certnz

Quarterly Report

Q4

1 October – 31 December
2017

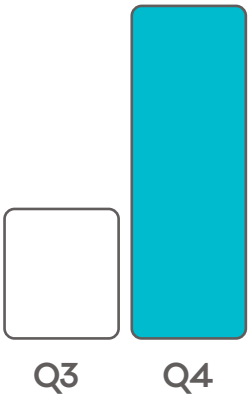
newzealand.govt.nz

Executive summary ///

Welcome to **CERT NZ's** report for the fourth quarter (Q4) of 2017, which provides essential information about the latest cyber security threats and incidents, and includes a summary of results for 2017.

Financial losses from cyber security incidents more than doubled during Q4

The value of the financial losses from reported incidents during this quarter was **$3,436,568**; more than double the losses reported in Q3. This includes nine incidents involving financial loss over **$100,000** each. In fact, 46% of incidents reported to CERT NZ during Q4 involved some form of loss, compared with 29% during Q3.



The value of the financial losses from reported incidents during this quarter was **$3.4 million**; more than double the losses reported in Q3.

New twists on familiar scams

Attackers have been hard at work developing new variations on existing scams, including:

- The evolution of fake tech support scams, with the use of fake websites to lure unsuspecting users.
- Scammers running fake investment websites and phishing email campaigns to steal cryptocurrencies.
- Users being tricked into installing malware designed to steal digital currencies from their e-wallets.

Cryptocurrency scams on the rise

Attackers are seeking to take advantage of increased investment in cryptocurrencies by New Zealanders. During Q4, 10% of scam and fraud cases reported to CERT NZ involved cryptocurrencies, resulting in losses of **$262,323**. We explore these scams in more detail in the focus area section in the back of this report.

Director's message

Since our launch in April 2017, we have advised hundreds of New Zealanders from all walks of life on a wide range of cyber security incidents. We've referred dozens of incidents to other government agencies for investigation, and prevented many potential incidents before they even occurred.

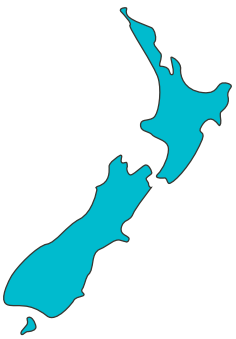
The insights gained from incident reports, combined with the intelligence gathered from the global CERT community help us form a better understanding of the threat landscape as it affects New Zealand. This robust data helps us provide New Zealand-specific advice and guidance to help people stay safe online. As we gather more information we will continue to provide insights across our constituency, from technical experts to everyday New Zealanders.

During Q4 we used our threat landscape information to issue advisories[1] about technical threats like KRACK vulnerabilities in Wi-Fi networks, and successfully staging our first nation-wide cyber security awareness campaign, 'Cyber Smart Week'[2].

CERT NZ also plays a connecting role, working alongside partner agencies to ensure that people get the best help. This quarter we not only referred almost 150 incidents to other agencies such as the NZ Police, Netsafe, and the National Cyber Security Centre (NCSC), our online reporting tool has also automatically directed more than 70 people to the appropriate external agencies for further assistance, such as the Department of Internal Affairs.

The focus area on cryptocurrencies at the back of this report is another good example of the central role we play. We gathered intelligence from our international counterparts and worked with other government agencies that are seeing the impacts of cryptocurrency scams across the financial and regulatory sectors. We combined this information with the incident reports we received to provide actionable advice.

We will continue to provide clear, trusted advice for all New Zealanders in the future.



> "This robust data helps us provide New Zealand-specific advice and guidance to help people stay safe online."

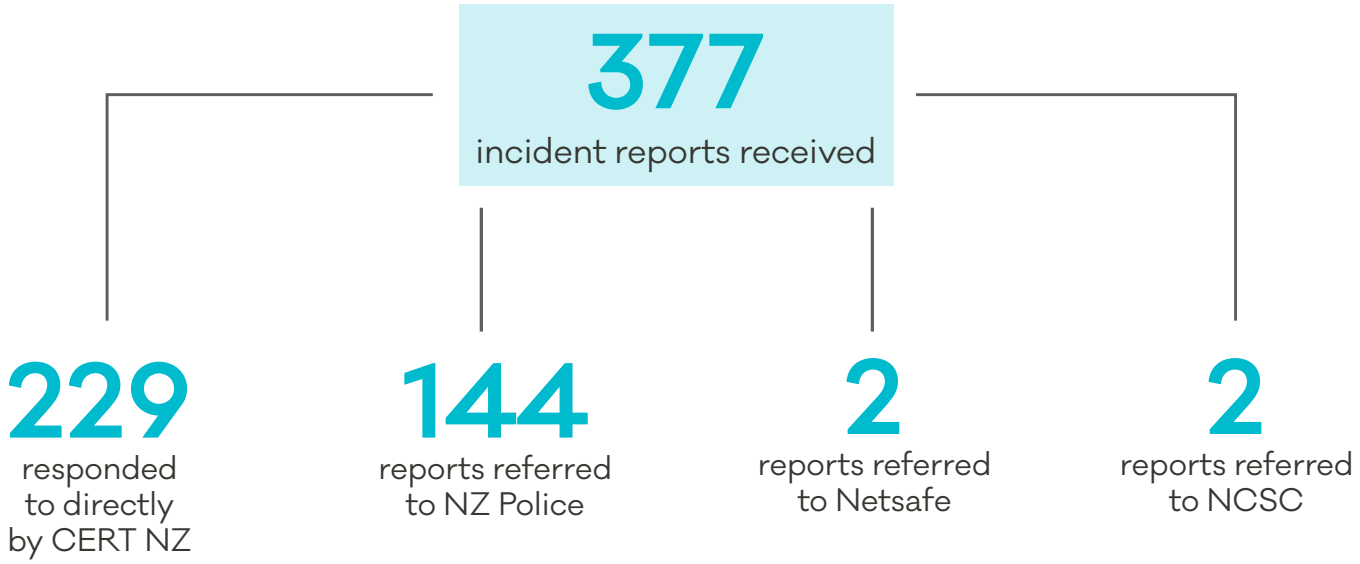
Rob Pope
Director, CERT NZ

1. https://www.cert.govt.nz/it-specialists/advisories/
2. https://www.cert.govt.nz/cybersmart/

Results ///

Between 1 October and 31 December, 377 cyber security incidents were reported to CERT NZ, similar to the 390 incidents in Q3.

Referrals to NZ Police increased whilst referrals to Netsafe decreased, and for the first time we have included the number of referrals to the National Cyber Security Centre (NCSC) in our figures.



Automatic handover from our website

When people report incidents to CERT NZ via our website, our online reporting tool can automatically direct them to the correct agency when it identifies that the issue is most likely outside CERT NZ's scope. We refer them to the agency that can give them the help they need. For example, spam is automatically passed to the Department of Internal Affairs (DIA), and instances of cyberbullying are automatically sent to Netsafe. For the first time this quarter we are sharing these direct website handover numbers. These numbers are not included in any further analysis in this report as they are managed by the external agencies.

48 website handovers to Netsafe

19 website handovers to DIA

8 website handovers to NZ Police

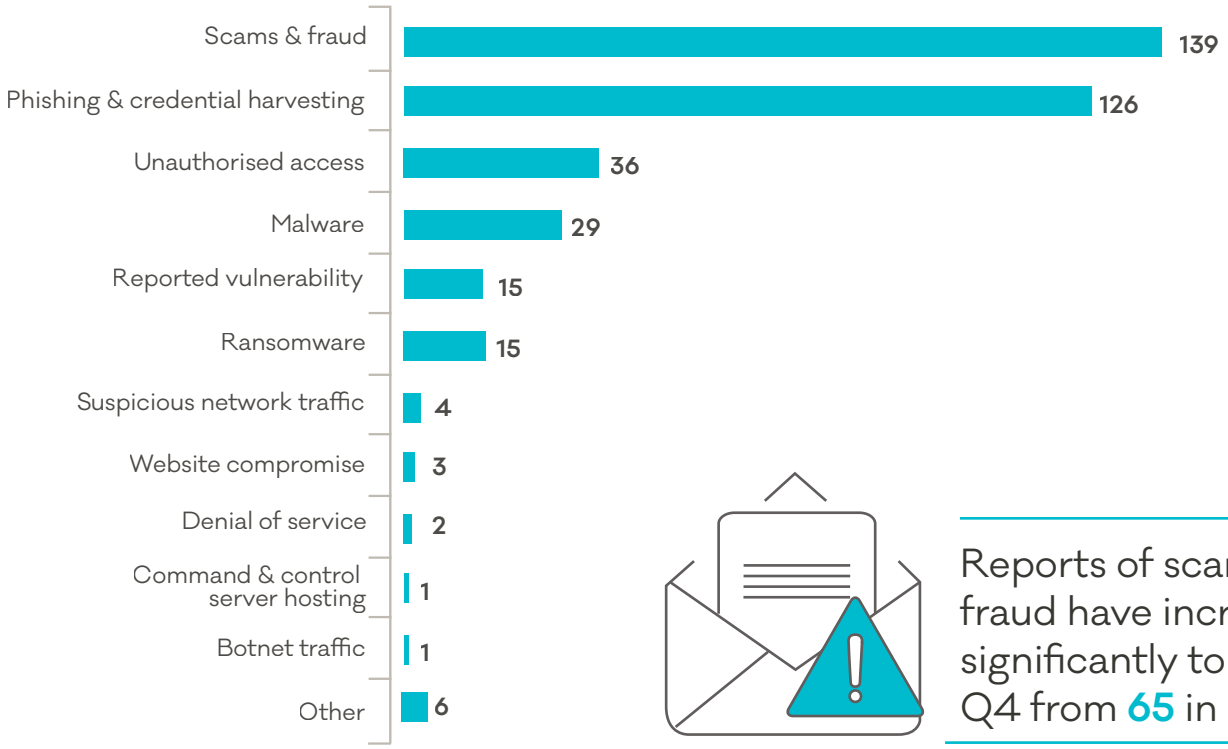
3. Information on our partners can be found at https://www.cert.govt.nz/about/our-partners/

Breakdown by category:

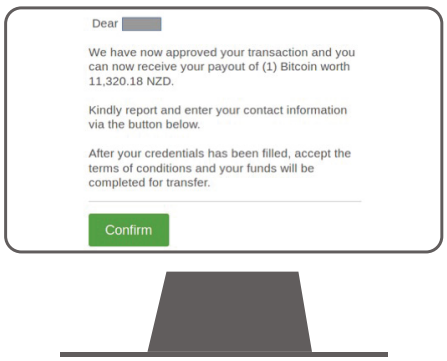
CERT NZ received **377** incident reports in Q4. This quarter we have expanded our category reporting to include all incidents, including those referred to NZ Police and Netsafe.

In Q4 the most commonly reported incident types were scams & fraud (37%) and phishing & credential harvesting (33%), followed by unauthorised access (10%), malware (8%), reported vulnerabilities (4%), and ransomware (4%).

The number of unauthorised access reports received has remained consistent throughout 2017. While not the largest in terms of volume, these incidents can have serious impacts when they occur. We explore this category in further detail on page 9 of this report.



Reports of scams and fraud have increased significantly to **139** in Q4 from **65** in Q3[4].



Case study - Get savvy about scam emails

Not everyone who reports a scam to CERT NZ has fallen for it. An individual received an email with an invoice that looked like it came from one of their software suppliers. When they checked the company's security alerts online, they found an alert that this was a scam along with an exact copy of the scam email and invoice. They reported it to CERT NZ, helping us gain a better understanding of the threats faced by New Zealanders.

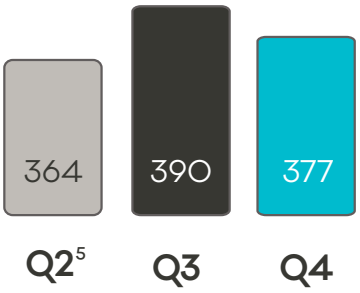
4. Work has been done to retrospectively re-categorise all reports received by CERT NZ, including those that have been referred to NZ Police, Netsafe, and NCSC. Because of this, the figures in this report cannot be directly compared with the Q2 and Q3 reports in 2017.

2017 Summary

1,131

incidents were reported to **CERT NZ** in 2017

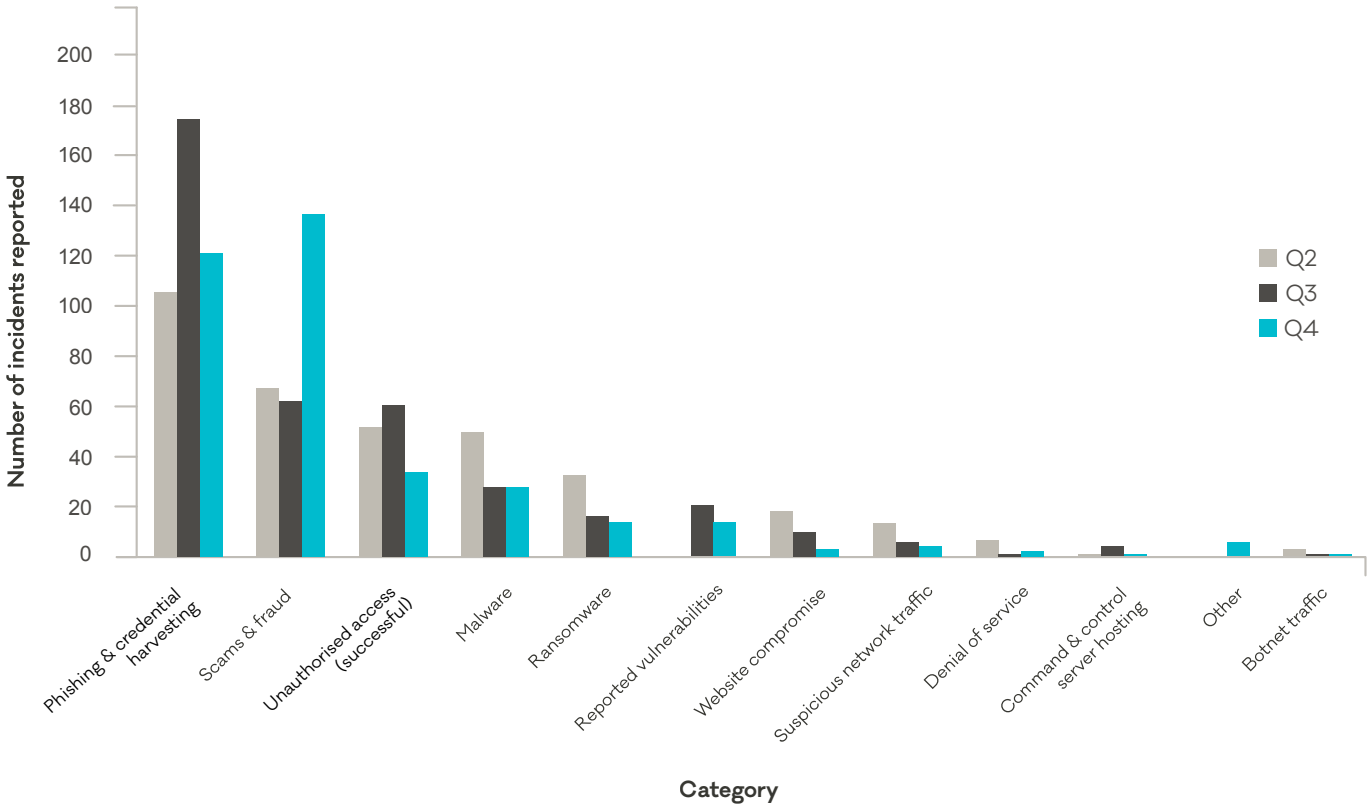
The number of **incidents** reported per quarter has remained fairly consistent:



Notable trends in reporting activity in 2017 include greater numbers of ransomware reports during the Wannacry and NotPetya ransomware campaigns in Q2. Since then, ransomware reports have significantly declined. There was a considerable increase in reports of scams and fraud in Q4, most likely resulting from the inclusion for the first time of incidents that were reported to CERT NZ and then referred to NZ Police.

Since the launch of CERT NZ's co-ordinated vulnerability disclosure service (CVD) in July 2017, we have seen a steady stream of vulnerability reports in Q3 and Q4.

2017 category distribution of all reported incidents

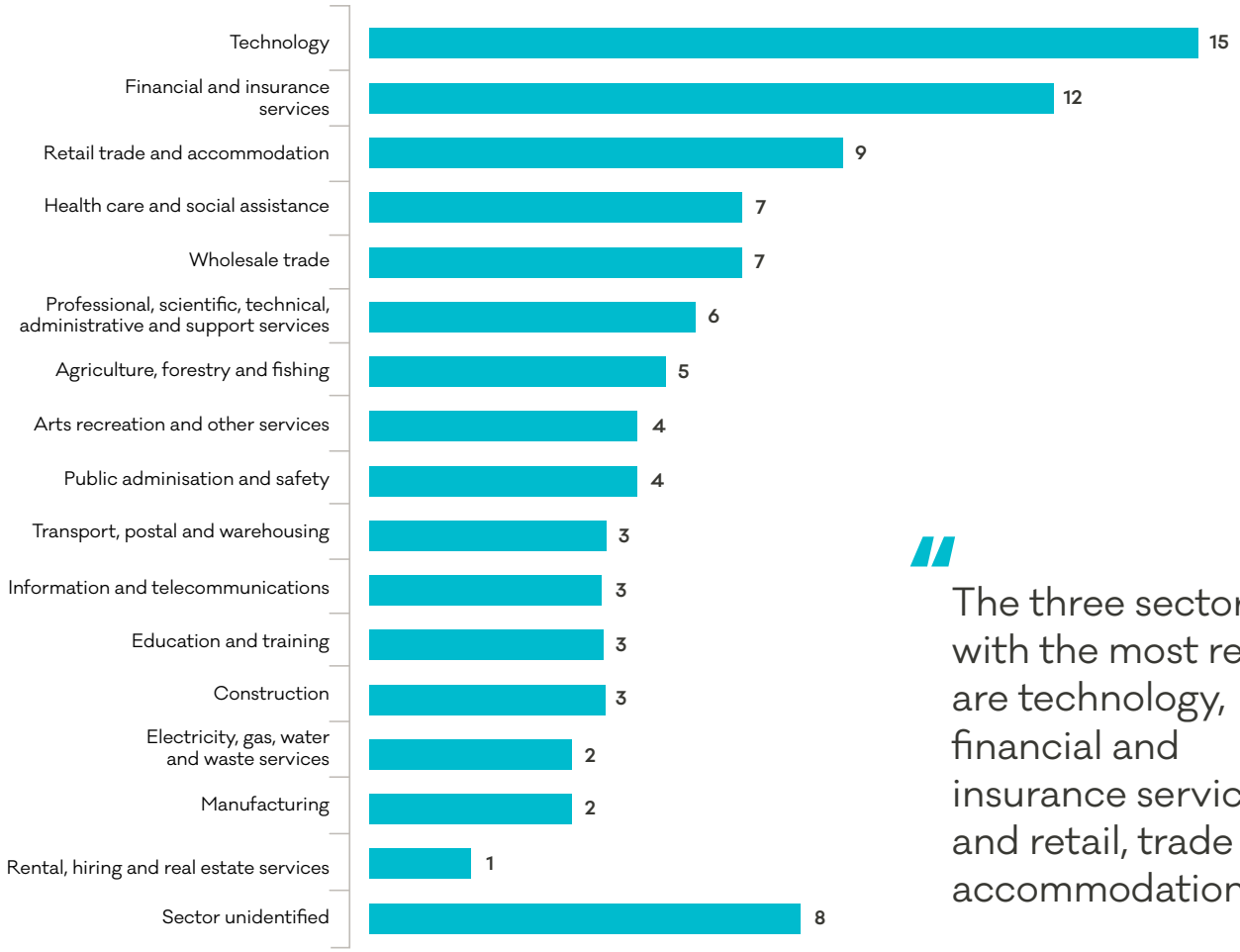


5. CERT NZ was established in April 2017, during Q2

Reporting by sector

Reports about individuals accounted for 75% of all reports received by CERT NZ in Q4 (up from 57% in Q3), including reports referred to other agencies.

Of the 25% of incidents that were reported about organisations, the three largest sectors[6] involved were technology (16%), financial and insurance services (13%), and retail trade and accommodation (10%).



> The three sectors with the most reports are technology, financial and insurance services, and retail, trade and accommodation.

Case study - Don't share verification codes

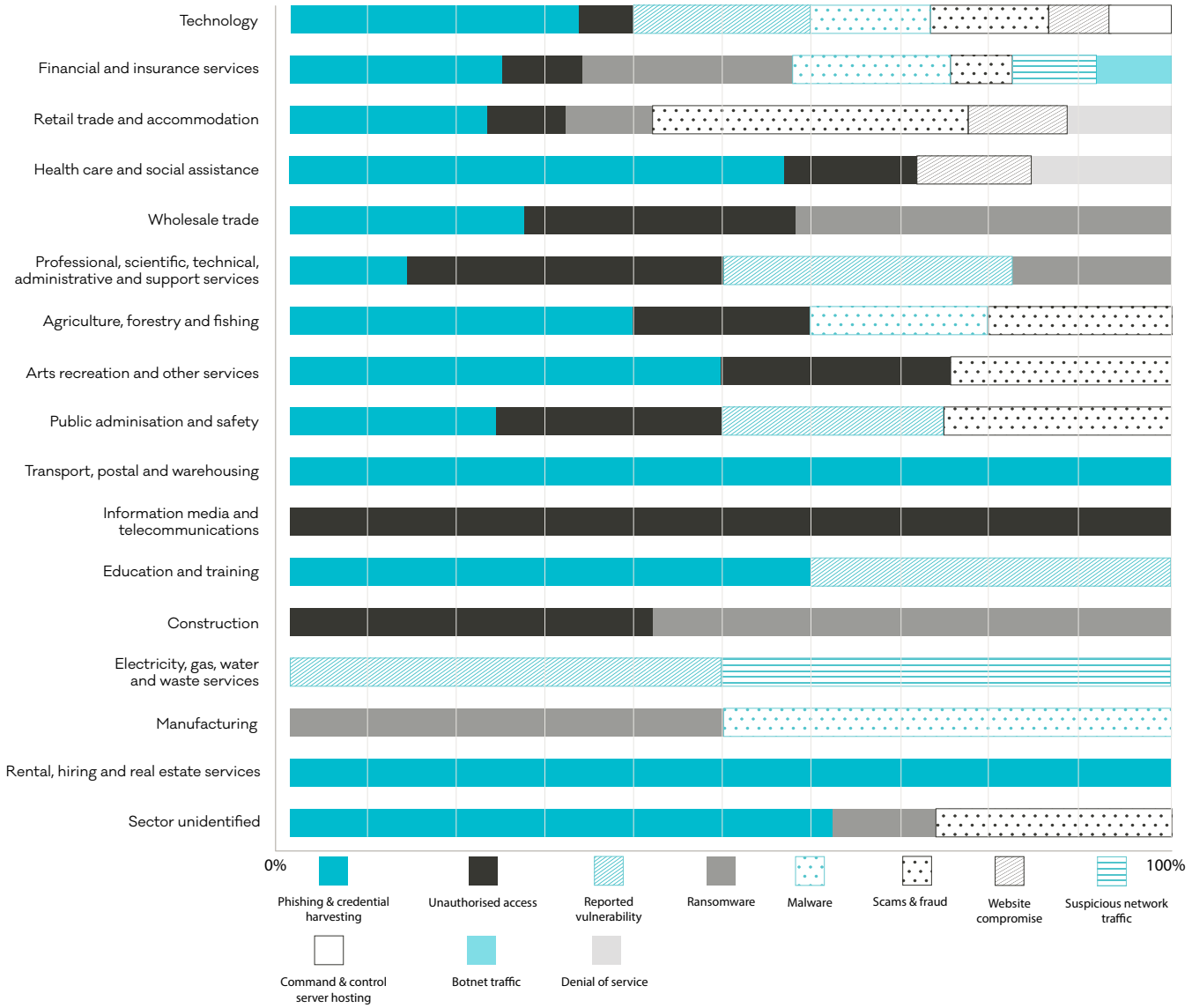
An individual contacted CERT NZ about their Google account. They had received a message from a friend's Facebook account saying they had been locked out of their Google account and needed help to get back in. The individual was asked to forward the Google verification code that was sent to their phone. They thought the request was genuine and replied, with the verification code they had received from Google. The request had not actually come from their friend. Instead an attacker had hacked into their friend's Facebook account. The verification code sent by the individual was used by the attacker to gain control of the individual's Google account, which they then used to access more of the friend's accounts, and those of their other contacts. The case was referred to NZ Police for further investigation.

6. The sectors are based on the Statistics NZ New Zealand Standard Industry Output Categories (NZSIOC). Percentages are calculated solely using sector reports.

Reporting by sector: incident category breakdown

The chart below shows how widespread cyber security incidents are across all sectors, and how sectors are affected by multiple types of threats. As organisations increasingly rely on technology, understanding how cyber security incidents can impact New Zealand businesses is crucial.

We have also received reports of vulnerabilities in systems across several sectors, which underscores the importance of having good IT security practices for all businesses, regardless of their industry.



Most incidents reported by organisations in Q4 were in the following categories:

↓ **35%** Phishing & credential harvesting (Q3: 38%)

↑ **14%** Scams & fraud (Q3: 3%)

↓ **12%** Reported vulnerability (Q3: 16%)

↓ **13%** Unauthorised access (Q3: 17%)

Unauthorised access

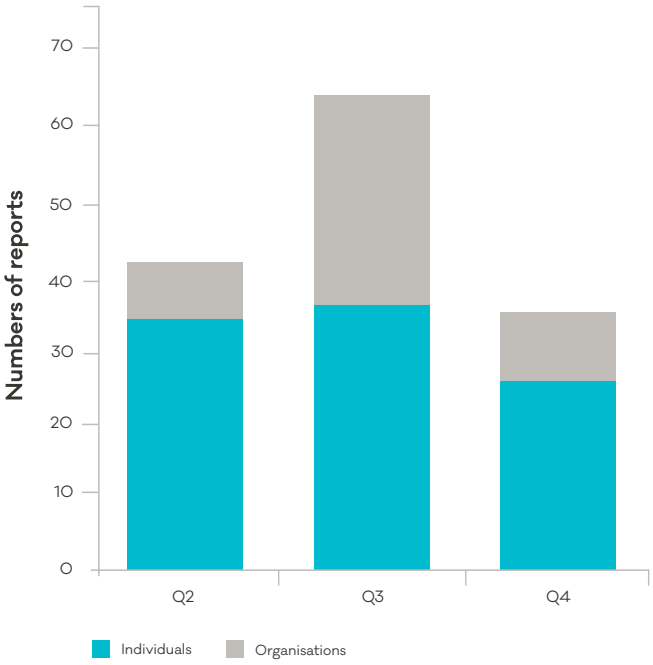
Unauthorised access can enable an attacker to conduct a wide range of malicious activities on a network, infrastructure or computer. Instances of unauthorised access are often serious and are a specific offence in New Zealand under the Crimes Act[7].

These activities are generally categorised under 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.

Reports to CERT NZ of unauthorised access have been relatively consistent throughout 2017. While organisations frequently identify attempts to access their networks, successful breaches that bypass security systems to compromise a network are less common. However, when they occur, these breaches can result in serious consequences.

Unauthorised access reports in 2017



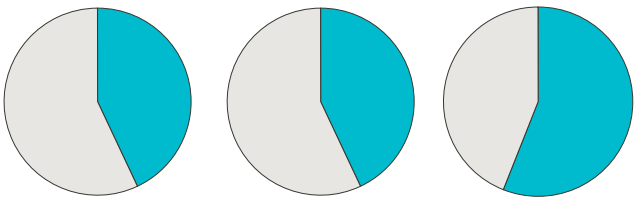
Most of the unauthorised access incidents we have seen use **phishing emails** to trick users into giving up their credentials, giving attackers access to the system.

Other attackers use emails with attachments containing hidden malware or links to websites that install malware on users' computers. A few instances have also involved unauthorised access to systems occurring after attackers have conducted brute force attacks by exploiting vulnerabilities in software.

Once an attacker has gained access, their activities may be 'noisy', such as installing ransomware or causing disruption, or 'stealthy', such as stealing information, installing key loggers, or establishing a sustained presence on the network.

56% of the unauthorised access incidents reported in Q4 involved some form of loss as a result of the attack. This is the highest proportion recorded since reporting began[8].

% of unauthorised access incidents that reported loss

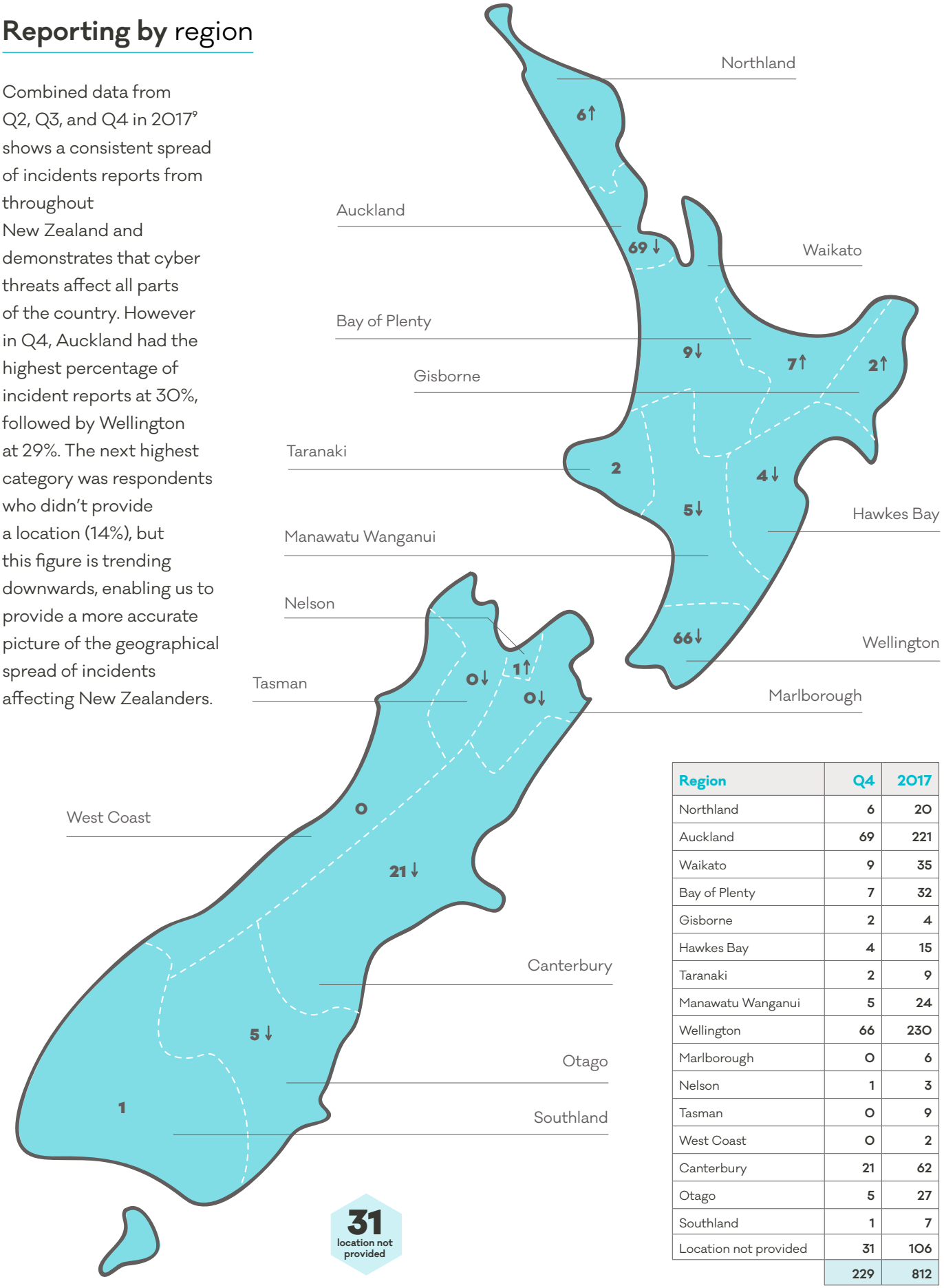


Q2 43 % **Q3 43 %** **Q4 56 %**

7. Section 252 of the Crimes Act http://www.legislation.govt.nz/act/public/1961/0043/latest/DLM327382.html
8. Q2 numbers in the graph do not include reports referred to NZ Police.

Reporting by region

Combined data from Q2, Q3, and Q4 in 2017[9] shows a consistent spread of incidents reports from throughout New Zealand and demonstrates that cyber threats affect all parts of the country. However in Q4, Auckland had the highest percentage of incident reports at 30%, followed by Wellington at 29%. The next highest category was respondents who didn't provide a location (14%), but this figure is trending downwards, enabling us to provide a more accurate picture of the geographical spread of incidents affecting New Zealanders.



Region	Q4	2017
Northland	6	20
Auckland	69	221
Waikato	9	35
Bay of Plenty	7	32
Gisborne	2	4
Hawkes Bay	4	15
Taranaki	2	9
Manawatu Wanganui	5	24
Wellington	66	230
Marlborough	0	6
Nelson	1	3
Tasman	0	9
West Coast	0	2
Canterbury	21	62
Otago	5	27
Southland	1	7
Location not provided	31	106
	229	812

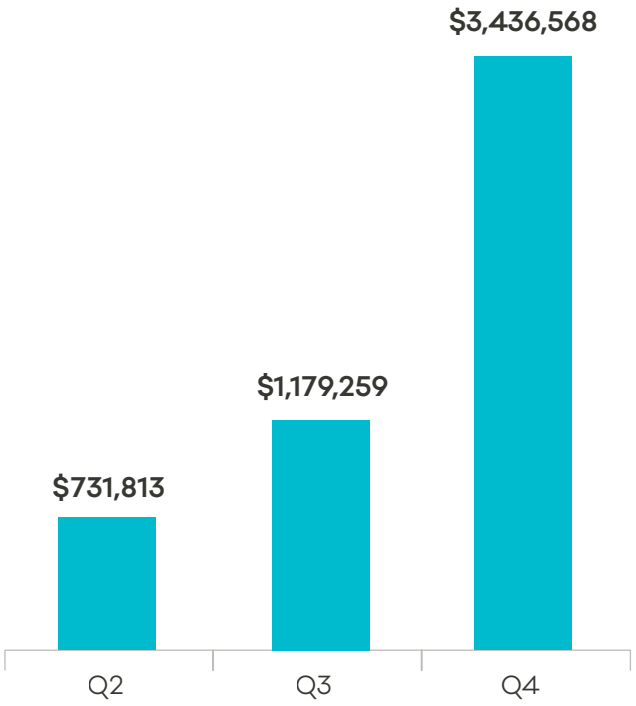
9. Regional data includes reports responded to by CERT NZ only.

Impacts ///

over 3.4 million

in **direct financial loss** has been reported to **CERT NZ** in Q4.

In Q4, reported financial losses totalled $3,436,568 (more than twice the amount of financial losses reported in Q3) due to a number of reported losses over $100,000.



Three quarters of all reports received by CERT NZ in Q4 were about individuals and of these, 77% involved some kind of loss. The spread of financial loss, between reports about individuals, and those about organisations in Q4 was:

- organisations reported **$2,058,631** (60% of all reported financial loss)
- individuals reported **$1,377,937** (40% of all reported financial loss)

These impacts are self-reported and are not verified. Impacts analysed in this section include all incidents reported to CERT NZ, including incidents referred to the NZ Police and Netsafe.

> Over **$5.3 million** in loss was reported to CERT NZ in 2017

Case study - Overseas company director's email hacked

A small New Zealand company reported fraudulent requests sent from the email account of one of the company's overseas-based directors. Someone had hacked the director's email account and used it to send requests for money to be transferred to accounts in a third country. Similar genuine requests had been received previously, so the money was sent, along with notification of the transfer in emails back to the director. The attacker intercepted these notification emails and responded to them pretending to be the director so the company would not be alerted to the scam. The attacker's activity was only caught when the foreign receiving bank found that the information they were provided didn't match up and queried a transfer. The case was referred to NZ Police for further investigation.

Parties reported different types of loss broken down as follows. These may include multiple types of loss:

34% 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 (Q3: 13%).

4% Data loss:

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

2% 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: 3%).

1% Reputational loss:

Damage to the reputation of an individual, business or organisation as a result of being the victim of an incident (Q3: 2%).

1% Technical damage:

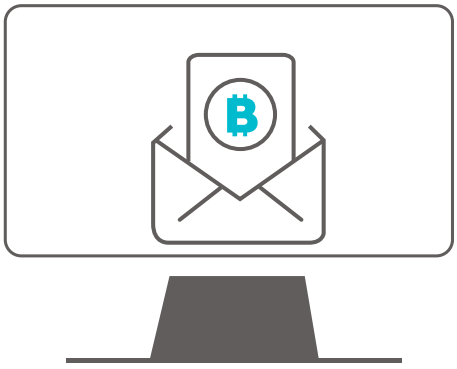
Impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation (Q3: 2%).

6% Other

Includes specific types of loss not covered in the other categories (Q3: 7%).

Case study - Watch out for fake 'security issues' emails

A cryptocurrency trader reported a Bitcoin theft to CERT NZ. The trader received an email that said their Bitcoin account had security issues, along with a link. They followed the link to a legitimate-looking website and logged on. The website requested further logons and the trader realised the email was a hoax, but by then their Bitcoin had already been stolen from their account. Although CERT NZ referred the case to the NZ Police, it is unlikely the trader's Bitcoin can be recovered.



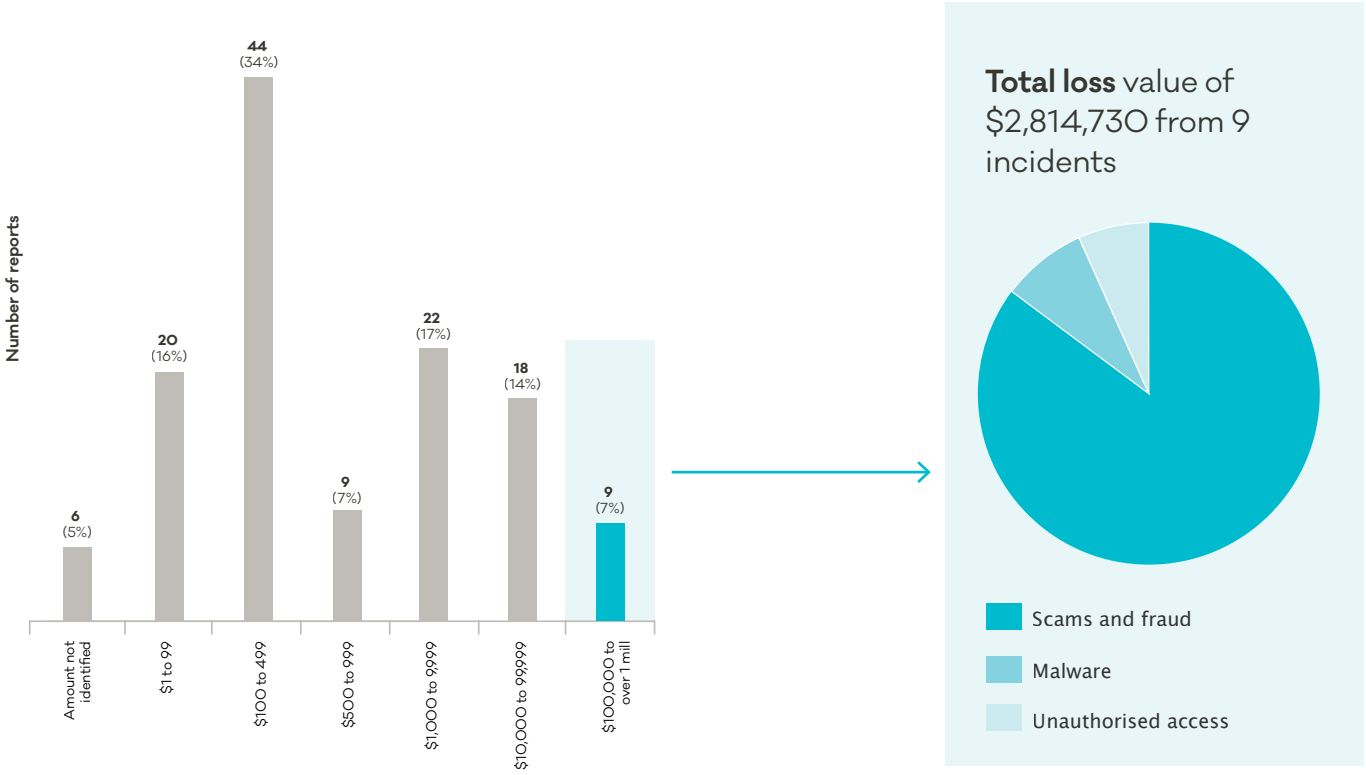
High value losses reported in Q4

Direct financial losses reported in Q4 were higher than in previous quarters largely because of an increase in the number of reported losses over $100,000.

During Q4, nine incidents involved losses of over $100,000, a total loss of $2,814,730.
Of these nine incidents:

- 6 involved scams and fraud resulting in losses of **$2,397,911**.
- 2 involved malware resulting in losses of **$228,659**.
- 1 involved compromise via unauthorised access resulting in losses of **$188,160**.

Q4 distribution of financial loss



Case study - Don't download fake crypto-wallets

CERT NZ received a report about cryptocurrency stolen using a fake Electrum wallet. The individual had searched the term 'Electrum' and clicked on a link in the list returned without doing any further research. They downloaded and launched an application. Once they had entered their details they realised that something was wrong with the application. When they checked the blockchain, they saw that their cryptocurrency had been transferred to another address. The loss was over $100,000 at the time of the report. The case was referred to NZ Police.

Focus area: cryptocurrency scams

Cryptocurrencies attract scammers

Cryptocurrency has been around since 2008, when Bitcoin and the technology that records its transactions, blockchain, were invented.

In the last year, cryptocurrencies such as Bitcoin and Ethereum have attracted wide-ranging attention, including from cyber criminals.

CERT NZ has received a number of incident reports of scams specifically aimed at stealing cryptocurrencies from unfortunate investors. Cryptocurrency scams featured in only 6% of the incident reports we received during Q4 but the sum lost represents 8% of the total financial loss this quarter – a total of $262,323.

Some of these scams are variations on existing ones, using simple phishing techniques to trick users into giving scammers their passwords and thereby access to their digital wallets. Others are more sophisticated, adapting cybercrime techniques to commit theft.

Tracing and recovering stolen cryptocurrencies is very difficult due to the nature of the technology.

In Q4 CERT NZ received reports of:

Cryptocurrency investment scams.

- These scams operate by sending out emails or setting up fake websites advertising cryptocurrency investment opportunities with attractive returns. Some scams also offer direct sales of cryptocurrencies, such as bitcoin, litecoins, or other altcoins, which don't result in any transfer once the victim has paid.

Stolen cryptocurrencies.

- These attacks use a fake website or application to gain credentials or private keys. These are then used by the criminal to transfer the cryptocurrency.

> Cryptocurrency scams featured in only 6% of the incident reports we received during Q4 but the sum lost represents 8% of the total financial loss this quarter – a total of **$262,323**.

Case study - Beware of Bitcoin buyers

An individual reported a loss related to the sale of their Bitcoin. They had offered to sell their Bitcoin on a site called localbitcoin.com. A buyer had contacted them directly and agreed a price. The buyer had then provided a screenshot of their payment transfer for the Bitcoins, along with a screenshot of their passport and their face. Based on this information, the individual had transferred the Bitcoin to the buyer, but the buyer's payment did not go through to the individual's bank account.

CERT NZ ADVICE

Protect yourself. There are precautions you can take to look after your cryptocurrency.

Two-factor authentication
2FA adds an extra security check on top of your password, making it an extra step harder for someone to access your wallet or exchange account. This can be a randomising token or something only you have, such as a fingerprint.

Password
Set a strong unique password to access your wallet and/or exchange account. We recommend using a passphrase, or a long and strong password, paired with 2FA to limit unauthorized access to your account.

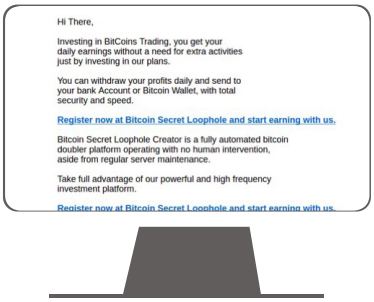
Backup
There are a number of issues that can cause you to lose your wallet, such as ransomware, your device breaks, or your wallet is deleted. Wallets which are used to store cryptocurrency should be backed up to offline storage. Test your backup so you know you can restore it if you need to.

Minimise risk
A cryptocurrency wallet is the same as a normal wallet. Only carry cash with you that you are willing to risk losing. To minimise risk, reduce the amount of money in your cryptocurrency wallet to an amount you are willing to lose and keep the rest in offline storage.

Encryption
Full disk encryption on all devices (from laptop to mobiles) will reduce the risk that an attacker with physical access to your device could extract your wallet while the device is powered off or locked.

For more information on cryptocurrency
Read the Financial Markets Authority advice: https://fma.govt.nz/investors/ways-to-invest/cryptocurrencies/

Read CERT NZ's advice: https://www.cert.govt.nz/businesses-and-individuals/guides/keeping-yourself-safe-secure-online/cryptocurrency-security/



Case study - Don't throw good Bitcoins after bad

A cryptocurrency trader reported losing money in a Bitcoin investment scam. They had sent Bitcoins to a website offering a return of 20 times their investment. However, the trader then received an email stating that due to price fluctuations they needed to transfer further Bitcoins. The trader did not action the transfer, but has been unable to recover the Bitcoins already sent.

Focus area: tech support scams ///

Hoax websites snare the unsuspecting

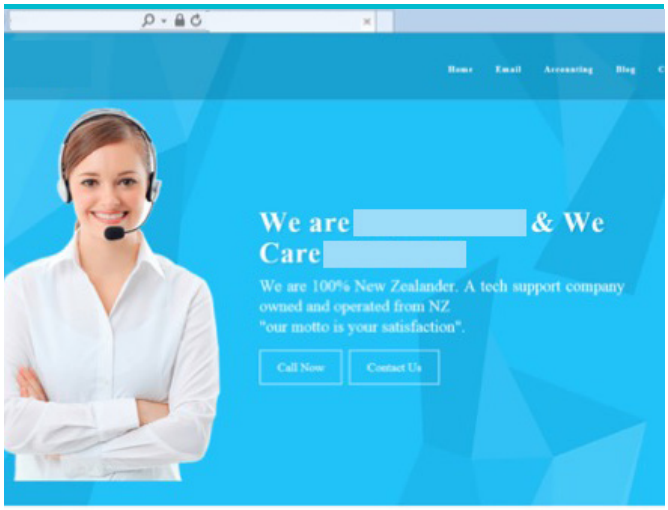
CERT NZ received 16 tech support scam reports in Q4 resulting in reported loss of over **$90,000**. Five of these reports show increased sophistication from earlier reports received in Q2 and Q3.

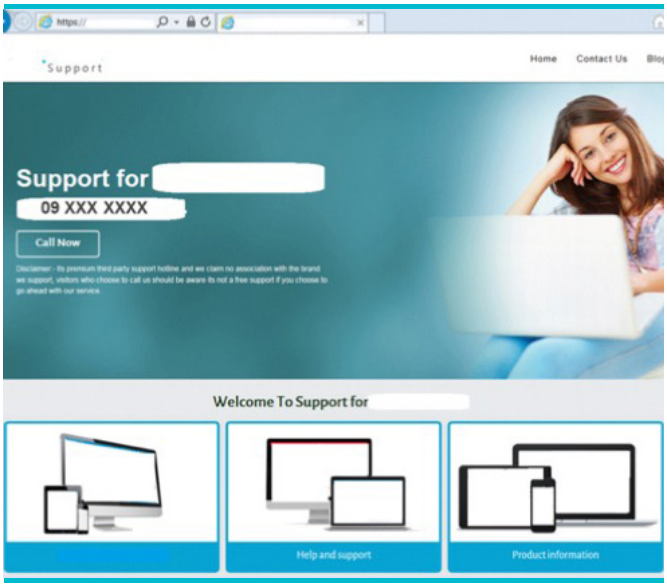
Scammers have been registering hoax tech support websites that take advantage of well-known brand names such as Google, Dell, Toshiba, Samsung, and Xero. They rely on users searching for a genuine product support website and instead finding the scammer's fake support site. Users are typically asked to pay a fee to receive support, but no help is provided and the unlucky users are left out of pocket.

Some websites reported to CERT NZ also listed phone numbers that put the victim in contact with the scammers who continued to push for money, credit card details, and access to the person's computer.

One scammer in particular had registered multiple domains for '.nz' websites and pretended to provide support in order to conduct scams. Their websites used terms that made them more prominent in search engine results for tech support queries. CERT NZ has been engaging with NZ Police and the Domain Name Commission to investigate the scammer further and address this domain abuse.

Examples of recent tech support scams:





CERT NZ ADVICE

How to stay safe from hoax support websites.

- Stop and think first – not everything on the internet is what it claims to be.
- Take the time to find the real website and support site for the company you want assistance from.
- Be suspicious of any request for money, personal details, or access to your computer. Take time to check out the company or ask someone's advice.
- Many well-known business names are used in scams or phishing. These businesses often have their own security page listing current scams or phishing they are aware of, often including examples. Check directly on their websites for known scams.
- Report scams you have discovered to CERT NZ. This helps to protect others from the scam.

For more information on scams:

- CERT NZ page on scams and fraud: https://www.cert.govt.nz/businesses-and-individuals/explore/scams-and-fraud/?topic=scams-and-fraud
- Consumer Protection's 'Is this a scam?' page: https://www.consumerprotection.govt.nz/get-guidance/scamwatch/identify-a-scam/is-this-a-scam
- Netsafe 'PC Tech Support Scam' page: https://www.netsafe.org.nz/pc-tech-support-scam/

Case study - Watch out for email invoice scams

A New Zealand company reported a sophisticated invoice scam to CERT NZ. Email communications with one of the company's customers had been intercepted by a scammer and replaced with similar domain names for both the company and their customer. This enabled the scammer to control the email communications. When invoices were sent, they replaced them with copies that had altered payment details but otherwise were the same. This allowed the scammer to steal over $100,000. The case was referred to NZ Police for further investigation.

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 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

If any individual or organisation needs to report a cyber security problem, we are a first port of call via www.cert.govt.nz or through **0800 CERT NZ**. Our team of cyber security experts will look into the incident, collect information about it and provide advice. If necessary incidents can be referred to another agency such as NZ Police, Netsafe, Department of Internal Affairs (DIA) and the National Cyber Security Centre (NCSC) if they are best placed to respond, with the customer's consent.

We report on threats by analysing international incidents and trends, track and analyse local data, co-ordinate multi-agency responses to cyber threats and incidents, and generally raise awareness of cyber security best practices in New Zealand.

A word about 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[10] and this report is subject to the CERT NZ standard disclaimer[11].

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 incident reports 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.

10. https://www.cert.govt.nz/about/privacy-and-information-statement/
11. https://www.cert.govt.nz/about/disclaimer/

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 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.

More tips for staying safe online can be found at
www.cert.govt.nz