COMMERCE COMMISSION NEW ZEALAND
Te Komihana Tauhokohoko

October 2019 security incident summary

Introduction

1 This document provides a summary of the security incident experienced by the Commerce Commission in October 2019 as well as the Commission's response to it. It should be read in conjunction with the reports of the two reviews undertaken in response to the incident (Fowler Report and KPMG Report), which can both be found on the Commission's website.

The security incident

2 In October 2019, one of the Commission's external providers advised that they had been the victim of a burglary and computer equipment containing information connected to Commission work had been stolen.

3 The provider had a long-standing relationship with the Commission and was subject to contractual and confidentiality obligations to ensure that information was stored safely and securely and deleted after use.

4 From conversations with the provider it became clear that they had not met their contractual and confidentiality obligations.

5 Given the provider was uncertain what information was on the devices and the last time they deleted information, a comprehensive effort was made by Commission staff to identify the information that may have been compromised. This was done by cross referencing work sent to the provider. This process concluded with an assessment that a range of documents relating to the Commission's work were at risk. Some of these documents contained confidential information businesses and individuals provided to the Commission.

The Commission's immediate response

6 In the immediate period following the security incident the Commission took the following actions:

6.1 Engaged with the New Zealand Police and their Electronic Crime Unit in attempting to track and secure the stolen information. To date none of the stolen items have been recovered and no arrests have been made.

6.2 Reported the incident to government agencies including the Ministry of Business, Innovation and Employment (MBIE), CERT NZ, the Government Chief Digital Officer, the Office of the Privacy Commissioner, State Services Commission and the Minister's Office.

6.3 Advised the external provider that it would no longer be using their services and brought the work in-house.

6.4 Urgently explored ways to help protect the confidentiality of the information.

6.5 Commissioned two reviews into the incident. The first to look into the circumstances relating to the specific incident and the second to look into the Commission's wider information management and security, including third-party supplier engagements.

6.6 On 8 October, the Commission's Chair issued a confidentiality order under section 100 of the Commerce Act. This made it a criminal offence for any person in possession of the devices or information from the devices to disclose or communicate it to anyone while the orders remain in force.

6.7 On 8 October, the Commission also began the process of advising affected parties of the potential disclosure of their confidential material. This was a lengthy and time-consuming process as it involved identifying what information was at risk and also the best way of contacting affected parties to ensure their confidentiality and privacy was not further compromised.

6.8 On the same day the Commission issued a media statement and a media conference was held with the Commission's Chair and Chief Executive.

6.9 On 8 October, the Commission sought an interim injunction from the High Court. The injunction was made against unknown persons who may at any stage possess information on or taken from the equipment. The injunction prohibited any person from dealing with the stolen information, including by copying, communicating and publishing it. The High Court also made orders suppressing information relating to the external service provider, the nature of the services provided to the Commission and information about the burglary not disclosed by the Police. Anyone failing to comply with these Court orders could be held in contempt of court. Full written reasons for the decision to grant the interim injunction were issued by the Court on 14 October.

6.10 On 25 October 2019, the Commission began the process of contacting current and past suppliers of services to the Commission to seek assurances that they had appropriate security processes and protocols in place to protect information they might hold relating to the work of the Commission. Based on the responses received, it was not considered necessary to take any further immediate steps with those suppliers.

Richard Fowler QC's independent report

7 Richard Fowler QC was formally instructed on 25 October 2019 to undertake an independent review of the circumstances relating to the security incident.

8 In summary, in relation to the specific incident, he finds that the external provider was clearly under contractual obligations with regard to information security, retention and disposal of confidential material, that the provider understood these obligations, and that the provider was plainly in breach of those obligations.

9 Mr Fowler recommends that the Commission consider assuming more direct control of services of the type the security incident related to.

10 While not central to his findings, he also notes that in the period following the incident the Commission treated the situation seriously and implemented a swift and efficient response.

11 A copy of the Fowler report can be found on the Commission's website. Redactions in this report have been made in a manner consistent with the suppression orders made by the Court and with the requirements of the Official Information Act.

KPMG Report

12 KPMG was formally instructed on 20 November 2019 to complete an independent assessment into the Commission's information management and security and to report to the Commission's Board on the Commission's maturity, culture, control gaps and improvement opportunities in relation to them. This included, but was not limited to, information held or accessible by the Commission's external providers.

13 The process of finalising the KPMG review report was delayed due to constraints arising from the COVID-19 pandemic. KPMG presented its final report to the Commission's Board in June 2020.

14 KPMG found that the Commission have implemented a number of processes and controls that appear fit for purpose and there is a strong information security culture and awareness among staff. Based on controls assessed, KPMG concluded that the Commission had a moderate level of maturity in security. It noted that the majority of findings are consistent with what they see in many other public and private sector organisations.

15 The report makes a number of recommendations in the areas of culture, policies, procedures and work practices, third party and contractor controls, and control effectiveness.

16 A copy of the KPMG report can be found on the Commission's website. Redactions in this report have been made in line with the Official Information Act.

Commission's response to the reviews

17 The Commission accepts the findings and recommendations from both reviews.

18 In response it has taken steps directly related to the security incident and it has engaged an information security expert to help design a broad ranging security improvement programme.

Responses directly related to the security incident

19 Actions taken in the days immediately following the security incident are described above. Other actions already undertaken since the security incident include:

- 19.1 Recruiting a Procurement Manager to improve contract management across the Commission.
- 19.2 Reviewing standard-form contracts with external providers to ensure they include appropriate security and confidentiality obligations.
- 19.3 Changing the approvals process to improve oversight of all external provider contracts.
- 19.4 Bringing the services provided by the external provider in-house or having external providers undertake these services on-site, removing the need to take any office equipment or material off-site.
- 19.5 Setting up a new secure cloud-based file transfer system for sharing information with external providers and third parties where information sharing is necessary to effectively facilitate the work of the Commission.

High-level security improvement programme

20 A wider security improvement programme has also been initiated in response to the KPMG review and additionally to implement the Commission's decision to voluntarily adopt the government's Protective Security Requirements (PSR). In addition to information security the programme addresses security governance, personnel security and physical security.

21 The security programme is designed to put the Commission on a trajectory to achieve a MANAGED maturity level (as defined in the PSR) with the programme expected to be substantially completed within 12 months.

22 The programme will address seven key themes:

- 22.1 Establishing a contemporary security baseline
- 22.2 Implementing the PSR framework
- 22.3 Policy, advice and training
- 22.4 Supply chain security
- 22.5 Personnel and physical security
- 22.6 Information security technology, services and operating model
- 22.7 Information security practices.

23 To achieve the MANAGED maturity level, the Commission is in the process of recruiting security professionals to support the delivery of the programme.


COMMERCE
COMMISSION
NEW ZEALAND
Te Komihana Tauhokohoko