NATIONAL CYBER SECURITY CENTRE (NCSC) — NEW ZEALAND

Quarter Two Cyber Security Insights 2026

Source: https://www.ncsc.govt.nz/insights-and-research/insights-reports/quarter-two-cyber-security-insights-2026/
Captured and compiled into this PDF on 19 August 2026.

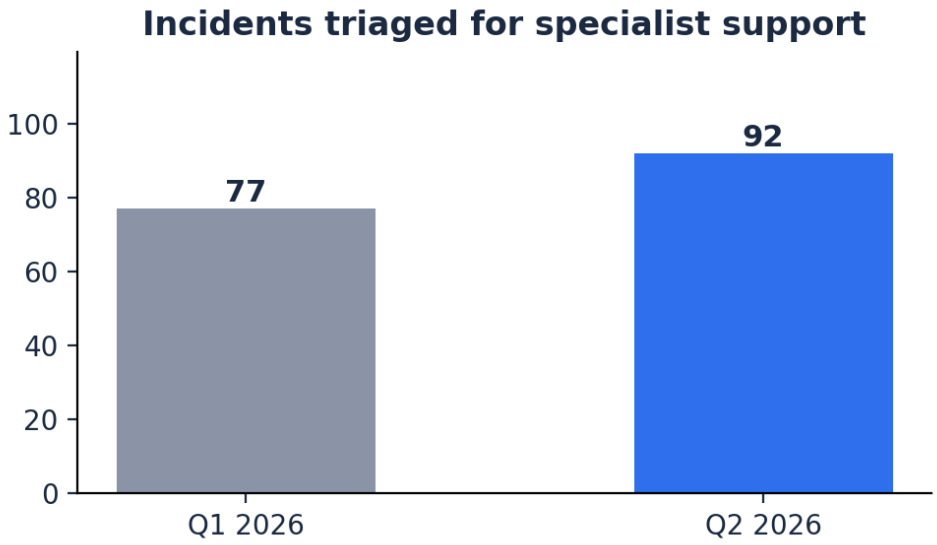
Overview

This report covers cyber security incidents affecting New Zealand from 1 April – 30 June 2026 (Q2 2026), as published by the National Cyber Security Centre (NCSC).

Key Statistics

Incident volume

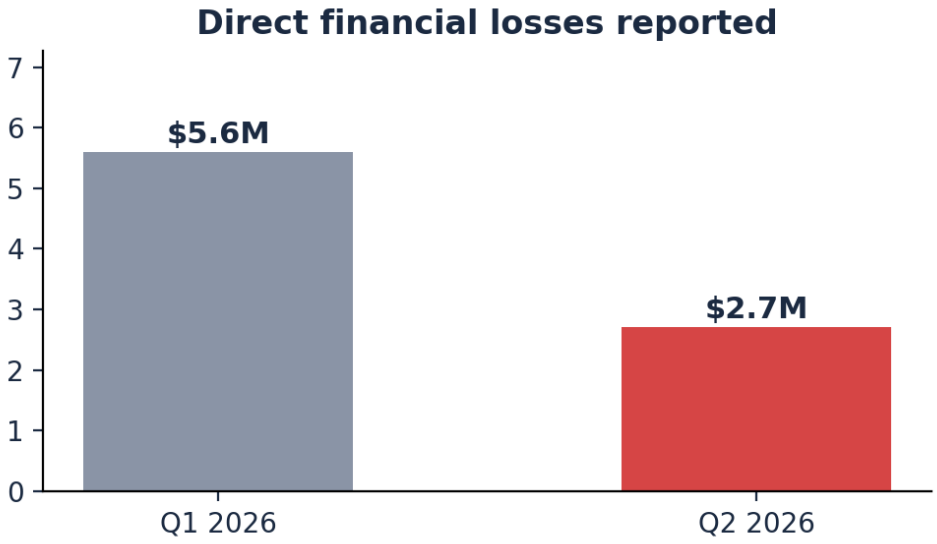
- 1,129 total incident reports received in Q2 2026
- 92 incidents triaged for specialist technical support — a 20% increase from Q1's 77
- 1,037 incidents did not require specialist support — a 5% decrease from Q1



Reconstructed from the figures stated in the report text (Q1 value for specialist-triaged incidents: 77; Q2: 92).

Financial impact

- $2.7 million in direct financial losses — a 52% decrease from Q1's $5.6 million
- 303 incidents reported a financial loss; 291 specified an amount
- Incidents exceeding $10,000 accounted for $2.4M (91% of the total loss) despite being only 49 cases



Reconstructed from the figures stated in the report text (Q1 loss: $5.6M; Q2 loss: $2.7M).

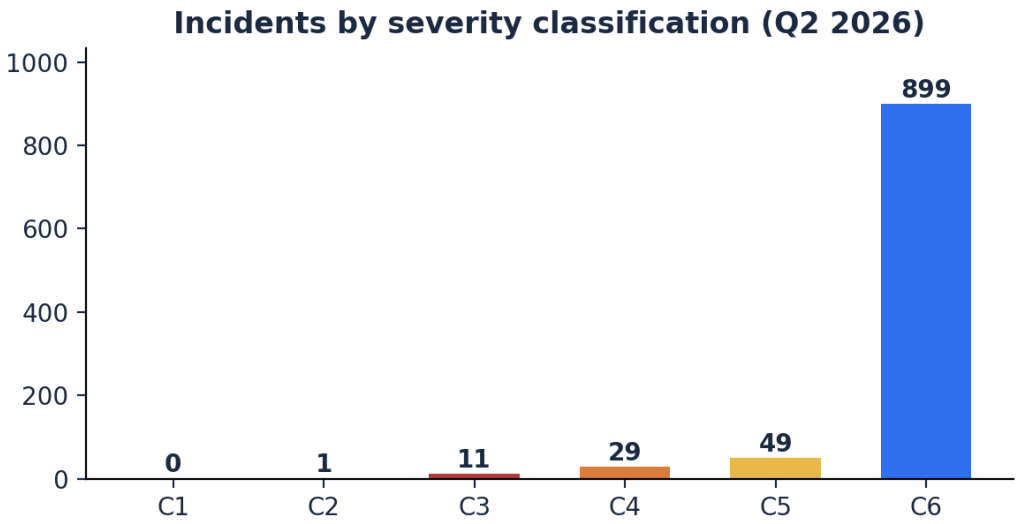
Incident categories

- Scams and fraud: 348 incidents (~$860K in losses) — the most common category
- Phishing and credential harvesting — the second most common category (exact count not published in text on the page)
- Unauthorized access: $1.3M in losses — roughly 50% of the quarter's total financial loss

Severity Classification

Of the incidents received in Q2 2026:

Classification	Description	Count
C1	National cyber emergency	0
C2	Highly significant	1
C3	Significant	11
C4	Moderate	29
C5	Routine	49
C6	Minor	899

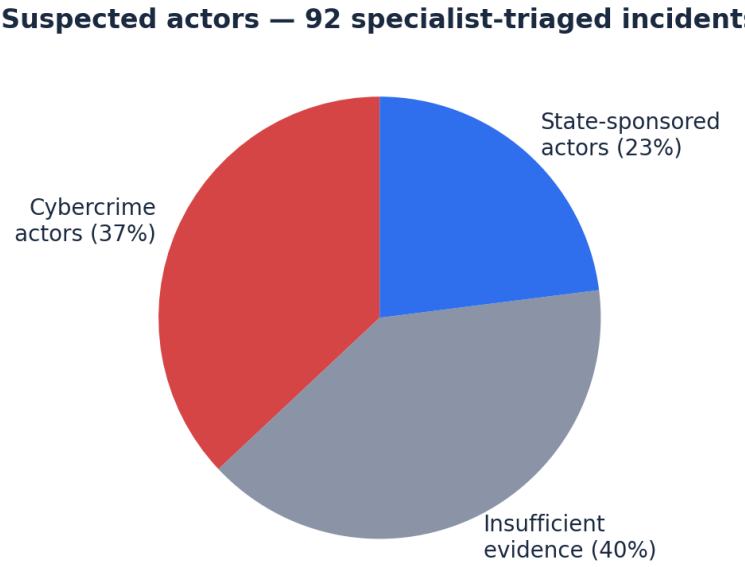


Bar chart reconstructed from the severity table above.

Suspected Actors

Of the 92 specialist-triaged incidents:

- 23% linked to state-sponsored actors
- 37% linked to cybercrime actors
- 40% had insufficient evidence for attribution



Pie chart reconstructed from the attribution percentages above.

Featured Topics

The report highlights malware scams and QR code phishing as emerging threats, with dedicated articles on each linked from this page:

- “Malware: Silent predators of cyberspace” — read the full article
- “QR codes: Think before you scan” — read the full article

Previous quarter: Quarter One Cyber Security Insights 2026 | See all quarterly reports

Notes on this PDF

This document was compiled from the publicly visible text of the NCSC web page above. The page's three original chart images (incidents per quarter, event sub-category counts, and loss per quarter) present some figures only as pixels in graphics rather than as page text, so their exact per-bar values could not be extracted; the bar/pie charts included here were redrawn from the numeric figures that the page does state in prose (e.g. Q1 vs Q2 triage counts, Q1 vs Q2 loss totals, the C1–C6 severity table, and the actor-attribution percentages). For the original chart graphics, see the source page directly.