



CENTRE for CRITICAL INFRASTRUCTURE PROTECTION

CONFIDENTIALITY CHARTER

Introduction

This Charter is designed to help critical infrastructure organisations interact with the Centre for Critical Infrastructure Protection (CCIP) in a secure, efficient and confidential manner in order to exchange information, report malicious cyber activity, or simply seek advice.

It creates a framework within which critical infrastructure organisations and the CCIP can work together to meet a common goal - creating a safer digital environment.

The accurate and timely reporting of malicious cyber and related activities provides vital information for the protection of critical infrastructure. This can be achieved only through mutual trust and a strategy of collaboration and cooperation between critical infrastructure organisations and the CCIP.

It is for this reason that the CCIP has developed this Confidentiality Charter. In doing so, we hope that it will provide reassurance that critical infrastructure organisations can report suspicious activity and attacks without fear of causing unwelcome interruption to their organisation's continuity.

Interaction with critical infrastructure organisations promotes a cross-flow and exchange of information and is vital if the CCIP and the critical infrastructure organisation community it serves are to operate in a safe digital environment.

In a climate of trust and security, the exchange of relevant information helps critical infrastructure organisations and the CCIP more effectively to understand and combat malicious cyber activity.

For the purposes of this Charter, malicious cyber activity means a range of activity within the electronic and networked environment that includes:

- Attacks from viruses and Trojans;
- Denial of service;
- Unauthorised access;
- Web site and email spoofing;
- Fraud, extortion and other criminal activity; and
- Unlawful interference with corporate or government data.

Continued on page 3.

Working with the CCIP

Continued:

Legislation places specific requirements on organisations and individuals engaged in the investigative process. Whilst the CCIP must comply with these requirements, it is also able to adopt measures to minimise the risk that commercially sensitive information might reach the public domain.

In general, criminal activity falls under the jurisdiction of the New Zealand Police.

The CCIP will ensure that the information flow is a dialogue. In particular, it is the express aim of the CCIP to:

- Support industry with an authoritative, comprehensive and timely strategic assessment of malicious cyber activity;
- Provide commentary upon, aggregate and analyse critical infrastructure organisation intelligence;
- Provide the conduit for sharing good practice advice;
- Support investigations into malicious cyber activities with the cooperation and collaboration of industry and its other strategic partners. To meet this objective, it is essential that organisations that are targeted be given the assurance that they can report such attacks without fear of adversely affecting their organisation. We intend that this Confidentiality Charter will help to foster a new era of closer working between the CCIP and the critical infrastructure organisation community it serves.

The Consultation Process

We understand the need for immediate and confidential consultation. Initial contact can be by telephone, fax, email or a person-to-person appointment.

It is essential to establish as early as possible whether events relate to a criminal or civil jurisdictional matter, as this will govern the way in which the enquiry is handled. The early consultation process is designed to promote a mutual appreciation of the issues relating to information management and incident investigation.

After initial notification, we begin the consultation process by meeting with key staff who are authorised by the organisation to liaise with the CCIP. During this initial consultation, we will discuss the following:

- The profile of the industry partner and its assessment of potential damage to its infrastructure, reputation and brand name;
- The effect on New Zealand's critical infrastructure;
- The extent of any internal investigation to date;
- Desired and agreed control mechanisms for the on-going investigative process;
- The extent of the existing knowledge loop and procedures for the dissemination of information;

Continued on page 5.

The Consultation Process

Continued:

- The likely disruption and cost to core operations from the investigative process, and agreement on processes to minimise these effects;
- The financial implications associated with the disclosure of intellectual property and other commercially sensitive information to third parties through the investigative process;
- Agreed measures to prevent disclosure of intellectual property and other commercially sensitive information;
- A commitment from the CCIP to undertake operational, tactical or strategic activity as a result of the preliminary consultation; and
- Any other matter raised by the industry partner.

The information that contributes most effectively to combating malicious cyber activity includes:

- Organisational and systems profile;
- Specific details of malicious cyber activity that requires analysis or investigation;
- Information that might lead to the identification of malicious activity;
- Information that might lead to the identification of the perpetrators;
- General details of attacks and vulnerabilities in relation to technology, policy and procedures; and
- Information relating to the impact of malicious cyber activity, generally or in particular.

CCIP can be contacted at:

Centre for Critical Infrastructure Protection
PO Box 12-209, Wellington, New Zealand

Tel: +64 4 498-7654 Fax: +64 4 498-7655

Email: info@ccip.govt.nz or incidents@ccip.govt.nz

Web: www.ccip.govt.nz