Yukon Information and Privacy Commissioner

3162 Third Avenue, Main Floor
Whitehorse, Yukon, Y1A 1G3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.yukonombudsman.ca

Advisory for custodians and public bodies regarding an active persistent cybersecurity threat

March 17, 2022

Audience

This advisory is intended for anyone with responsibility for the operation or content of IT systems (ITS managers) containing personal health information (PHI) or personal information (PI) for custodians[1] under the Yukon's *Health Information Privacy and Management Act* (HIPMA) and public bodies[2] under the Yukon's *Access to Information and Protection of Privacy Act* (ATIPPA).

Overview

On February 24, 2022, the Canadian Centre for Cyber Security (CCCS) issued a warning[3] regarding the deployment of so-called wiper-ware targeting organizations linked to Ukraine. The purpose of this type of malware is to destroy data on computer systems and disable the ability to re-boot or otherwise recover the machine. These attacks are predominantly propagated via phishing email.[4] Other threats such as attacks on VPN networks and routers have also been reported. Attacks may be accompanied by extortion attempts.

The CCCS is reporting that it has received no indication of activity in Canada yet but is amplifying this information out of an abundance of caution.

It has come to the attention of the Yukon Information and Privacy Commissioner (IPC) that in recent days cyberattacks of this kind have escalated to target nations beyond Ukraine. Given this, there is a risk to Canadian organizations, including those in the Yukon. This advisory is to alert public bodies and custodians about the risks, so they can take the necessary measures to limit the risks associated with these attacks.

Details and further information

As a result of this threat, PHI or PI in your organization may be at risk of unauthorized access, disclosure, theft and/or may become unavailable. This may in turn disrupt your ability to provide health care services, government programs and activities, or other associated activities.

---

[1] Custodians are defined under HIPMA and include but are not limited to doctors, dentists, pharmacists, optometrists, physiotherapists, chiropractors and operators of health care facilities.
[2] See the schedule of the ATIPPA regulation for a list of public bodies here.
[3] https://www.cyber.gc.ca/en/alerts/disruptive-activity-against-ukrainian-organizations
[4] https://www.zscaler.com/blogs/security-research/hermeticwiper-resurgence-targeted-attacks-ukraine

The IPC recommends that ITS managers take the following actions to reduce the risk of a successful attack.

- Inform employees about:
  - what phishing is and how it can occur;
  - how to recognize phishing attempts;
  - the importance of using strong passwords in accordance with the latest guidance;[5]
  - how to detect an incident and to whom an incident should be reported and when;
  - breach response and reporting obligations under ATIPPA and HIPMA (as applicable);
  - the importance of proper information management practices, i.e., storing documents in the appropriate places, e.g., in a document management system and not in email inboxes or on desktops, to reduce the risk and impact of breaches and other incidents.
- Implement multi-factor authentication.
- Utilize proper patch management and vulnerability scanning.
- Deploy end point protection.
- Configure inbound and outbound phishing protections.
- Ensure "backup and restore" procedures are in place and tested.

The IPC further recommends that ITS managers keep a close eye on information security news sources such as NIST[6], CISA[7], CCCS[8] and CERT-EU[9] for the latest updates on the situation and to obtain more specific information for their respective IT infrastructure and possible exposures.

Obligation to report privacy breaches

Both custodians and public bodies are required to notify individuals about a breach of their PHI or PI where there is a risk of significant harm to the individuals, as a result of the breach. In addition, the Yukon's IPC must be informed about the breach.

Should a breach of privacy occur as a result of this recent information security threat, custodians and public bodies need to assess, in accordance with applicable privacy law, whether they are required to notify individuals about the breach and to inform the IPC.

Contact the Office of the Information and Privacy Commissioner:

Phone: (867) 667-8468 (tollfree in Yukon 1-800-661-0408 ext. 8468)
Email: info@yukonombudsman.ca

Disclaimer

The purpose of this document is to inform custodians and public bodies about the risks to privacy associated with a recent information security development and to support them in meeting their privacy and security obligations under HIPMA and ATIPPA. This document is not intended as, nor is it a substitute for, legal advice or other advice about how to secure or protect PHI or PI that may be at risk of breach as a result of the information security development. This document is not binding on the Yukon's Information and Privacy Commissioner.

[5] https://pages.nist.gov/800-63-3/sp800-63b.html. Also see https://www.auditboard.com/blog/nist-password-guidelines/ for a synopsis.
[6] https://nvd.nist.gov/vuln
[7] https://www.cisa.gov/uscert/
[8] https://cyber.gc.ca/en/alerts-advisories
[9] https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html