



17 JUL 2018



Dear 

On 7 June 2018, you emailed the Ministry requesting, under the Official Information Act 1982, information regarding cyber attacks and cyber security incidents.

The Ministry takes its role seriously to protect the security of the information we are trusted to manage. The Ministry's Information Security team has a shared services agreement to provide Information Security services to Oranga Tamariki and the Social Investment Agency (SIA). In some cases the data relating to cyber security incidents is unable to be broken down by agency.

For the sake of clarity, your questions will be addressed in turn.

- *the number, and details of the number of cyber attacks and cyber security incidents (ie an actual breach) experienced in the last two years*

The Ministry has a large internet presence and therefore is regularly subject to a range of cyber-attacks. The Ministry uses a range of technologies from global leading companies to protect itself including its information repositories. To test these protections the Ministry has completed an external "Red Team" exercise in the last year which was unable to compromise any of our internet facing services.

In a sample of 10 days activity on our external facing outer layer of firewalls, there were nearly 43 million connection attempts blocked from the internet. Further protections are built in behind those firewalls. It is likely that over the last two years over a billion attempts have occurred.

The security tools used by the Ministry are not designed for large scale reporting. They are intended to target specific events rather than gather data on every incoming internet session. As the Information Security services are operated under the shared service agreement it is nearly impossible to differentiate which agency a cyber attack was aimed at. In order to differentiate between attacks, the Ministry would need to manually review every incident to determine which agency the attack was aimed at and in some cases it may not be aimed at a specific agency but the server itself.

Due to the complexity of extracting this data, differentiating between each organisation and the lack of large scale reporting capability, the Ministry is unable to provide an accurate number over the two years you have requested. As such I refuse your request for this information under section 18(f) of the Official Information Act. The greater public interest is in the effective and efficient administration of the public service.

Page 1 of 4

I have considered whether the Ministry would be able to respond to your request given extra time, or the ability to charge for the information requested. I have concluded that, in either case, the Ministry's ability to undertake its work would still be prejudiced.

Further attacks are carried out through phishing emails and viruses that staff inadvertently access through the internet and details of these are provided in response to your following questions.

I have decided not to provide you with the details of the connection attempts and the technology used as providing this information could compromise the security of the Ministry as the information may be used by people to target the Ministry. As such, this information would be withheld under section 6(c) of the Official Information Act where making that information available would be likely to prejudice the maintenance of the law, including the prevention, investigation and detection of offences.

- *how many involved malware (malicious software like computer viruses, worms, Trojan horses, ransomware, spyware, scareware)*

The Ministry uses market leading endpoint protection to reduce the risk from malware. This technology is constantly under review to ensure it is suitable for the ever-changing methods of malware infection.

In the 12 month period 1 June 2017 to 31 May 2018, 721 potential viruses were detected by the Ministry's shared systems. 718 of these were blocked, automatically deleted or put into quarantine. Of the 721, 23 were found on USB devices, 445 were from staff accessing the internet and 253 were false positives on internal software. I can advise you that the remaining three viruses were targeted at Oranga Tamariki and more information will be provided in their response to you. There were no cases of malware causing a loss of client data.

Due to a change in anti-virus software in 2017, the Ministry is unable to report on data prior to 1 June 2017. As such, your request for this information is refused under section 18(e) of the Official Information Act as this information no longer exists.

- *how many of these involved phishing emails aimed at staff? Did any obtain sensitive information eg client info, usernames, passwords, credit card details?*

The Ministry is not aware of a situation where any sensitive information has been compromised through phishing emails. A change in policy in 2017 blocked staff from accessing personal webmail on Ministry PCs to reduce the risk of viruses and Phishing through personal emails.

The Ministry protects its users with a range of Cloud and local services to filter incoming email based phishing and malware. There were 17,624,798 inbound emails scanned between 1 June 2017 and 31 May 2018 over the 16 different email domains that the Ministry operates. Of the inbound emails scanned, 5,484,393 were blocked as Spam, and 25,232 as malware and phishing. Out of those 25,232, around 61 per cent was malware and 39 per cent was phishing. A further 272,327 were blocked due to other email content protection rules.

As no system can filter out all phishing attacks, guidance is provided to all staff to further reduce the chance of a successful attack.

These services used to filter incoming email based phishing and malware have a 12 month capability for reporting and as such, your request for this information prior to 1 June 2017 is refused under section 18(e) of the Official Information Act as this information no longer exists.

- *on how many occasions was there a loss or breaches of data as a result of cyber security incidents. Please give details.*

The Ministry is not aware of any occasions where there was a loss or breach of data as a result of a cyber security incident. However, in the interest of transparency, in March 2017, the Ministry was made aware that the system used to collect Individual Client Level Data (ICLD) from providers had allowed one provider to see another provider's detail. It is important to note that this was not a cyber security incident and there was no financial impact or breach of client information. Further information about this is available here: www.msd.govt.nz/about-msd-and-our-work/publications-resources/information-releases/client-level-data.html

- *on how many occasions was there a financial loss as a result of cyber security incidents? Please give details.*

The Ministry is not aware of any cyber security incidents that have resulted in a financial loss.

- *is training in cyber security awareness mandatory for staff?*

Security Awareness training is mandatory for all staff through an e-learn module that covers privacy, information management and information security.

The principles and purposes of the Official Information Act 1982 under which you made your request are:


- to create greater openness and transparency about the plans, work and activities of the Government,
- to increase the ability of the public to participate in the making and administration of our laws and policies and
- to lead to greater accountability in the conduct of public affairs.

This Ministry fully supports those principles and purposes. The Ministry therefore intends to make the information contained in this letter available to the wider public shortly. The Ministry will do this by publishing this letter on the Ministry of Social Development's website. Your personal details will be deleted and the Ministry will not publish any information that would identify you as the person who requested the information.

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with this response, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Yours sincerely

A handwritten signature in blue ink, appearing to be 'S. Crombie', written over the text 'Yours sincerely'.

Stephen Crombie
Deputy Chief Executive, Corporate Solutions