4.11.

CYBERSECURITY INCIDENT MANAGEMENT

BACKGROUND

The Ville de Montréal (the City) uses many information systems that process a very large amount of data, some of which are confidential, such as personal information, which must be protected to prevent misuse. Currently, all major organizations are connected in one way or another to the entire globe and are exposed to cyberattacks that are experiencing exponential growth.

Cybersecurity is the act of protecting the organization from cyberattacks from outside or inside the organization. Cybersecurity tools may include all frameworks, technical tools, security concepts, security mechanisms, risk management approaches, and awareness and training programs to protect the data of its citizens and employees, users and the organization's information assets. These primarily include applications, servers, databases and telecommunication and network equipment.

Cyberattacks are increasing exponentially. The question is no longer whether, but when, the City will be attacked.

A cybersecurity incident can cause significant harm, for example:

- significant financial costs when a cyberattack lasts too long;
- the theft and dissemination of confidential information (e.g., personal information, strategic information);
- taint the city's reputation;
- loss of citizens' trust;
- lawsuits.

If the City is not properly prepared, an incident may have a negative impact on its business operations. In order to significantly reduce the impacts of a cyberattack, proper management of cybersecurity incidents is critical and must include the following:

- Adequate documentation of policies and procedures;
- Formal assignment of responsibility for managing cybersecurity incidents to experienced people;
- A cybersecurity awareness and training program;
- Technological and administrative detection tools to prevent and thwart cyberattacks;
- Categorization of cybersecurity incidents to prioritize those with the greatest impact and probability;
- An incident coordination, communication and monitoring process to reduce attack time and improve overall management of cybersecurity incidents.

OBJECTIVE AND SCOPE OF THE AUDIT

The objective of the audit was to assess the process implemented to ensure that the City manages cybersecurity incidents properly in order to address them in a timely manner, limit their impact and prevent them from reoccurring.

For obvious security reasons, we cannot disclose the objective and results of this audit in this annual report. Moreover, the business units concerned would have implemented appropriate action plans to address any deficiencies we would have noted.