National Headquarters
Level 12
80 The Terrace
PO Box 2133
Wellington
New Zealand

Phone +64 4 496 3600

3 July 2018

[redacted]

Information Request – Cyber Incidents

I refer to your official information request dated 7 June 2018. You requested:

- the number, and details of the number of cyber attacks and cyber security incidents (ie an actual breach) experienced in the last two years
- how many involved malware (malicious software like computer viruses, worms, Trojan horses, ransomware, spyware, scareware)
- how many of these involved phishing emails aimed at staff? Did any obtain sensitive information eg client info, usernames, passwords, credit card details?
- on how many occasions did was there a loss or breaches of data as a result of cyber security incidents. Please give details.
- on how many occasions was there a financial loss as a result of cyber security incidents? Please give details.
- is training in cyber security awareness mandatory for staff?

Cyber attacks are a common problem that organisations and individuals face, meaning it is essential for organisations to invest in security. The March 2018 CERT NZ report shows that there has been recent growth in activity, vulnerabilities and losses in New Zealand. In the quarter to March 2018, the following increases in activity were identified:

- phishing and credential harvesting (55% increase)
- unauthorised access (67% increase), and
- reported vulnerabilities (133% increase).

There are many ways an attack can occur, but using email as an example, on a daily basis our email filtering service identifies and blocks over 3000 emails identified as spam, phishing or containing malware.

We are unable to provide specific details of cyber attacks both because of the frequency of low-level attacks such as phishing emails but also because providing further details could provide hints as to how to target our security systems. We can confirm that we have no recorded instances of any loss or breaches of data as a result of cyber attacks.

Earlier this year we experienced a sustained attack on our systems. The incident did not have any impact on our emergency responses or operations. The actions we took to protect against this incident led to some members of the organisation temporarily being unable to access emails from their personal devices. As a result of the work generated by this incident, Fire and Emergency has spent approximately $400k on staffing. Fire and Emergency has received advice on this incident, which included considering the broader implications of the increasingly sophisticated attacks, and made the decision to bring forward investment in IT security.

To keep our systems and information safe we follow good practice approaches, guided by the NZ Government's Protective Security Requirements and New Zealand Information Security Manual. These approaches include;

- having formalised security governance
- technical controls such as firewalls, encryption, access authentication and monitoring
- processes such as risk assessments for new systems and changes, system certification and accreditation, incident response
- control validation such as security penetration testing, and
- covering off the people aspects through things like security vetting, clearances and security awareness education of our personnel.

We continue to invest in measures to not only keep our approaches current as our technology and processes evolve, but also strengthen our security as threats and the sophistication evolve.

We have an ongoing programme to educate our staff and maintain awareness of the need to be vigilant about cyber security. Measure we take include:

- maintaining an ICT Acceptable Use Policy which is signed by personnel before they are provided access to our systems
- an online learning module which is part of the induction checklist for new personnel and contractors, and managers are responsible for their personnel refreshing themselves on this annually, and
- frequent communications to personnel through our cyber security communications plan. This utilises a variety of methods including face-to-face forums, intranet notices, regular publications to the workforce, posters, and emails. These communications provide guidance on a variety of matters, for example how to protect against attacks that may be prevalent at the time, or focussed on attacks that are known to be commonly experienced, or focussed on higher risk functions of our organisation. We also align some of our communications around events and activities of organisations like CERT NZ and NetSafe, and utilise their resources.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602. Note also that this response (with your personal details removed) may be published on the Fire and Emergency website.

Yours sincerely

Leigh Deuchars
Director, Office of the Chief Executive