SAINT JOHN

COUNCIL REPORT

M&C No.	2019-13
Report Date	January 23, 2019
Meeting Date	January 28, 2019
Service Area	Corporate Services

His Worship Mayor Don Darling and Members of Common Council

SUBJECT: Click2Gov Data Breach and Cybersecurity Priorities

OPEN OR CLOSED SESSION

This matter is to be discussed in open session of Common Council.

AUTHORIZATION

Primary Author	Commissioner/Dept. Head	City Manager
Stephanie Rackley-Roach ***Jonathan Taylor***	***Neil Jacobsen***	***John Collin***

RECOMMENDATION

The City Manager recommends that Common Council endorse the cybersecurity strategy presented in this report.

EXECUTIVE SUMMARY

On December 21, 2018, it came to the City's attention through two online articles that an unknown third-party may have gained access to confidential customer payment information provided through the Click2Gov application, an online payment tool to pay such things as parking tickets. In working with CentralSquare Technologies, the owner of the Click2Gov application, a breach of confidential information belonging to individuals that had paid parking tickets using purchasing cards was confirmed. This report outlines the details of the data breach that spans from May 2017 to December 2018, including how the breach happened and why the City was not aware of the breach sooner.

The Right to Information and Protection of Privacy Act requires that the City provide notification to individuals of potential data breaches. As a result, the City mailed a written notice, in both official languages, to anyone that may have paid a City of Saint John parking ticket using a purchasing card during the at-risk timeframe. In addition to two public updates posted on the City's website, the mailed notification was sent to over 10,000 individuals potentially at risk.

The current Click2Gov software application was taken offline and continues to be unavailable to the public to pay parking tickets. In order to ensure trust in the payment system, of both the public and staff, the City is investigating another online payment solution.

Cyber threats to municipalities are on the rise. Given the risk and potential damages from cyberattacks, staff is proposing short-term actions to improve cybersecurity in 2019. Over the next year, these actions will evolve into a long-term, comprehensive cybersecurity strategy.

PREVIOUS RESOLUTION

N/A

REPORT

Overview of Data Breach and Investigation

On December 21, 2018, it came to the City's attention through two online articles that an unknown third-party may have gained access to confidential customer payment information provided through the Click2Gov application. The City uses the Click2Gov software owned by CentralSquare Technologies to provide customers with the ability to pay parking tickets online through the City's website. The City of Saint John was among forty-seven (47) municipalities in North America that were identified in the online reports as having experienced a potential breach using this CentralSquare Technologies software.

City staff immediately started an investigation to determine if there was any validity to the claims outlined in the articles. A case was opened with CentralSquare Technologies at the City's insistence to complete a forensic investigation. CentralSquare Technologies then engaged Sylint, an internationally recognized cybersecurity and digital data forensics firm with extensive experience discretely addressing some of today's biggest breaches.

Sylint initially completed a live scan of the City's server and immediately determined there had been malicious activity. Through a more in-depth review of the City's server, Sylint was able to outline how the attackers were able to gain access and collect user information. Attackers captured the following information: name (including first name, last name, and middle initial), account number (i.e., card number), CVV number (security code), card expiry date, and address.

From the investigation, Sylint was able to determine when the City's server was first injected with card capturing code (May 2, 2017) and the last web access by the attacker (December 11, 2018). Sylint was not able to determine the true at-risk date of the attack, meaning when card data was actually extracted from the City's server. The investigator was also not able to identify which individuals had their card information breached.

The process used by the attacker involved them accessing the City's server through the web to download a file with captured card information. Once downloaded, the attacker would delete the file, which would trigger the creation of a new file with card information. With this process, the attacker essentially did not leave any evidence of their attack on the City's Click2Gov server.

Based on the details provided by Sylint on malicious activity on the City's Click2Gov server, City staff determined the at-risk period to be May 1, 2017 to December 16, 2018.

Those at risk of a potential beach in their information included anyone that paid a parking ticket using a payment card online, by telephone, or in person.

Click2Gov Maintenance and Due Diligence

CentralSquare Technologies is the current owner and support of the City's HTE Naviline Enterprise Resource Planning (ERP) system that includes the Click2Gov software. Information Technology (IT) staff have been diligent in ensuring the City is using the latest version of Naviline and have been testing the upgrades prior to using them in a live environment. Maintenance of the system, including patching, is carried out regularly, either by staff or the vendor. Patching involves uploading a set of changes to a computer program, or its supporting data, to update, fix, or improve it, including addressing security vulnerabilities.

The City received a concern from an individual on November 16, 2018 claiming their payment had been breached after paying a parking ticket on the City's website. City staff opened a case with CentralSquare Technologies to determine if there was validity in this claim. The vendor completed a scan of the City's Click2Gov server and found no malicious activity. CentralSquare Technologies also indicated that the version of Click2Gov the City was using was not part of the targeted attacks. The breach of information in other municipalities was on servers using the new Click2Gov3 version.

While investigating the validity of the breach December 21, 2018, CentralSquare Technologies advised they had completed a proactive scan of the City's server in July of 2018. At that time there were no indications of any breaches or malicious activity on the City's server.

The City received a security advisory in September of 2017. In that advisory, Superion (now CentralSquare Technologies) "were investigating a report of potentially compromised customer data from a Click2Gov3 customer that has different characteristics". Superion also indicated they "have not seen any evidence that the servers were compromised through a security issue with the Click2Gov software, Superion takes security issues very seriously and we are continuing to investigate".

Upon receipt of the advisory, the IT team completed the mitigation that was outlined, which included a review of the City's server to check for vulnerabilities and to apply security patches. It is noteworthy that the City was using Click2Gov1, as an upgrade to Click2Gov3 for parking ticket payment was not in production.

In November 2018, as City staff was working on upgrading to Click2Gov3, online research revealed continuing breaches to the Click2Gov application as late as October in the same year. Staff proactively connected with CentralSquare Technologies to ensure that the migration to Click2Gov3 was safe. Again, staff was advised that the data breaches were occurring on Click2Gov3 servers and their customers were being notified of the security mitigation protocols.

Notification to Impacted Individuals

Immediately upon verifying a breach of the City's Click2Gov1 server on December 21, 2018, the City's response team updated Common Council and issued a public notice on the City's website and the notice was pushed out using social media and traditional media outlets. This notification outlined a potential impact to those individuals that paid parking tickets using the online application, the steps the City was taking to

investigate the breach and ensure the safety of user information, steps users should take if they thought they may have been impacted, and how to pay parking tickets while the online functionality was unavailable.

A second public notice was issued on December 31, 2018. This notification provided a timeframe for those that may have been impacted by the breach. The public was made aware that the breach could impact anyone who had paid a City-issued parking ticket over the past two years, from early 2017 to December 16, 2018.

As required through provincial legislation, the Common Clerk, the head of privacy and access for the City of Saint John, notified the Office of the Integrity Commissioner (the Integrity Office) on December 24, 2018. This involved completing a reporting form and submitting it to the Integrity Office. A case manager was assigned to the City to review notification requirements and next steps with the City's response team.

Given that the forensic investigation was unable to determine which individuals were impacted by the breach (i.e., from whom purchasing card information was stolen), City staff decided to mail a notice to any individual that paid a parking ticket by purchasing card between May 1, 2017 and December 16, 2018. Mail was determined to be the only way to notify individuals that their personal information may have been breached, as phone numbers and email addresses were not recorded as part of the payment process for parking tickets.

During a conference call with the Integrity Office case manager on January 4, 2019, the draft notice was reviewed, feedback was provided, and next steps were discussed. The case manager was complimentary of the City's efforts to ensure public awareness and notification on the breach of personal information.

The notice was mailed out on January 10 and 11, 2019 to approximately 10,000 individuals (in both official languages) who paid parking tickets with purchasing cards during the aforementioned timeframe. In mailing these notices, there is a risk that individuals who may have moved since paying their parking ticket will not receive the notice of a potential breach to their personal information. The City is using the information that is available to determine addresses.

Since the notice was mailed out, the City telephone line provided in the notice received twelve (12) calls. Most callers wanted to know what to do or asked when the ticket was paid as they did not recall. The Police Force has reported eighteen (18) calls on file.

Corrective Measures and New Payment System

The City disabled the Click2Gov application on the City's website immediately upon learning of a potential breach. The online payment option has remained offline since December 21, 2018. Individuals that need to pay parking tickets can do so with the other options outlined on the City's website or on the parking ticket: by mail, telephone, or in-person through point of sale terminals.

City Staff are investigating the implementation of a new online payment solution. The solution being investigated is currently used by Saint John Energy, Halifax Water, and Maritime Electric to take payments. This system is also currently being used by the Saint John Parking Commission for recurring monthly billing for off-street parking.

City staff has completed preliminary investigation with the vendor to determine the feasibility of the new solution, including functionality to integrate with parking ticket information and Payment Card Industry Data Security Standard (PCI-DSS) compliance. Provided that all requirements are met to securely process parking tickets, the expected timeline for launching the online payment solution is the second quarter of 2019.

City of Saint John Cybersecurity Strategic Actions

Cyberattacks on municipal governments are on the rise. With thousands of attacks launched daily around the world, it is not a matter of "if", but "when" an organization will experience a cyberattack.

Local governments are attractive targets for cyberattacks given they house private data (on-premise servers), cyber security is not a top priority, attacks have been successful, and are public-facing. The cost of successful cyberattacks include interruptions in essential service delivery, loss of data or records, loss of productivity, cost recovery at the expense of taxpayers, inability to collect revenue, and erosion of trust.

Municipalities in Ontario and Quebec made headlines in 2018 as victims of cyberattacks. In these cases, municipalities were forced to negotiate with cyber attackers on payment amounts to release files encrypted through ransomware attacks.

As part of the 2019 budget process, the IT team highlighted cybersecurity as a priority. Additional funds were included in the budget to enhance the safeguarding of the City's information systems and data. The following chart outlines the strategic cybersecurity actions that will be undertaken in 2019. These are short-term actions required to enhance the safeguarding of the City's information systems and data, and will evolve over the next year to address more long-term requirements.

Action	Description
Risk Threat Assessments	As per the agreement approved by Common Council on December 17, 2018, the IT team will work with the Canadian Institute of Cybersecurity (CIC) to assess and evaluate security measures, as well as to identify vulnerabilities and risks to the security of all information along with the recommended mitigations.
Enhanced Antivirus Solution	The ways in which cyber attackers are creating and deploying malware have evolved to evade traditional antivirus detection. The Information Technology team will investigate and implement more antivirus solutions.
Firewall Upgrades and Security Information and Event Management System (SIEM)	The Information Technology team is in the process of upgrading firewalls and investigating the purchase of a new SIEM to provide more robust monitoring of information systems for detection and response to cyberattacks.
Cybersecurity Expertise	The TI team will invest in improving security expertise within the IT team through a combination of training and contracted support.

Actions Continued	Description
Employee Education	The IT team will work with the CIC to deliver awareness programs aimed at educating all employees in how they can identify and prevent cybersecurity threats.
Cyber Insurance	With the support of the Risk Management team, the City will secure cyber insurance that will meet the City's needs in the event of a successful cyberattack.
Security and Recovery Plans	The IT team will ensure there is a well-documented disaster recovery and business continuity plan in place in the event of future attacks.

STRATEGIC ALIGNMENT

The proposed cybersecurity strategy aligns with Council's priority of valued service delivery. The actions outlined in the strategy focus on service improvements that enhance the safeguarding of the City's information systems and data, ensuring that service delivery is seamless and customer information remains confidential.

SERVICE AND FINANCIAL OUTCOMES

Strategic initiatives outlined in this report are funded in the 2019 General Fund Operating Budget.

INPUT FROM OTHER SERVICE AREAS AND STAKEHOLDERS

The report has been reviewed by the Click2Gov breach response team. The team includes Information Technology, Finance, Communications, Risk Management, Legal, Common Clerk's Office, and Parking Commission staff.

ATTACHMENTS

Presentation