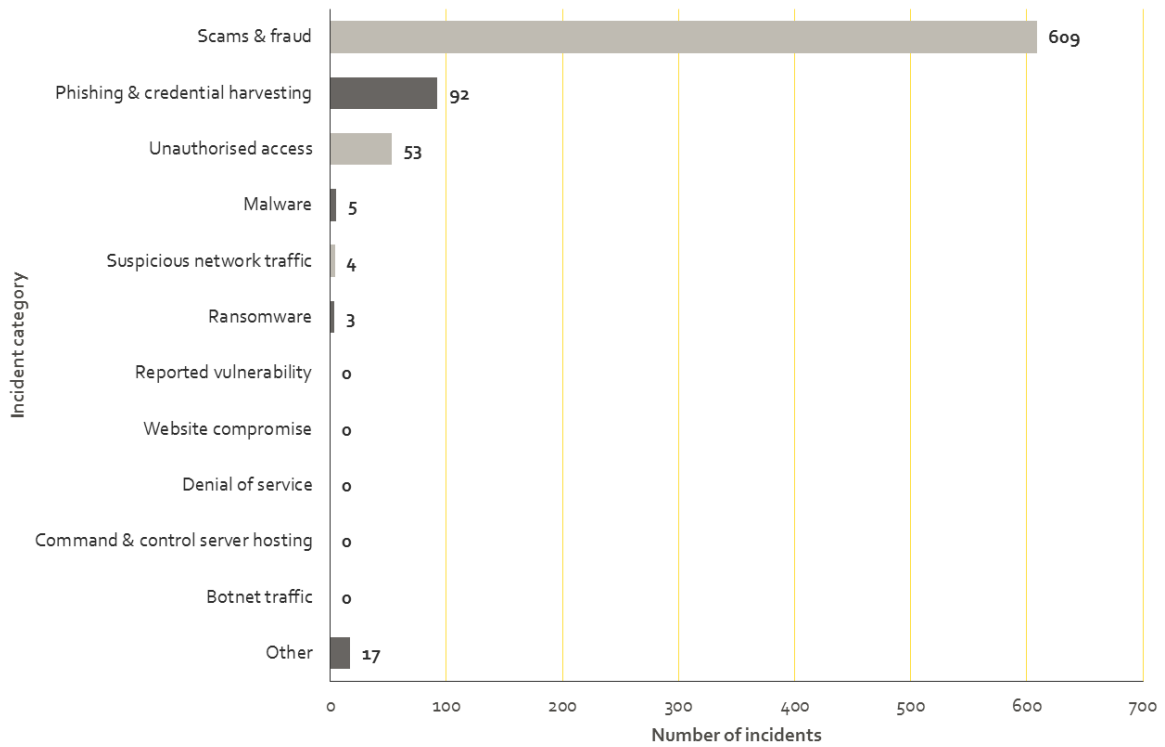


## Breakdown of incidents about individuals

783 (59%) of incidents reported were about individuals, up 130% from 341 last quarter.

The number of incident reports related to email extortion scams<sup>1</sup>, jumped significantly this quarter. This contributed to a jump of almost three-and-a-half times in the number of scam and fraud incident reports from individuals this quarter (175 scam and fraud reports were received in Q3 2018).

**Figure 3: Breakdown of incidents about individuals**

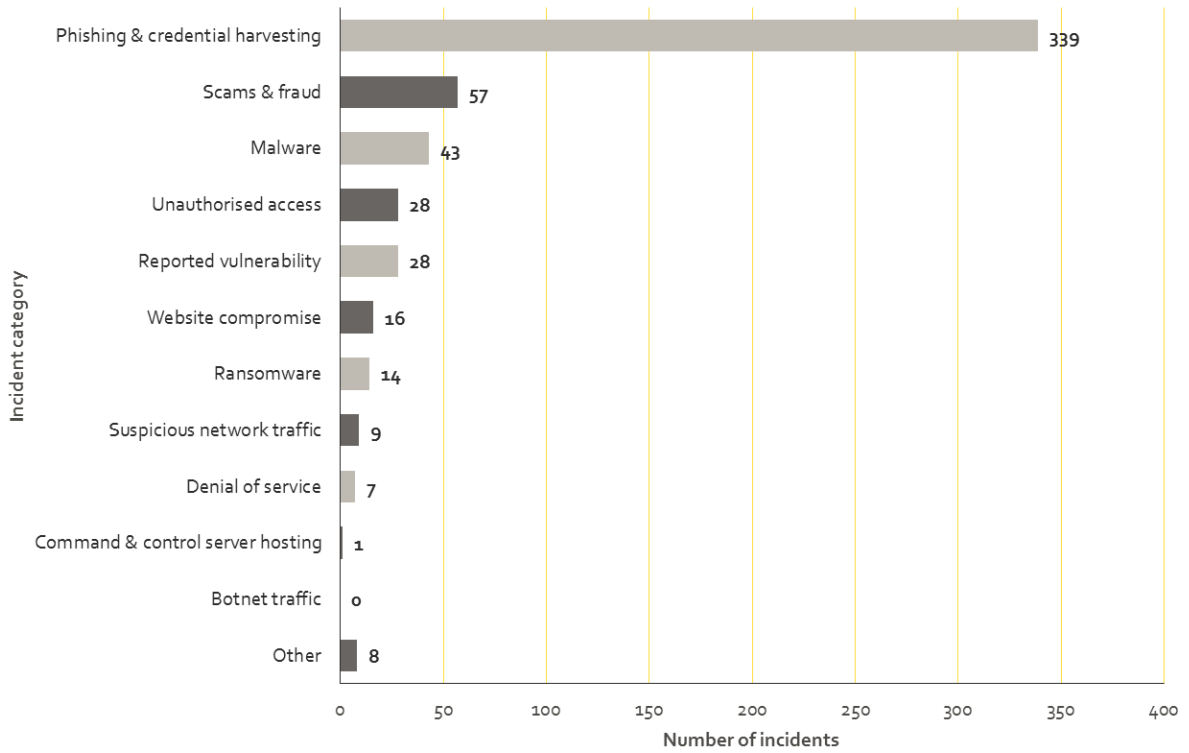


<sup>1</sup> <https://www.cert.govt.nz/businesses-and-individuals/recent-threats/webcam-and-password-blackmail-scam/>

## Breakdown of incidents about organisations

550 (41%) incidents reported were about organisations, up 4% from 529 last quarter. The number of malware reports from organisations more than doubled this quarter. A phishing campaign containing malware targeting business customers of some New Zealand banks<sup>2</sup> contributed to this jump.

Figure 4: Breakdown of incidents about organisations



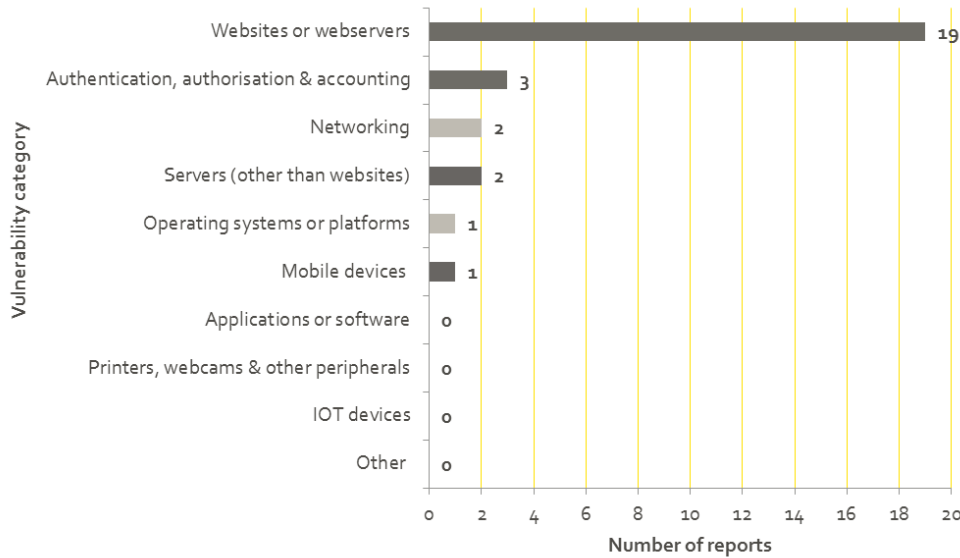
<sup>2</sup> <https://www.cert.govt.nz/businesses-and-individuals/recent-threats/malware-targeting-business-customers-of-new-zealand-banks/>

## 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.

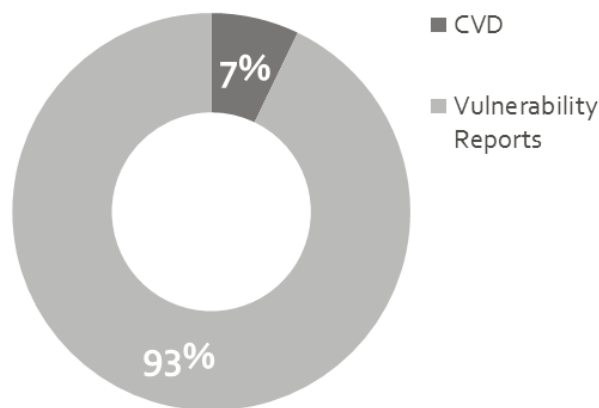
This quarter, CERT NZ received 28 reported vulnerabilities. The largest category was reports about websites or web servers, making up 68%. This reflects a consistent trend throughout 2018. There is a corresponding increase in website compromise incident reports, up 45% from 11 in Q3 2018 to 16 in Q4 2018.

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 two vulnerability reports using the CVD policy this quarter<sup>3</sup>. This is down from previous quarters in 2018.

Figure 6: Proportion of coordinated vulnerability disclosures



<sup>3</sup> <https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/>

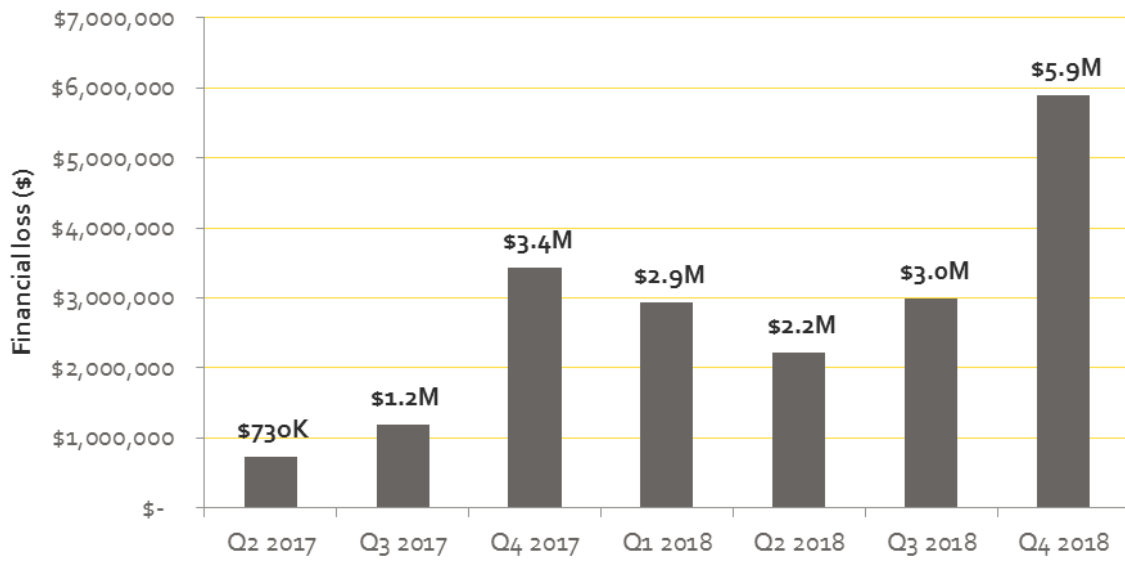


## 4. Impacts

### Total financial losses

Direct financial losses totaled \$5,901,447 this quarter, almost double the loss from last quarter. For 2018 the total direct financial loss reported was just over \$14 million, up from \$5.3 million in 2017.

Figure 7: Direct financial losses per quarter



## Distribution of financial loss

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

- organisations reported \$1,264,755 (21% of all direct financial loss)
- individuals reported \$4,636,691 (79% of all direct financial loss).

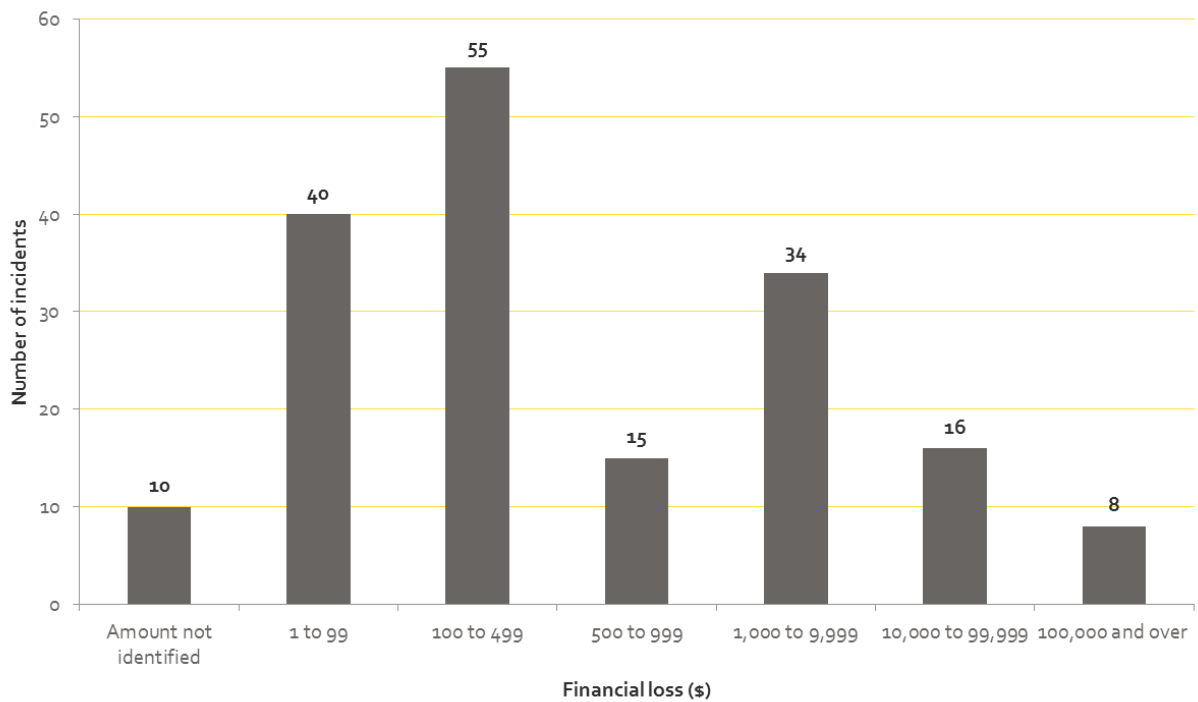
For individuals where a date of birth and loss amount was provided, the average amount lost from incidents was \$8,396, and the average age was 53.

During this quarter, eight incidents involved losses of \$100,000 or more, a total of \$5,233,462. Of these eight incidents:

- six involved scams and fraud, including two invoice scams affecting businesses
- one involved unauthorised access
- one involved malware.

The percentage of incidents reporting direct financial loss was 13% (178). This is a 14% increase from the 156 incidents reporting direct financial loss in Q3 2018.

**Figure 8: Distribution of direct financial loss**



## Types of loss

Of the incidents reported this quarter, 22% (288) reported some type of loss (not just financial). This number is up from the 234 incidents that reported some type of loss last quarter. Note that some reports include multiple types of loss.

Of the 783 incidents reported about individuals, 26% (202) involved some type of loss. Of the 550 incidents reported about organisations, 16% (86) involved some type of loss.

Losses experienced are broken down by type as follows:

**Table 2: Types of loss**

### 13% 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 (Q3 2018: 18%).

### 1% Reputational loss:

Damage to the reputation of an individual or organisation as a result of being the victim of an incident (Q3 2018: 1%).

### 4% Data loss:

Loss or unauthorised copying of data, business records, personal records and intellectual property (Q3 2018: 5%).

### 1% Technical damage:

Impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation (Q3 2018: 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 (Q3 2018: 4%).

### 5% Other:

Includes types of loss not covered in the other categories (Q3 2018: 2%).

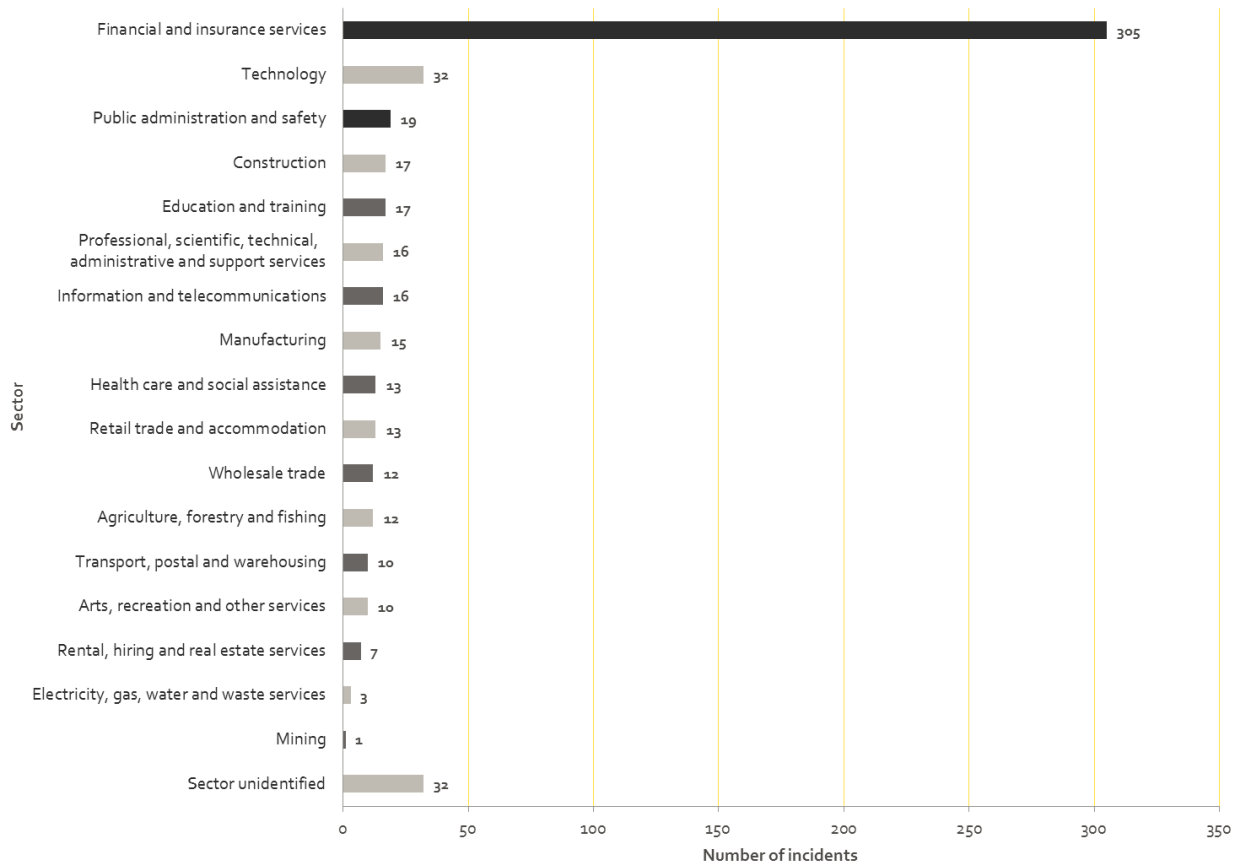
# 5. Demographics

## Reporting by sector

Of the 550 incidents reported about organisations, the three sectors with the most reports were:

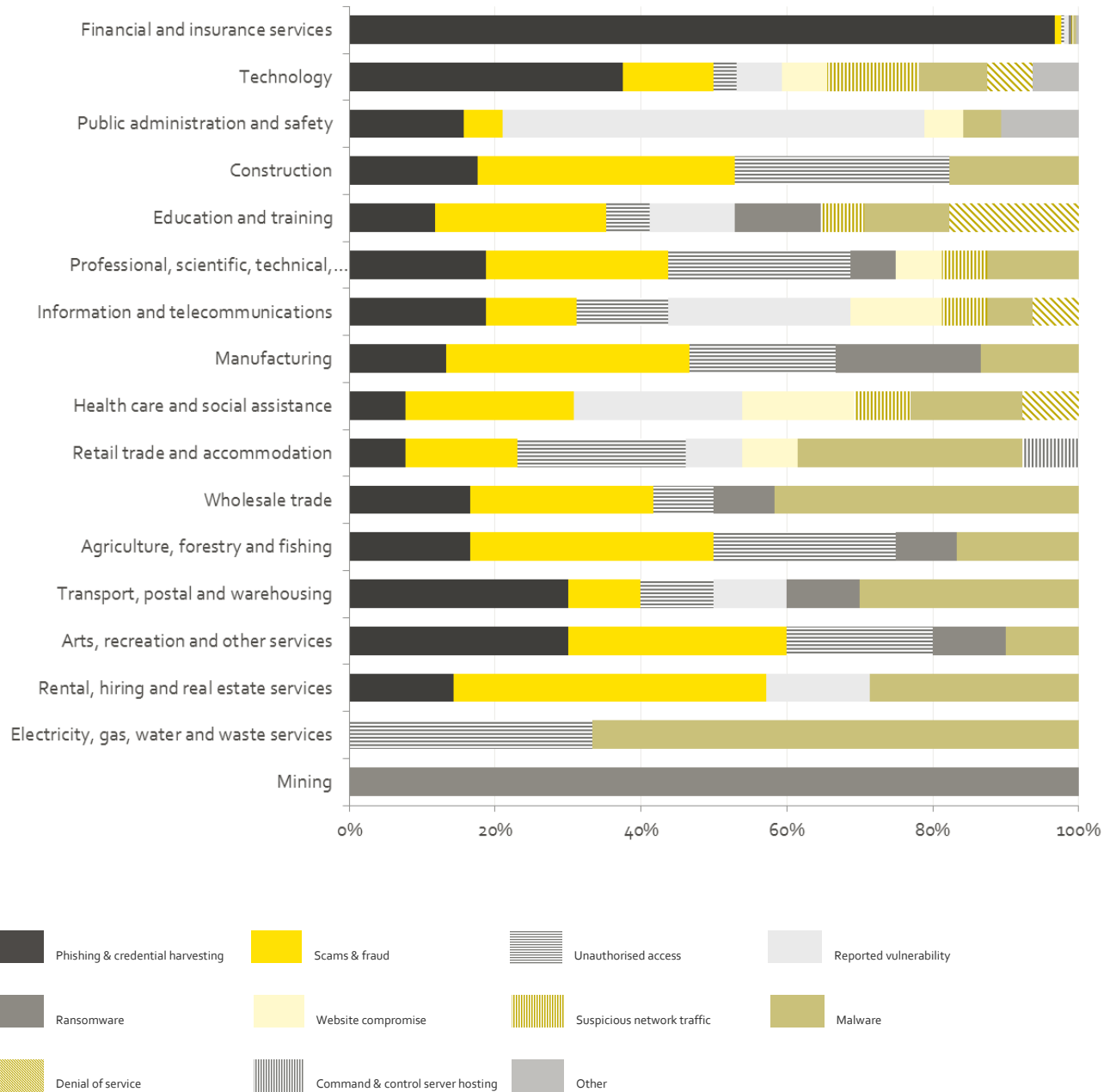
- finance and insurances services, 305 (55%)
- technology, 32 (6%)
- public administration and safety, 19 (3%).

Figure 9: Reports about organisations; breakdown by sector



### Figure 10: Breakdown by sector and incident category

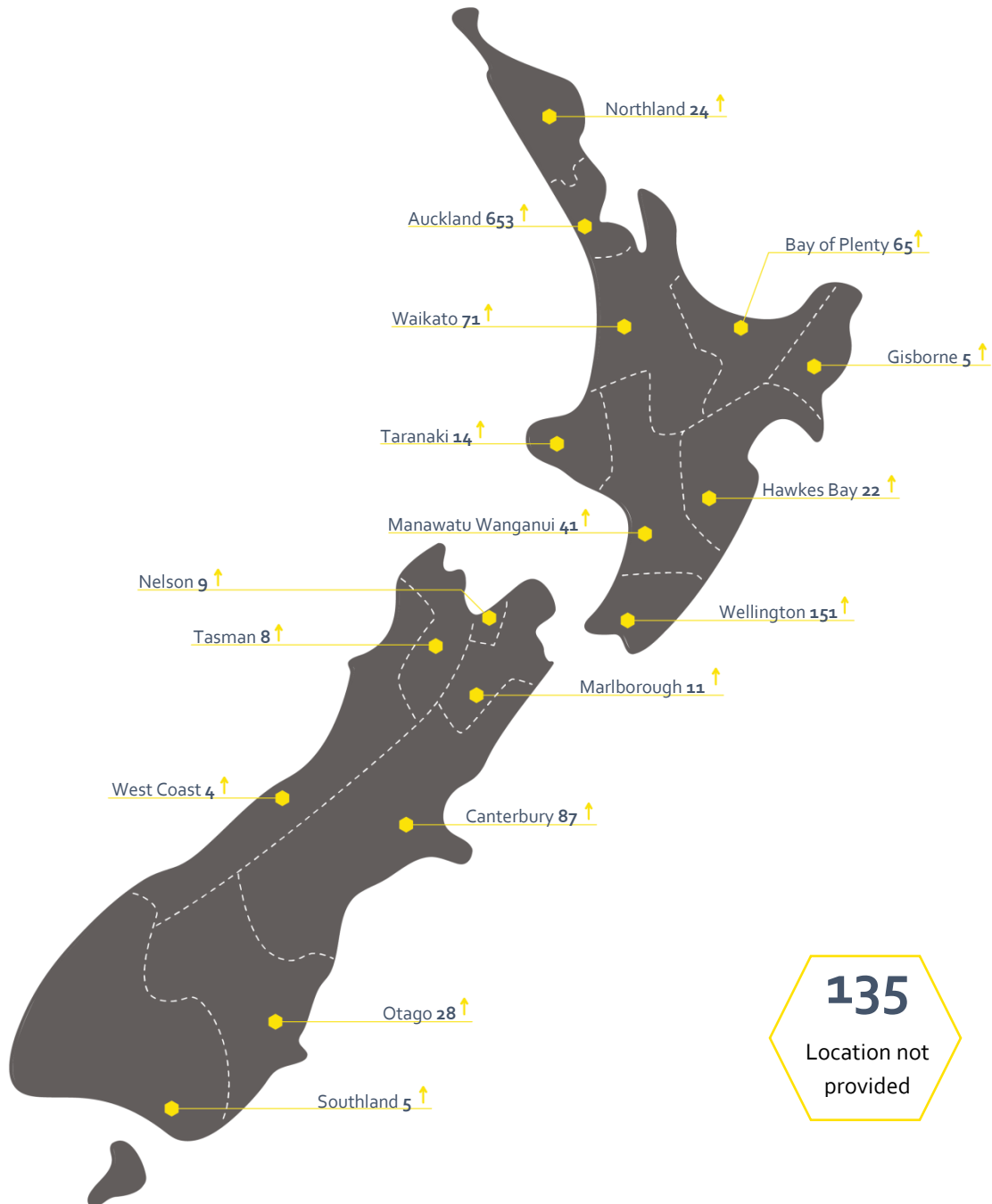
Almost all sectors have been affected by phishing and credential harvesting, scams and fraud and malware this quarter. As seen in other quarters, unauthorised access affects a wide number of sectors as well.



## Reporting by region

Incidents reported increased across every region by more than 60% compared to last quarter, with the exception of Auckland which increased by 47%. The email extortion scam reports from individuals have contributed to this increase as they were seen across all regions in New Zealand.

Figure 11: Breakdown by region

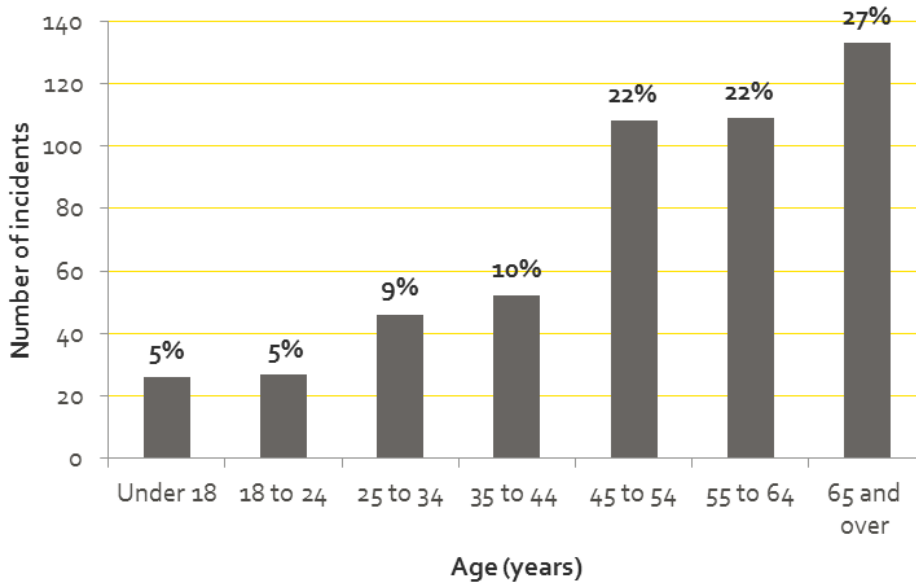


## Reporting by age

Of the 783 incidents reported about individuals, 501 (64%) provided their date of birth. Of these (501), the age range with the most incidents reported was 65 years and over (27%:133 incidents).

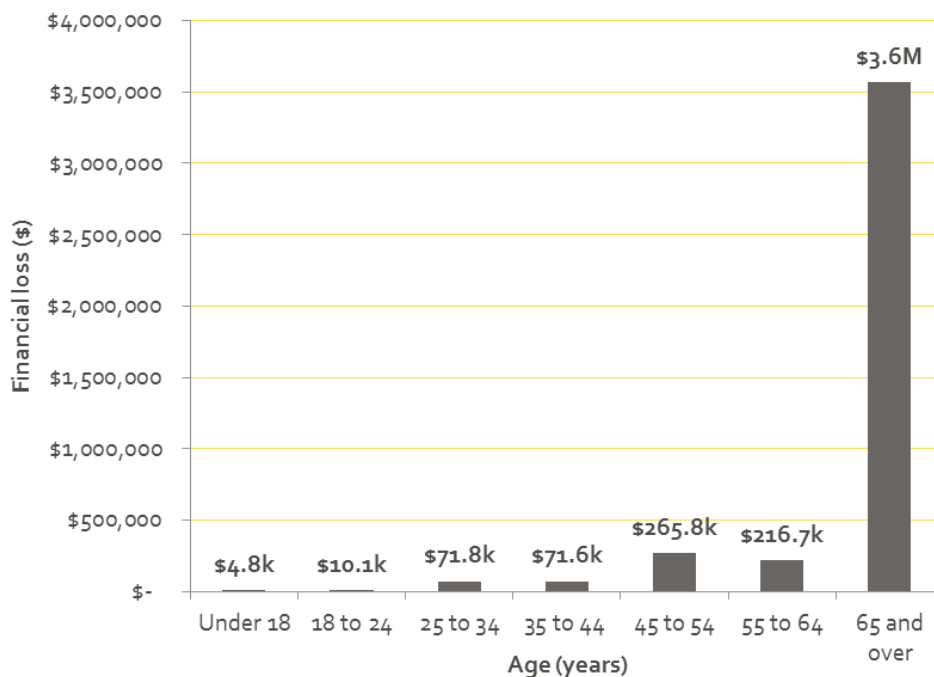
The spread of incident reports across affected age ranges varies this quarter when compared to previous quarters. This quarter the number of reports received increases with the age of the group reporting, the first quarter with this pattern.

**Figure 12: Reports about individuals; breakdown by age**



While all age groups experienced incidents, in this quarter those 65 and over experienced the highest value of direct financial loss with 85% of the value of direct financial losses.

**Figure 13: Distribution of direct financial loss reported by age**



For the 94 incidents about individuals with a date of birth and loss amount provided, the average loss was \$8,396 and the median loss was \$252.

**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
\$4,786	\$10,117	\$71,813	\$71,633	\$265,778	\$216,711	\$3,565,331



## 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](http://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.

**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.

**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.

**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.