

EMAIL paula.lombardi@siskinds.com

FILE NO. 863752

Sent via Email

September 18, 2019

Joan Thomson, AMCTO CMO  
Acting Chief Administrative Officer  
The Corporation of the City of Stratford  
P.O. Box 818, 1 Wellington Street  
Stratford ON N5A 6W1

Dear Ms. Thomson:

**Re: Cyber Incident – City of Stratford**

In response to your request for an overview of the cyber incident experience by the City we can advise as follows. On April 15th, 2019, Deloitte LLP (Deloitte), a global leader in cyber incident response, was retained to assist the City of Stratford (the City) respond to a ransomware incident. This summary provides an overview of incident management activities including the incident background, response activities, and determination of data exposure. Deloitte's engagement began on April 15th, 2019 and ended on May 31st, 2019.

The City detected the incident on April 14<sup>th</sup> after identifying several crucial services which became unresponsive and unavailable. The City proceeded to retain Deloitte to assist in managing and assessing the cyber incident. Deloitte provided incident management guidance to the City and forensically gathered evidence which was reviewed, analyzed and correlated with other data. Deloitte followed a methodology based on industry good practices and well-established frameworks, in search of anomalies, instances of malicious activities including unauthorized access to the environments, malicious ingress/egress connection attempts and irregular patterns. Deloitte has noted that there were some identified limitations in the acquisition of evidence, due to several critical servers being encrypted, or with overwritten and unrecoverable evidence.

Mr. Kevvie Fowler, the Global Incident Response Leader at Deloitte, when asked about the scope of the incident stated, "On April 14th, a cyber criminal was able to gain unauthorized access to and executed malware on eight of the City of Stratford's servers which contained

**DIRECT**  
**TELEPHONE** (519) 660-7878  
**FACSIMILE** (519) 660-7879

**HEAD OFFICE**  
**TELEPHONE** (519) 672-2121  
**FACSIMILE** (519) 672-6065

4017428

Personally Identifiable Information (PII) as defined by NIST<sup>1</sup>. Based on procedures performed and information available, Deloitte did not identify any evidence of loss, access or disclosure of PII in relation to the ransomware incident.”

To contain the incident, all endpoints were disconnected from the network, and Deloitte deployed network security monitoring and forensics tools across the City's environment to monitor for malicious behaviour between April 26th, 2019 until May 31st, 2019. As part of Deloitte’s investigation, Deloitte identified several security controls in place at the City that potentially limited the propagation and impact of the ransomware incident.

The City engaged Deloitte to serve as an incident advisor and to assist in the response to the ransomware incident. Deloitte was able to maintain visibility, holistically, across the City’s response activities and in Deloitte’s report, captured that the City and contracted third parties worked together in an effective manner to recover from the incident and:

- Minimize the impact to the City of Stratford and its residents; and,
- Improve the technological and administrative security controls within the City to help reduce the imminent risk of a repeat ransomware incident.

Should you have any questions or wish to discuss in more detail please contact the undersigned.

Yours truly,

Siskinds LLP



Per:

Paula Lombardi  
Partner

---

<sup>1</sup> NIST Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).  
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>