



NCSIP Position Paper

Managing the Cyber Threat to Cabinet Members

Prepared on behalf of NCSIP with input from Committee Members by

Martin Dinel, BSc, ISP, ITCP, CISSP/ALBERTA

2017-11-09

INTRODUCTION

As elected members of the government, cabinet members are in the public eye and are increasingly leveraging social networks and news media to perform their duties. As a result, much of their personal information is becoming available in the public domain and they've become excellent targets for cyber criminals.

NCSIP POSITION

All Canadian Federal, Provincial and Territorial jurisdictions have some form of cyber security awareness program that is made available to their organization's staff. These programs often include access to online resources as well as in-class presentations. The programs are offered to employees who are usually required to take courses annually however cabinet members are rarely exposed to the same programs despite being an attractive target.

Topics covered by cyber security training programs include, but are not limited to:

- Phishing and Social Engineering;
- General safe practices while using computers and mobile devices;
- Information Security Classification & Information Management; and
- Freedom of Information and Protection of Privacy (FOIPP).

It is important to consider that cabinet members are provided with highly sensitive information, critical to government operations and, often, to the well-being of their constituents. A breach of this information **will** impact the reputation of government and their constituents' trust that their information assets are secure. A breach **could** also have financial implications (job loss, missed opportunities, legal repercussions, etc.).

The cyber threat could manifest itself in many forms for cabinet members when information publicly available from social networks or media outlets is used to:

- guess passwords and credentials or trick the cabinet member into divulge their passwords and credentials;
- gain access to sensitive information, modify information or impersonate the cabinet member to convince someone to perform an activity on their behalf (e.g. MacEwan University administrative staff in Alberta received a fake email with enough information to convince them to change accounts payable information for the contractor, resulting in an \$11M fraud); and

National CIO
Subcommittee on
Information Protection



- determine a location frequented by the cabinet minister, such as a coffee house, to perform a “man-in-the-middle” attack enabling the threat actor to read emails or perform online activities without the users knowledge.

While all jurisdictions agree that cabinet members should be made aware of these threats and how to respond to them, only two jurisdictions currently have direct access to their cabinet members:

- Government of Canada – cabinet members are informed on matters of cybersecurity through a variety of means, including DM breakfasts and Cyber Meetings, and at executive decision-making bodies as required.
- British Columbia – The Chief Information Security Officer has the ability to connect directly with cabinet to provide general awareness presentations.

RECOMMENDATION

NCSIP members agree that it is critical that employees at all levels, especially key leadership such as cabinet members, be made aware of cyber threats that may impact them and are provided with relevant information on how to recognize, deter and respond to the threats.

We recommend the following be implemented in all jurisdictions as soon as possible:

- Annual 15-20 minutes cybersecurity awareness sessions outlining the cyber threat, ensuring vigilance, and providing an overview of how to recognize and respond to threats;
- Cabinet members should be provided the same cybersecurity awareness training programs as provided to internal employees;
- Cybersecurity briefings should be made mandatory for all cabinet members traveling out of country before their departure (see NCSIP Position Paper titled “*Managing the Cyber Threat Resulting from Foreign Travel*”).

NCSIP requests PSCIOC’s assistance to implement these recommendations.