

OOP FOI PREM:EX

From: Howlett, Tim GCPE:EX
Sent: December 17, 2019 2:16 PM
To: Hockin, Amber PREM:EX
Subject: LifeLabs Background for 4pm meeting
Attachments: Background.docx

Info and relevant QAs attached.

Top line is that Govt will assist with OIPC investigation and looks forward to recommendations and lessons that can be drawn.

Cybersecurity is a growing challenge – Govt contracts include undertakings from providers that they will protect private data (private companies are also obliged to do so under BC's Personal Information Protection Act)

Life Labs - Background:

- On December 17, it was announced that LifeLabs experienced a significant data breach stemming from a cyber-security incident.
- The breached data included patient names, addresses, province of residence, postal codes, practitioner names, personal health numbers, gender and dates of birth.
- LifeLabs says their investigation has revealed no evidence British Columbians' lab test results were impacted (lab test results from 85,000 Ontario customers were taken).
- Government and health authority systems were not impacted.
- LifeLabs is providing all customers access to free identity theft insurance and monitoring and has implemented additional safeguards to further secure their networks.
- BC is pursuing formal assurances and documentation from LifeLabs to ensure that they are taking adequate security measures to prevent this from re-occurring.
- The Privacy Commissioners are investigating LifeLabs.
- Cyber-attacks have become common events. There are 308 million unauthorized access attempts on B.C. government networks daily – that's 3,565 per second.
- The number of attempts on government has increased from 240 million per day since last year – an increase of more than 28%.

1. Are you re-evaluating your relationship with Lifelabs?

- We are pursuing formal assurances and documentation from LifeLabs that they have taken adequate security measures to prevent this from re-occurring.
- Next steps for this incident will be determined based on our agreement with LifeLabs.

2. The Ministry of Health holds a service agreement with LifeLabs – what protections are in place when data is in the custody of a contractor or service provider?

- Government's contract with LifeLabs, which includes the privacy terms to which LifeLabs must adhere, sets a robust standard for LifeLabs to meet with respect to privacy and security.

3. What does the Ministry do to enforce these protections/policies with service providers?

- Service agreements are drafted that include both a privacy protection schedule and a security schedule that set out the legal requirements that the contractor must abide by.
- Expectations that service providers must meet the terms set out in their agreements are clearly communicated both in the agreement and verbally.

- Service providers who manage personal information are also required to take privacy training as an added measure to ensure this requirement is fully understood.
- If any evidence is received that a service provider is non-compliant with any terms of their agreement, the service provider must then conduct an investigation or cooperate with government's investigation, depending on the circumstances.
- We are pursuing formal assurances and documentation from LifeLabs that they have taken adequate security measures to prevent this from re-occurring.
- Next steps for this incident will be determined based on our agreement with LifeLabs.

4. How do the Freedom of Information and Protection of Privacy Act (FOIPPA) and Personal Information Protection Act (PIPA) legislation apply in this case?

- Government and the rest of the public sector are subject to FOIPPA, whereas private sector organizations are subject to PIPA.
- Government's contract with LifeLabs, which includes the privacy terms to which LifeLabs must adhere, sets a robust standard for LifeLabs to meet with respect to privacy and security.

5. The Information and Privacy Commissioner has called for changes to the *Personal Information Privacy Act*. Why hasn't the Province acted?

- PIPA applies to over 300,000 private organizations so any changes must be carefully considered to ensure the intended result is achieved.
- We have received recommendations from the Office of the Information and Privacy Commissioner, past Special Committees, advocacy groups and the public.
- This feedback will help inform any future legislative or policy changes to improve the way organizations protect personal information.

6. What does government do to protect the personal information they are entrusted to protect?

- Government has security controls to protect networks, systems and data - with systems monitoring 24 hours per day, seven days a week.
- We regularly upgrade security measures to protect government users from threats like malicious emails and websites.
- B.C. is the only province with a centralized team of highly trained information incident investigators to address any government privacy breaches thoroughly using an established and effective incident management process.
- The incident response team is mobilized to react to any incidents that occur and they lead ministries through the containment of any threats and the mitigation of associated risks and harms.

Wensink, Alison PREM:EX

From: LeGuilloux, Marg GCPE:EX
Sent: December 17, 2019 10:42 AM
To: Aaron, Sage PREM:EX
Subject: FW: LifeLabs NR is out

FYI.

Marg LeGuilloux

Executive Director
Communications - Social Ministries
GCPE
778-584-1259

From: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>
Sent: December 17, 2019 10:33 AM
To: LeGuilloux, Marg GCPE:EX <Marg.LeGuilloux@gov.bc.ca>
Subject: LifeLabs NR is out

LifeLabs NR is out

J M P

Desk: 236-478-0302
Cell: 250-886-2154

From: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>
Sent: December 17, 2019 10:29 AM
To: Prevost, Jean-Marc GCPE:EX <Jean-Marc.Prevost@gov.bc.ca>; Rongve, Ian HLTH:EX <Ian.Rongve@gov.bc.ca>
Subject: FYI - LL website live w/ open letter

Just FYI – below from CITZ

And online: <https://www.newswire.ca/news-releases/lifelabs-releases-open-letter-to-customers-following-cyber-attack-889534499.html>

From: Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca>
Sent: December 17, 2019 10:21 AM
To: Carroll, Scott CITZ:EX <Scott.Carroll@gov.bc.ca>; Donaldson, Ian R CITZ:EX <Ian.Donaldson@gov.bc.ca>
Cc: Marriott, Sarah GCPE:EX <Sarah.Marriott@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Lauvaas, Kirsten GCPE:EX <Kirsten.Lauvaas@gov.bc.ca>; Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>
Subject: RE: FOR REVIEW: LL KM Q A Dec 16 6pm

Their website is live:
<https://www.customernotice.lifelabs.com>
or
<https://customernotice.lifelabs.com/>

Here's the text:

An Open Letter to LifeLabs Customers

To our customers:

Through proactive surveillance, LifeLabs recently identified a cyber-attack that involved unauthorized access to our computer systems with customer information that could include name, address, email, login, passwords, date of birth, health card number and lab test results.

Personally, I want to say I am sorry that this happened. As we manage through this issue, my team and I remain focused on the best interests of our customers. You entrust us with important health information, and we take that responsibility very seriously.

We have taken several measures to protect our customer information including:

- Immediately engaging with world-class cyber security experts to isolate and secure the affected systems and determine the scope of the breach;
- Further strengthening our systems to deter future incidents;
- Retrieving the data by making a payment. We did this in collaboration with experts familiar with cyber-attacks and negotiations with cyber criminals;
- Engaging with law enforcement, who are currently investigating the matter; and
- Offering cyber security protection services to our customers, such as identity theft and fraud protection insurance.

I want to emphasize that at this time, our cyber security firms have advised that the risk to our customers in connection with this cyber-attack is low and that they have not seen any public disclosure of customer data as part of their investigations, including monitoring of the dark web and other online locations.

We have fixed the system issues related to the criminal activity and worked around the clock to put in place additional safeguards to protect your information. In the interest of transparency and as required by privacy regulations, we are making this announcement to notify all customers. There is information relating to approximately 15 million customers on the computer systems that were potentially accessed in this breach. The vast majority of these customers are in B.C. and Ontario, with relatively few customers in other locations. In the case of lab test results, our investigations to date of these systems indicate that there are 85,000 impacted customers from 2016 or earlier located in Ontario; we will be working to notify these customers directly. Our investigation to date indicates any instance of health card information was from 2016 or earlier.

While you are entitled to file a complaint with the privacy commissioners, we have already notified them of this breach and they are investigating the matter. We have also notified our government partners.

While we've been taking steps over the last several years to strengthen our cyber defenses, this has served as a reminder that we need to stay ahead of cybercrime which has become a pervasive issue around the world in all sectors.

Any customer who is concerned about this incident can receive one free year of protection that includes dark web monitoring and identity theft insurance.

Yours sincerely,

Charles Brown

President and CEO
LifeLabs

Page 6 of 8 to/à Page 8 of 8

Withheld pursuant to/removed as

s.3