Cyber security

GCSB's contribution to combatting cyber threats

The New Zealand Intelligence and Security Bill 2016

DEPARTMENT *of the*
PRIME MINISTER *and* CABINET
Te Tari o Te Pirimia me Te Komiti Matua

CASE STUDY NO. 4

The cyber threat

The internet has enriched the lives of New Zealanders but it has also increased our vulnerability. People with malicious intent now target New Zealand from afar through the same communications infrastructure that New Zealanders, government and business rely on every day.

Those with malicious intent realise that people represent the weakest link in an organisation's defences. They often exploit this knowledge by targeting individuals rather than technology infrastructure directly.

The most common attacks that the Government Communications Security Bureau (GCSB) sees are emails carrying malicious attachments or links. If a user accidentally opens these emails, someone with malicious intentions can gain direct and immediate access to the device the victim is using, often a computer connected to an organisation's network.

Confronting the threat – GCSB's role

The vision of New Zealand's Cyber Security Strategy is that New Zealand is secure, resilient and prosperous online. This includes GCSB providing certain cyber-security services. GCSB ensures the integrity and confidentiality of government information, and investigates and analyses cyber incidents against New Zealand's critical infrastructure.

There is a trend towards more sophisticated cyber threats, so the level of investment required by organisations to protect themselves (in terms both of technical security expertise and specialist tools) is growing. Victims of cyber-attacks often need to call in expertise from outside their organisation. In some circumstances, GCSB helps organisations defend against, respond to and repair the damage of cyber threats.

Cyber security in action

As part of its efforts to provide cyber security, GCSB operates the CORTEX project, which counters cyber threats to organisations of national significance. The organisations receiving CORTEX protections include government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

In the twelve months ending 1 April 2016, 316 cyber incidents were logged by GCSB's National Cyber Security Centre, the part of GCSB that operates the CORTEX capabilities. This compares with 190 for the twelve months ending 30 June 2015. Over the past year, GCSB has provided hands-on, highly intensive assistance to 17 organisations, including six from the private sector.

In a typical month, GCSB:

- detects seven cyber intrusions affecting one or more New Zealand organisations;
- receives 12 new incident reports that are self-reported by the organisation dealing with them;
- receives five requests for some form of concrete assistance (requests come from both the private and public sector).

The harm caused by cyber threats outlined above has been varied, and has ranged from information theft to financial loss to system failure and reputational damage.