TAB# 38

Session Briefing Note

FALL 2023

Cyber Security

Highways and Public Works

Recommended response:

- Keeping our information systems and government-held information secure is a key objective of our government.
- Over the last decade the number of cyber attacks around the world affecting both governments and private companies has increased.
- This trend is consistent for the Yukon. In recent years, the Yukon government, like other governments across Canada, has experienced an increase in cyber attacks and risk.
- We take cyber security seriously, and in an effort to counter cyber threats, Highways and Public Works is:
    - continuously evolving our security threat monitoring and detection solutions to repel attacks;
    - improving the government's resiliency by taking new approaches to the ways in which we protect information;
    - conducting security threat risk assessments on systems and regularly mitigating vulnerabilities; and
    - working with a security operations centre service contractor to monitor our IT infrastructure 24 hours a day, seven days a week.

Additional response:

- Recently, on September 14, 2023, the Yukon government experienced a distributed denial of service attack. The attack resulted in the inability to access to Yukon.ca web sites and disrupted access to cloud services for internal government employees.

- This type of attack seeks to disrupt access to services by overwhelming the online systems with a massive load of requests. The attacks are not designed to gain access to internal information.
- We were able to introduce some measures to minimize the impacts of the attack and make services available again within the same day.
- The attack was halted a couple of days later. The measures that were put in place to mitigate the impacts of distributed denial of service attacks will help in any future attacks.
- There is no evidence that any unauthorized access to private citizen data, government systems or government files took place.
- Highways and Public Works continues to monitor the security measures that we've put in place.

Third response:

- The Yukon government is an active member of the Canadian Centre for Cyber Security. We attend weekly briefings with the centre about emerging threats and receive all security alerts and recommendations for actions to be taken.
- For example, on September 5, 2023, Google issued a security advisory to address vulnerabilities in Chrome for Desktop. The Yukon government reviews these alerts and applies updates to its systems as necessary.
- We are also active members of the Federal, Provincial, Territorial Committee on cyber security, where governments share information about threats, advice and best practices. The Yukon government also provides input into cyber security position papers that are produced by this committee.

TAB# 38

Session Briefing Note

FALL 2023

Cyber Security

Highways and Public Works

Context—this may be an issue because:

- People are aware of significant security breaches in other governments and in the private sector, and that the number of breaches is on the rise.

Background:

- State-sponsored cyberattacks are on the rise due to global geopolitical tensions. Notably, the recent NATO summit in June 2023 coincided with threat actors using sophisticated '0-day' attacks against western governments. Foreign interference through misinformation campaigns intended to interfere with elections and influence policy decisions are a growing concern.
- In early 2023, the Government of Nunavut had a significant ransomware attack that crippled their government's services for weeks. While capabilities were re-built and re-deployed, ultimately some data was never recovered.
- Newfoundland and Labrador's Health Authority experienced a significant attack in 2021 that exposed sensitive personal information for ransom resulting in impacts to delivering health care.

Approved by:	
C Harwood	September 29, 2023
Deputy Minister, Highways and Public Works	Date Approved