certnz

Quarterly Report: Data Landscape

Q3 2019

1 July – 30 September, 2019

New Zealand Government

/// Contents

1. Introduction 2

2. Incidents and referrals 2

Incident summary 2

Incidents per quarter 3

3. Reporting by incident category 4

Breakdown by category 4

Breakdown of scam and fraud incidents 5

Breakdown of incidents about individuals 6

Breakdown of incidents about organisations 7

Breakdown of reported vulnerabilities 8

Figure 7: Proportion of coordinated vulnerability disclosures 8

Total financial losses 9

Distribution of financial loss 9

Types of loss 10

5. Demographics 11

Reporting by sector 11

Reporting by region 13

Reporting by age 14

6. About CERT NZ 16

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 analysis of the latest trends. Analytical comment is provided where meaningful or interesting trends were identified.

The report covers the quarter 1 July – 30 September 2019.

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 July and 30 September 2019, 1,354 incidents were reported to CERT NZ. This is up 13% from the previous quarter (from 1,197).

Of the 1354 incidents reported:

- 1,116 (82%) were responded to directly by CERT NZ, up 16% from 828 in Q1 2019
- 212 (16%) were referred to NZ Police, down 3% from the 219 in Q2 2019.
- 24 (2%) were referred to Department of internal Affairs, up 118% from 11 in Q2 2019

Table 1: Incident partner referrals

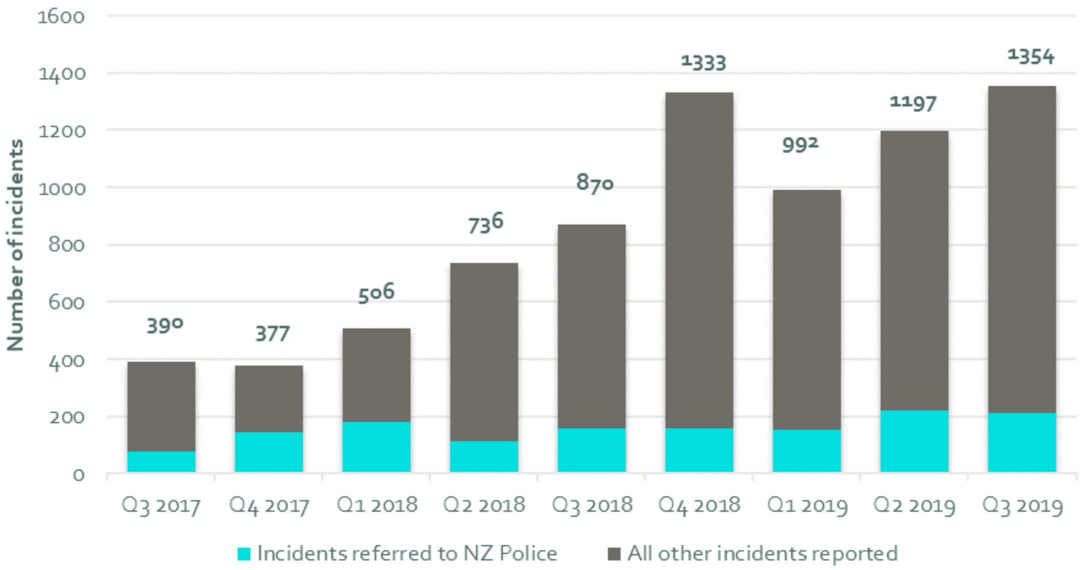
1,354 incidents reported	
1,116	responded to directly by CERT NZ
212	referred to NZ Police
1	referred to Netsafe
1	referred to National Cyber Security Centre
24	referred to Department of Internal Affairs

Another 218 events were automatically directed to other agencies and not recorded as incidents 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 over the last 12 months is 4,876.

Figure 1: Number of incidents reported by quarter



3. Reporting by incident category

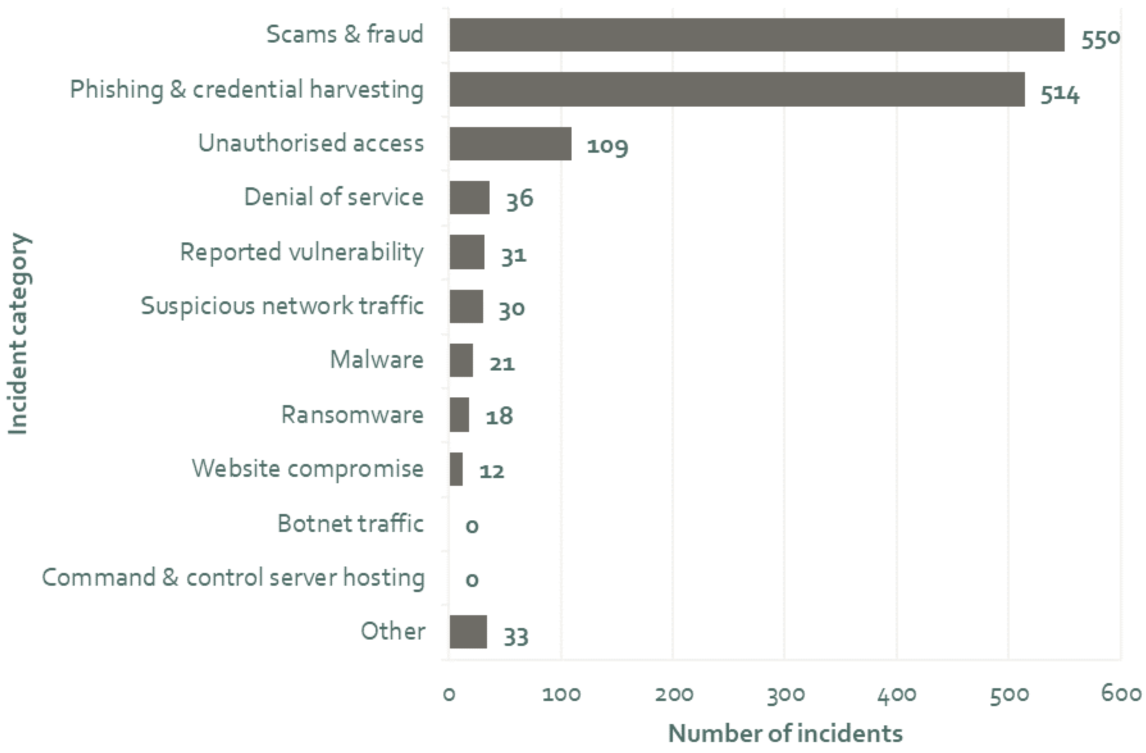
Breakdown by category

Scam and fraud incidents are up on last quarter, with 550 reports received. This quarter has seen:

- a 27% increase in phishing and credential harvesting, from 404 (Q2) to 514 (Q3)
- a 20% increase in scam and fraud reports, from 458 (Q2) to 550 (Q3)
- a 54% decrease in suspicious network traffic report, from 65 (Q2) to 30 (Q3)
- a 25% decrease in unauthorised access reports, down from 145 (Q2) to 109 (Q3).

Read CERT NZ's Q3 2019 Quarterly Report: Highlights on https://www.cert.govt.nz/about/quarterly-report/ for more information about the incident reports received.

Figure 2: Breakdown by incident category



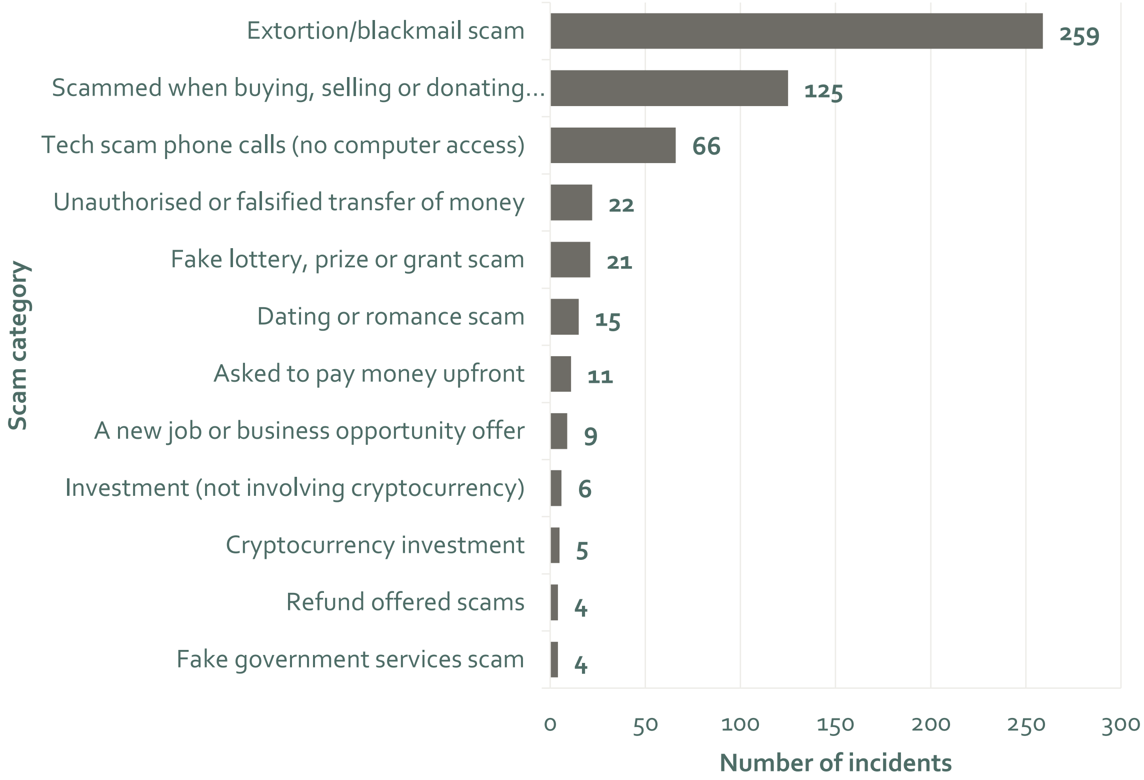
Breakdown of scam and fraud incidents

Of the incidents reported this quarter, 550 (41%) were about scams and fraud. The scam and fraud category is consistently one of the largest categories of incident reports this quarter CERT NZ has seen:

- Extortion/blackmail email scams continue to be the most common type of scam reported, with a rise of 16% incidents reported from Q2
- reports of scams occurring when buying, selling or donating online has risen by 44% this quarter from Q2
- tech scam calls not resulting in computer access has also risen by 50% from Q2.

You can read CERT NZ's Q3 2019 Quarterly Report: Highlights document[1] for more information about the incident reports received in this category.

Figure 3: Breakdown of scam and fraud categories

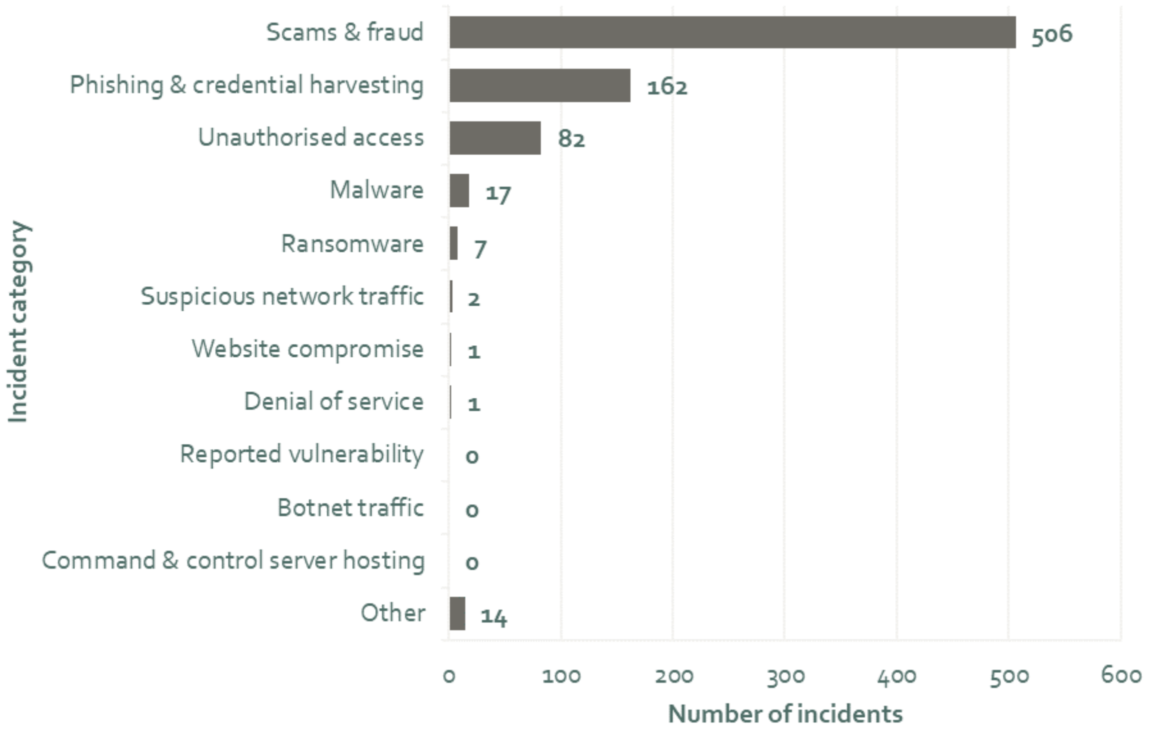


[1] https://www.cert.govt.nz/about/quarterly-report

Breakdown of incidents about individuals

In quarter three, 792 (58%) of incidents reported were about individuals, up 11% from 712 in Q2. The number of malware reports from individuals has jumped significantly, with more than double those received in the previous quarter. Individuals reported over 80% of all malware reports this quarter.

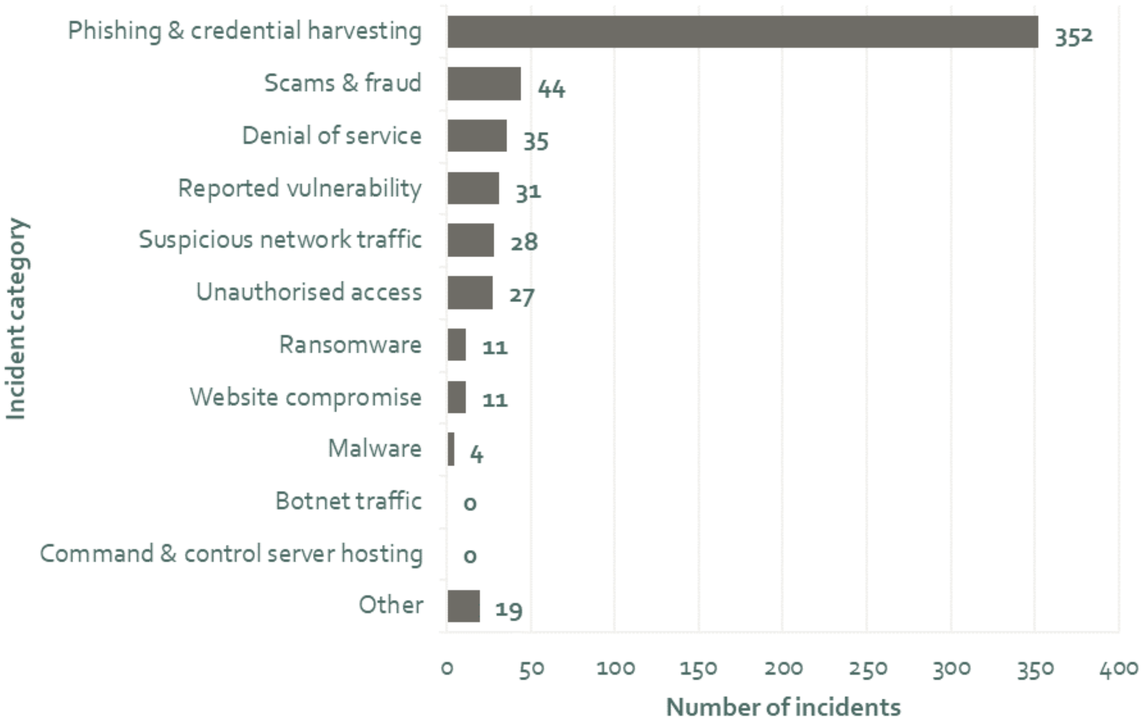
Figure 4: Breakdown of incidents about individuals



Breakdown of incidents about organisations

562 (42%) incidents reported were about organisations, up 16% from Q2. There was a 133% increase in Denial of Service reports affecting organisations, with 35 being reported, up from 15 in the previous quarter (In Q3, we noted a decrease in the number of Suspicious Network Traffic reports from organisations from last quarter, down 56% from 63 (Q2) reports last quarter to 28 (Q3).

Figure 5: Breakdown of incidents about organisations

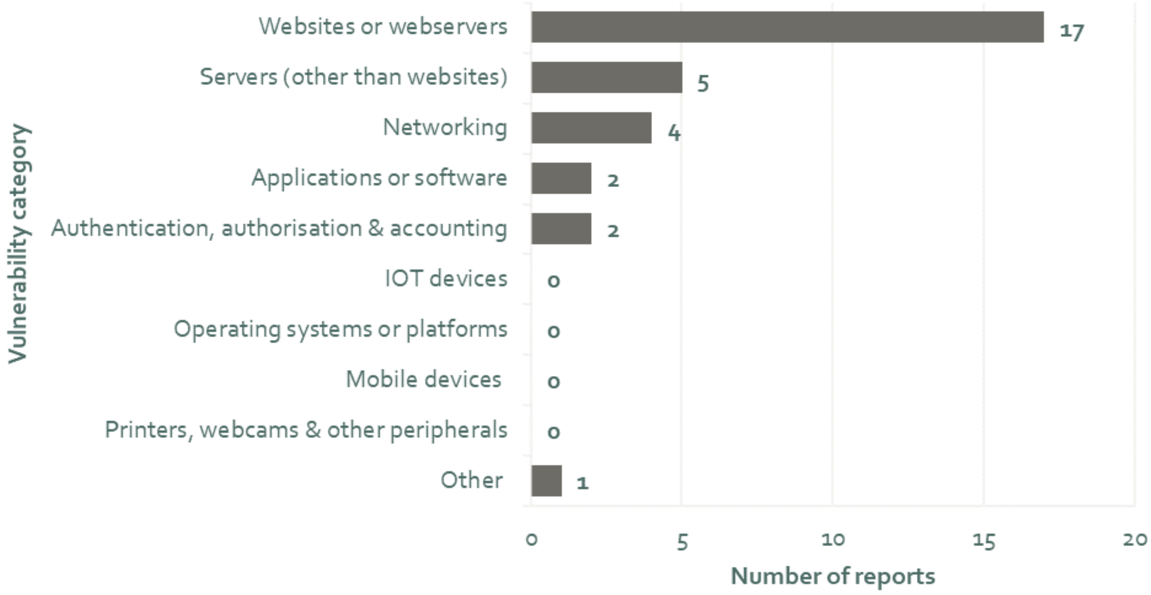


Breakdown of reported vulnerabilities

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.

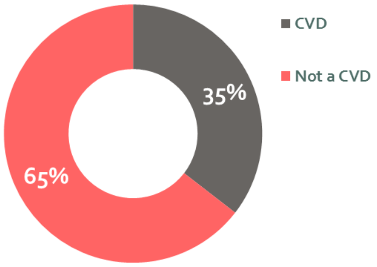
CERT NZ received 31 vulnerability reports, up from 15 in Q2. While a small amount, this represents a 107% increase in the number of reported vulnerabilities reported from last quarter.

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 also received 11 vulnerability reports using the CVD policy2, making up 35% of the vulnerability reports received in Q3. Websites and webserver vulnerabilities remain the top vulnerability category reported to CERT NZ, comprising 55% of reported vulnerabilities, as compared to 33% in Q2.

Figure 7: Proportion of coordinated vulnerability disclosures

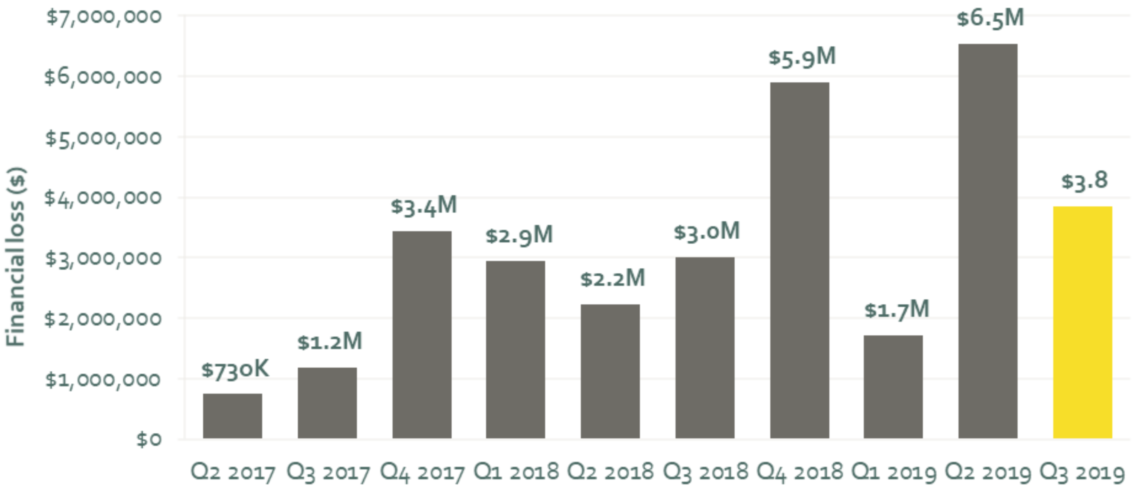


[2] https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/

Total financial losses

Direct financial losses totalled $3,843,543 this quarter. This is a 41% decrease from the reported losses in Q2.

Figure 8: Direct financial losses per quarter



Distribution of direct financial loss

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

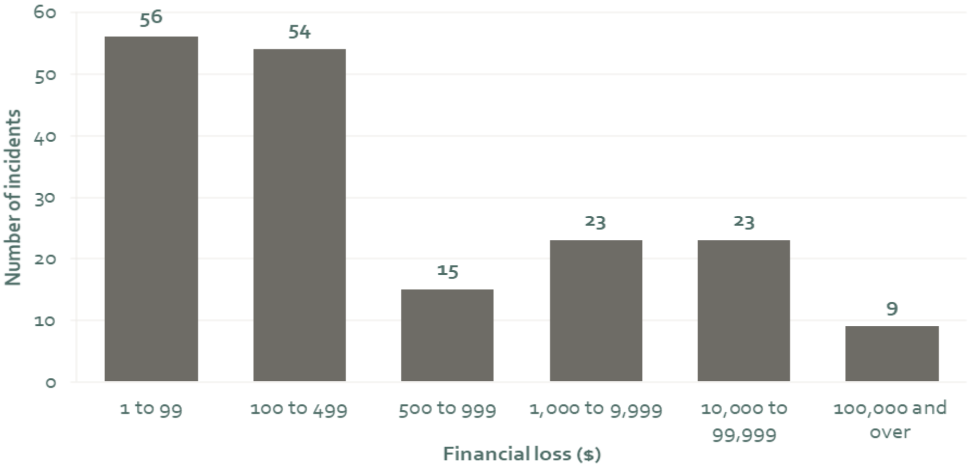
- Organisations reported $1,834,191 (48% of all direct financial loss).
- Individuals reported $2,009,352 (52% of all direct financial loss).

For individuals where a date of birth and loss amount was provided, the average amount lost from incidents was $13,851, and the average age was 45.

During this quarter, nine incidents involved losses of $100,000 or more. All of these incidents were scams and fraud, of which six involved the unauthorised or falsified transfer of money scams.

The percentage of incidents reporting direct financial loss was 13% (180). This is a 21% decrease from the 205 incidents reporting direct financial loss in Q2 2019.

Figure 9: Distribution of direct financial loss



Types of loss

Of the incidents reported this quarter, 18% (243) reported some type of loss (not only financial). This number is down from the 277 incidents that reported some type of loss last quarter. Note that some reports include multiple types of loss.

Reported losses are broken down by type, as follows:

Table 2: Types of loss

15%	**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, like the cost of contracting IT security services or investing in new security systems after an incident (Q2 2019: 17%).
1%	**Reputational loss:**	Damage to the reputation of an individual or organisation as a result of being the victim of an incident (Q2 2019: 2%).
4%	**Data loss:**	Loss or unauthorised copying of data, business records, personal records and intellectual property (Q2 2019: 3%).
0%	**Technical damage:**	Impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation (Q2 2019: 0%).
0%	**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 2019: 2%).
1%	**Other:**	Includes types of loss not covered in the other categories (Q2 2019: 1%).

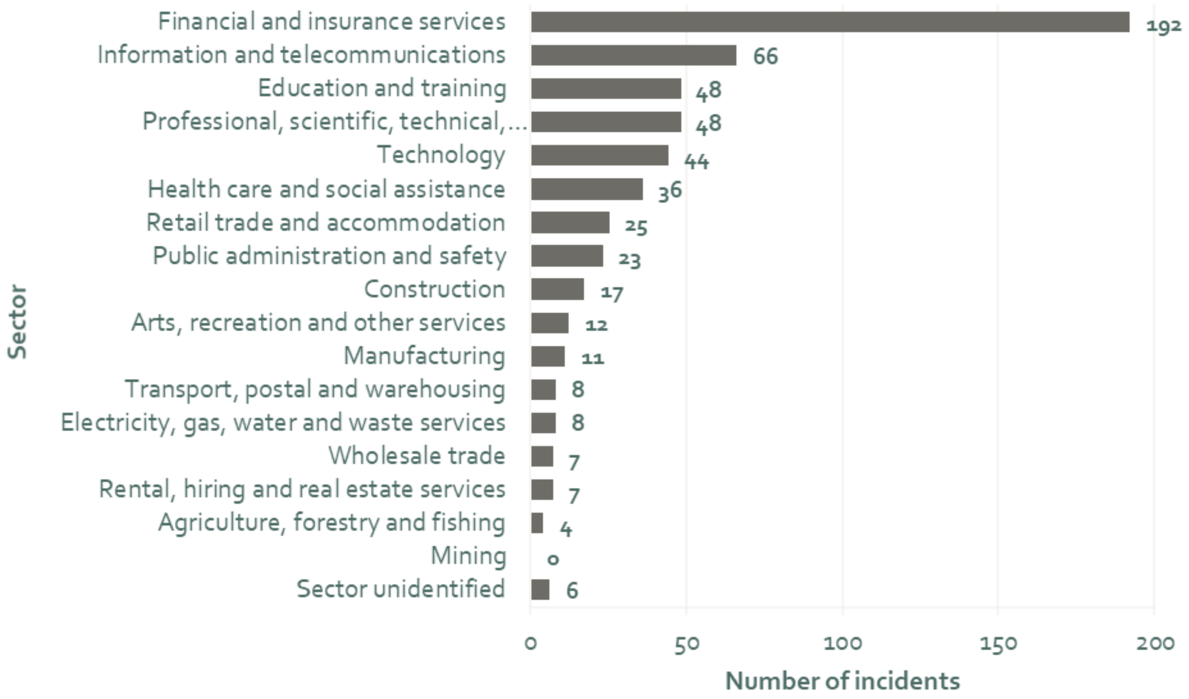
5. Demographics

Reporting by sector

Of the 562 incidents reported about organisations, the three sectors with the most reports were:

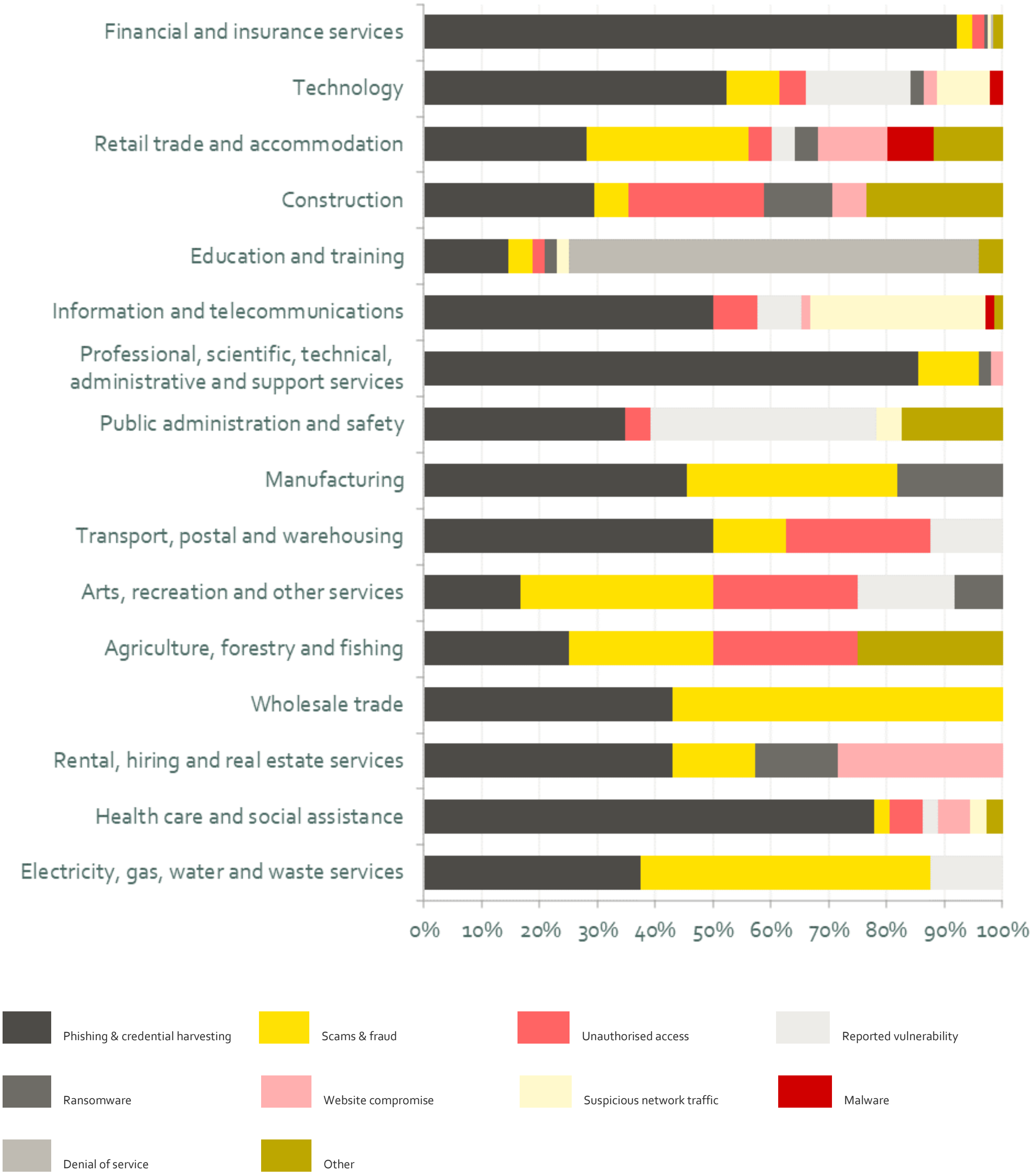
- Financial and insurances services, 192 (34%)
- Information and telecommunications, 66 (12%)
- Education and training, 48 (9%).

Figure 10: Reports about organisations; breakdown by sector



All sectors have been affected by phishing and credential harvesting, and scams and fraud this quarter. Unauthorised access was also broadly reported (across 11 sectors). 94% (34 of 36 incidents) of all Denial of Service reports came from the education and training sector. Denial of Service reports comprised 71% of incidents affecting the education and training sector for Q3.

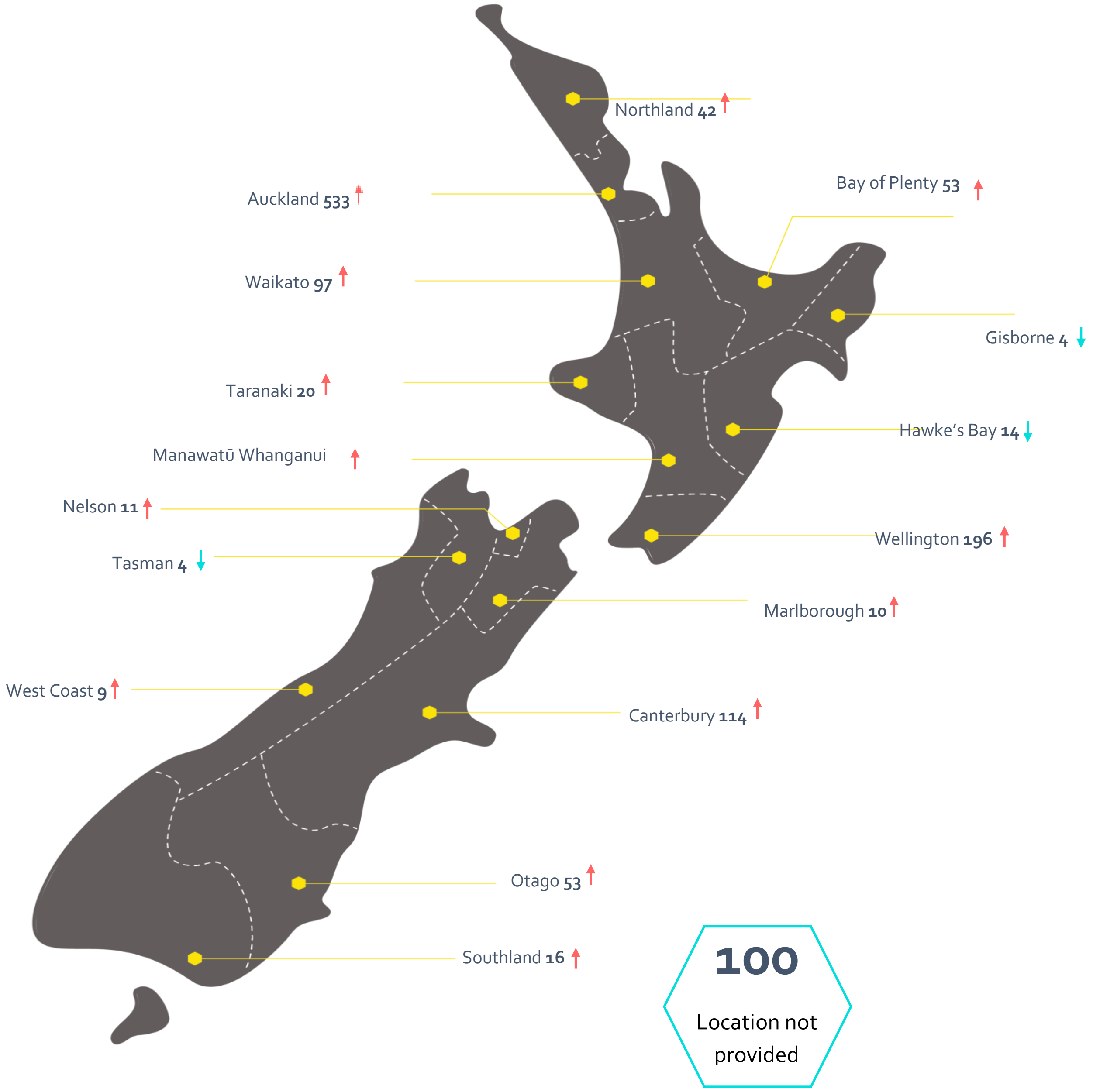
Figure 11: Breakdown by sector and incident category



Reporting by region

Incident reports increased in most regions, with the exception of Gisborne, Hawke's Bay and Tasman. CERT NZ has seen a steady rise in incident reports over the past year from Canterbury, Otago, Waikato and Manawatū/Whanganui. The number of reports not linked to any region has declined from Q2 2019 to Q3 2019, by 42%.

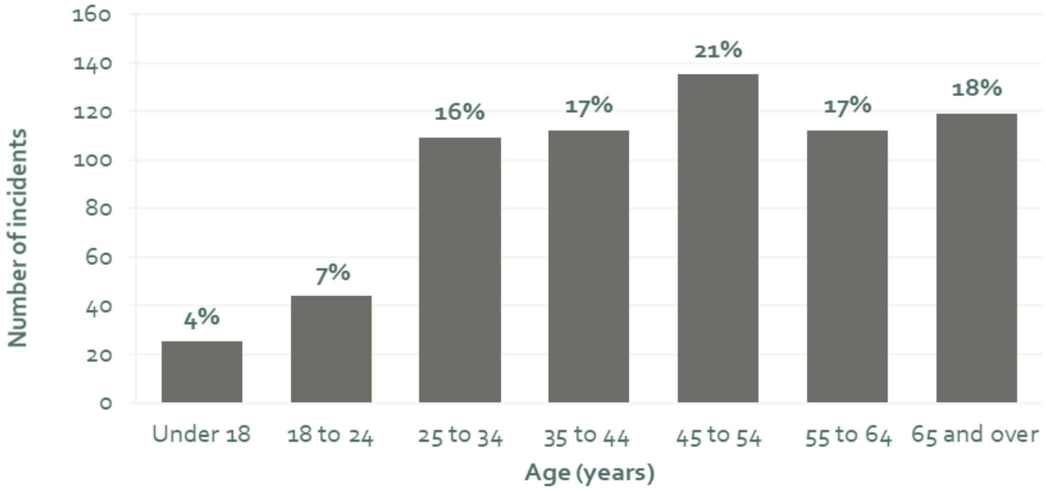
Figure 12: Breakdown of reports by region



Reporting by age

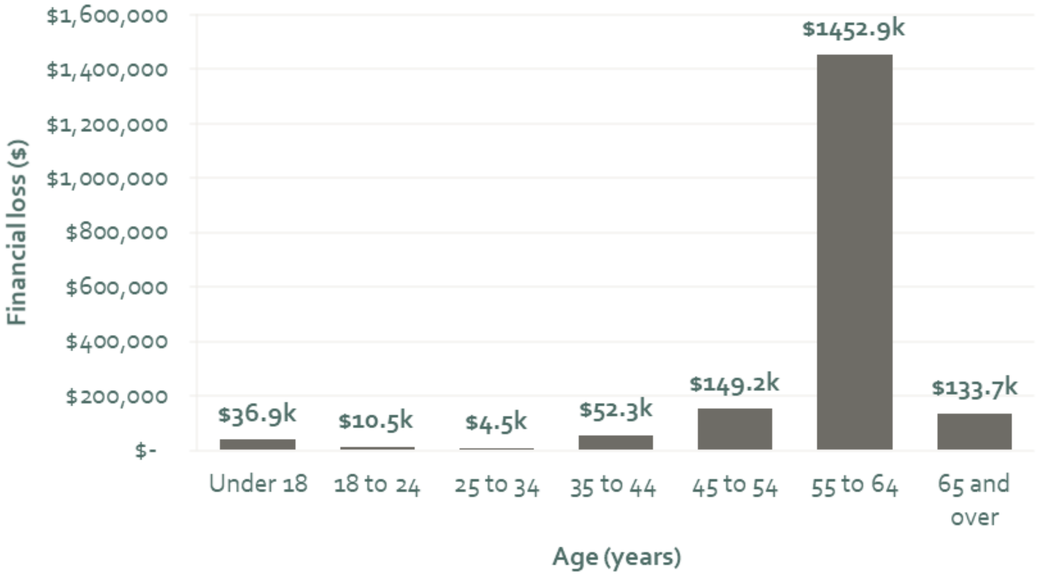
Of the 792 incidents reported about individuals, 656 (83%) provided their date of birth. Those in the 45 – 54 age group reported the most incidents, with 135 reports (21%). This is the first time that this age group has been the top reporters of incidents— in previous quarters the Over 65s were consistently the top reporting age group.

Figure 13: Reports about individuals; breakdown by age



While New Zealanders of all age groups experienced incidents, in this quarter those in the 55 – 64 age group experienced the greatest direct financial loss, accounting for 89% of the total of direct financial losses. The amount lost for this age group this quarter decreased by 64% from Q2 2019 ($ 4,068,511).

Figure 14: Distribution of direct financial loss reported by age



Of the 128 incidents about New Zealand individuals where a date of birth and loss amount was provided, the average loss was $21,353.02 and the median loss was $287.58

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
$36,872	$10,521	$34,283	$52,235	149,173	$1,452,938	$133,748

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. We are the first port of call for New Zealand individuals, businesses and organisations needing to report a cyber security problem.

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 undertake 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 the Privacy and Information statement published on our website. This report is subject to the CERT NZ standard disclaimer.

We base our sectors 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 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 owner's knowledge. They 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 is either stopped 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. Malware 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. 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 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.