THE CASE OF THE MISSING COMPUTERS: LESSONS LEARNED FROM HEALTH CANADA

Posted on September 21, 2022

Categories: Insights, Publications

An audit of Health Canada's information technology ("**IT**") systems (the "**Audit**") found a long list of problems, including, among others, insufficient or inefficient tracking of IT assets, lack of proper maintenance of IT hardware assets, outdated IT hardware assets decommissioning processes, and overall inadequate governance and support for planning and engagement for IT asset management.[1] This bulletin aims at the lessons companies can learn from the Audit and highlights the importance of having and implementing a robust internal IT and cybersecurity program.

The Audit and Its Findings

The Audit included the examination and assessment of systems, records, personnel, and physical properties related to IT assets of Health Canada and the Public Health Agency of Canada (collectively, the "**Department**") up to June 2019. Although the Audit was completed in 2019, it was not made public until June 2022. The Audit was not the first audit of the Department's IT assets; an initial 2009 audit found several issues, and a subsequent 2013 audit found that improvements had been insufficient and the management of the applicable IT assets had not been adequately improved. These earlier audits led to an overhaul of the Department's IT related protocols in 2017, which the Audit was intended to evaluate.

Material findings from the Audit include the following:

- Insufficient documentation and tracking of IT hardware assets, with certain IT hardware assets not tracked at all. Ultimately, the auditors could not confirm the existence and location of approximately 74% of the IT hardware assets or a total of 35,000 devices;
- Insufficient and error-prone tracking of software assets, where the purchase orders for 51% of the software assets tested could not be located;
- Lack of process to ensure the management of low dollar value IT assets such as USB sticks, servers, laptops, tablets, computers, and monitors;
- Insufficient controls for the maintenance of IT hardware assets; and
- Lack of adherence to the Department's requirements and process for decommissioning IT assets and

lack of oversight of the said process.

Risks for Companies

Poor IT inventory management and a lack of robust IT and cybersecurity program can lead to massive risks to both public and private organizations, including the following.

- *Loss of data*: Poor IT asset tracking and management reduce organizations' ability to accurately account for, maintain, and properly safeguard their IT assets, which can lead to the loss of both confidential information of the organizations and personal information in the organizations' custody. This can lead to both financial and legal liabilities to the organizations.
- *Breach of contractual obligations*: Many agreements, whether related to IT assets, have requirements to properly safeguard confidential information and personal information. As soon as such information is exposed to poorly managed IT assets, it is at risk of theft and/or misuse, which may lead to substantial liability to organizations. Further, the use of software is governed by software licenses. The absence of appropriate tracking of the use of software assets can lead to breach of software licenses and intellectual property infringement claims.
- *Privacy complaints*: Under Canadian privacy laws, individuals can complain to the applicable privacy commissioners about organizations for their mishandling of personal information, failure to provide access to personal information, or failure to correct mistakes in personal information. Poorly managed IT assets reduces organizations' ability to handle personal information in accordance with applicable privacy laws and increases the likelihood that a complaint is filed against the organizations.
- *Breach of privacy laws*: Under private sector privacy laws, businesses are responsible for personal information in their custody. Under public sector privacy laws, these obligations are also owed by service providers to public entities. Failing to properly safeguard personal information as a result of poorly managed IT assets may amount to a breach of these obligations, which may lead to reputation loss as well as financial and legal liabilities.

In sum, failing to properly track, maintain, manage, and dispose of IT asset, whether laptops, mobile devices, servers, or USB drives (among others), increases the risk that an organization will be in breach of any applicable agreements tied to those assets, and any data residing on such assets cannot be appropriately monitored, maintained, or safeguarded.

Takeaways

Proper management of IT assets is a critical component of a robust IT and cybersecurity program. All businesses should ensure that their IT and cybersecurity policies and procedures extend to IT asset

management, and address the risks of not properly tracking and safeguarding any device containing personal, confidential or proprietary information. This may include IT inventory tracking systems, regular audits of IT assets, and policies and/or procedures for managing the lifecycle of IT assets.

If you have any questions about any IT and cybersecurity related policies, practices or procedures, or Canadian privacy laws more generally, a member of our Privacy & Data Protection Group would be happy to assist you.

[1] Health Canada, *Audit of Information Technology Asset Management* (2022 June), online: *Government of Canada*.

by Robert Piasentin, Yue Fei, and Kristen Shaw

A Cautionary Note