By the numbers
Mā ngā tau

The NCSC in 2023/24

The NCSC receives and handles incident reports through two distinct triage processes. Most incident reports are handled through the NCSC's general triage process because they do not require specialist technical attention. Often these incidents affect either individual New Zealanders or small to medium businesses. The NCSC acknowledges that while these incidents did not require specialist attention, they remain highly impactful for the people or organisations they affect.

A much smaller proportion of incidents are triaged for more specialist technical support because of the nature of the victim, or the nature of the incident. These incidents could cause high impact at the national level and are referred to as incidents of potential national significance. These are incidents affecting organisations such as operators of critical infrastructure, and those that have the potential to impact large groups of New Zealanders. This report examines both categories of incident and provides analysis of key statistics and trends within them.

7122

Total incident reports recorded by the NCSC

DISRUPTIONS AND INDICATORS

10.3m

In 2023/2024, the NCSC disrupted over 10.3 million malicious cyber events via Malware Free Networks® (compared to 250,000 in 2022/2023).

This exponential growth has continued since the reporting period closed.

28,804

Indicators of malicious activity published in 2023/24 via Malware Free Networks.

11,386

Phishing indicators published in 2023/24 via the Phishing Disruption Service.

343

Incidents triaged for specialist technical support because of potential national significance

Compared to 316 incidents in 2022/2023 - an increase of 8.5%

110

or 32% of 343 incidents of potential national significance indicated links to suspected state-sponsored actors

Compared to 28% in 2022/2023

65

out of 343 incidents of potential national significance, or 19%, were likely criminal or financially motivated

Compared to 28% in 2022/2023

6779

Incidents handled through the NCSC's general triage process, often affecting individual New Zealanders or small to medium businesses

Compared to 7744 in 2022/2023, a decrease of 12.5%

HARM REDUCTION AND FINANCIAL LOSS

$38.8m

$38.8 million worth of harm prevented in 2023/2024. Since June 2016, the NCSC has prevented an estimated $421.2 million worth of harm to Aotearoa New Zealand's nationally significant organisations.

$21.6m

Total financial loss reported to the NCSC in incidents handled through the NCSC's general triage process

Compared to $22.4 million in 2022/2023

Since 2017, the estimated total financial loss reported through the CERT function is $121 million.

THE NCSC IN A TYPICAL MONTH THIS YEAR:

Detected 7 cyber incidents affecting one or more nationally significant organisations through the NCSC's cyber defence capabilities.

Received 22 new incident reports or requests for assistance for incidents of potential national significance. Of the new incident reports received each month, 15 came from international or domestic partners while 7 came from self-reporting by victim organisations.

Recorded 565 incidents handled through the NCSC's general triage process, often affecting individual New Zealanders and small to medium businesses and organisations.

IN THE 2023/2024 YEAR THE NCSC AND GCSB:

Received 143 notifications of network change proposals under the Telecommunications (Interception Capability and Security) Act 2013 (TICSA).

Conducted 21 assessments of regulated space activities under the Outer Space and High-altitude Activities Act 2017 (OSHAA).

Conducted 74 assessments of regulated radio spectrum activities under the Radiocommunications Act 1989.

Provided advice on 39 assessments under the Overseas Investment Amendment Act 2021 (OIAA).

THE NCSC INCREASED AOTEAROA NEW ZEALAND'S COLLECTIVE CYBER RESILIENCE:

Delivered 82 incident reports to customers.

Published 19 advisories for customers, including 16 co-authored with domestic and international partners.

Published 30 critical vulnerability alerts.

Co-chaired 24 sector-based Security Information Exchanges.