YOUNG ANDERSON
BARRISTERS & SOLICITORS

April 30, 2020

BULLETIN

CYBERATTACKS ON THE RISE WITH COVID-19

Cybercrime is on the rise as we all grapple with the effects of the COVID-19 pandemic and local governments are not immune to this increasing threat.

One security firm has recently reported an increase of 30,000 % in COVID-19 themed phishing, malicious websites, and malware targeting remote users since January. The U.K.'s National Cyber Security Centre and the U.S. Department of Homeland Security Cybersecurity and Infrastructure Agency have also put out a joint advisory warning of an increasing number of malicious cyber actors exploiting the COVID-19 pandemic. The Canadian Centre for Cyber Security has also published an alert for Canadian health organizations, including policy-making organizations, that the COVID-19 pandemic presents an elevated risk.

Local governments are undoubtedly vulnerable to this increased risk as they transition to using new and sometimes untested tools to allow remote work to continue providing essential services to their citizens. We strongly urge clients to make use of their in-house or consultant IT professionals to help assess and mitigate the risks they face, especially given the necessarily rapid deployment of remote work technologies. This is important for many reasons. It is vitally important because local governments' obligations under the *Freedom of Information and Protection of Privacy Act* to protect the personal information still exist, pandemic or not.

We are particularly concerned about highly sophisticated "spear phishing" or social engineering tactics being used to compromise local government systems. These types of attacks are particularly effective when employees are not physically in the same space and able to informally verify odd requests in person, such as an email appearing to be from a colleague that urgently asks the recipient to provide accounting or payroll information. We therefore recommend that clients remind their employees of the need for vigilance in preventing cyber attacks, and the need to report incidents if they occur.

The Office of the Information and Privacy Commissioner has published some general guidance on protecting personal information while away from the office: https://www.oipc.bc.ca/guidance-documents/1447.

If a breach is discovered, a robust and effective breach containment and response protocol is essential to mitigate the damage to affected individuals. The OIPC has also published guidance responding to privacy breaches: https://www.oipc.bc.ca/guidance-documents/1428.

If you need help with mitigation of or response to the legal risks, do not hesitate to contact our lawyers with expertise in this area.

Ethan Plato and David Loukidelis, QC