From: Desmond, Kevin <Kevin.Desmond@Translink.ca>
Sent: Friday, December 4, 2020 12:56 PM
To: TransLink All (Including Contractors)
Cc: McDaniel, Michael; LADRAK MICHEL; Dave Jones
Subject: CEO update on network disruption

Good afternoon,

As you are aware, very early on Tuesday morning, our Business Technology Services team identified suspicious activity on our network. We have confirmed that TransLink was the target of a cybersecurity event in which a third party deployed encryption software – otherwise known as ransomware – within our network.

Thanks to the efforts of our Business Technology Services team, who took immediate and decisive steps to respond, including isolating and shutting down key IT infrastructure and systems, we were able to contain the threat and reduce the impact on our infrastructure.

We are currently working on a business resumption plan to restore full access to our systems as quickly and safely as possible. This process will take time, and we thank each and every one of you for your patience and resilience as we work to get it done.

Impact on the Business

While the restoration efforts are ongoing, all corporate, on-premise systems, including PeopleSoft, MyK2, Q, OWL, MyTime, etc. will remain off-line.

You will still have access to Office365, including Outlook, Teams and OneDrive. You will also have access to offline programs such as Word and Excel. If your work is directly impacted by system outages, we ask you to connect with your manager and discuss alternate ways to spend your time.

Employee Data

We are conducting a comprehensive forensic investigation to determine if any sensitive information may have been compromised as a result of the incident. We continue to investigate and we will continue to keep employees informed.

While the investigation is ongoing, to help alleviate any concerns employees may have, we will be offering a one-year subscription to credit monitoring and fraud protection services for any employees who are interested. As soon as we receive more information about signing up for these services, we will provide a further update. As a matter of best practice, employees should always monitor their accounts for any unusual activity.

Through the forensic investigation we will be seeking to understand exactly how the incident occurred and to identify opportunities to further strengthen our defenses. Although no

organization can be entirely immune, the incident serves as an important reminder that we all play a role in protecting our information technology infrastructure.

As a reminder:

1. Please remain vigilant about emails with links or attachments or that request sensitive information – even if they appear to be from an individual or company you know or trust. If you're unsure, please report them through the Report Message functionality in Outlook or contact BTS via servicedesk@translink.ca or 778.375.7575. It is better to be overcautious than sorry.
2. Practice good password hygiene. Use unique or complex phrases, never share your password, and never use the same password for multiple accounts, websites, or applications. Never use your TransLink password for third-party applications or systems.

Finally, if you are contacted by an external stakeholder or a member of the media, please direct them to media@translink.ca.

Thanks for your ongoing support and dedication. Together, we will get through this.

Sincerely,

Kevin

Kevin Desmond

Chief Executive Officer
T: 778.375.7777 | kevin.desmond@translink.ca

TransLink

South Coast British Columbia Transportation Authority

400-287 Nelson's Court, New Westminster, BC, V3L 0E7, Canada