LESSONS LEARNED FROM THE TTC'S RANSOMWARE ATTACK

Posted on April 23, 2024

Categories: Insights, Publications

Cybersecurity policies are only as good as the systems in place to make sure they're followed. The recent investigation by the Information and Privacy Commissioner of Ontario ("**IPC**") into the effectiveness of the Toronto Transit Commission's ("**TTC**") cybersecurity measures to prevent a cyber attack underscores this point.[1]

This bulletin will review the IPC's key findings and recommendations relating to the TTC's cybersecurity and incident response practices.

Background: The Ransomware Attack and the TTC's Response

In late 2021, the TTC experienced a ransomware attack on its IT systems. A threat actor sent an email to a TTC employee from the email address of a trusted third party, whose systems the threat actor had compromised. The employee clicked a malicious link in the email, allowing the threat actor to infiltrate the TTC's systems. The threat actor then exploited a security vulnerability and used malware to encrypt and transfer data, including personal information. The TTC was able to detect the breach and activated its IT security protocols to mitigate the threat.

The TTC managed to restore most of its systems from backups, but the incident resulted in the theft of personal information of thousands of past and present employees. The types of personal information confirmed to have been affected by the incident included names, contact information, employment history and medical conditions. For a small number of records, the data may have also included sensitive information such as criminal history, immigration information, financial information, and Social Insurance Numbers. The TTC also noted that a small sample of TTC files may have been briefly posted on the dark web.

The TTC issued a public notification at the outset of the incident and later followed up with private notification to all individuals potentially affected by the incident with an offer of credit monitoring.

IPC Investigation and Findings

The IPC investigation considered two issues: (1) whether the TTC had reasonable measures documented and in place to prevent unauthorized access to personal information within its systems, in accordance with

MFIPPA;[2] and (2) whether the TTC responded adequately to the breach.

Finding #1: The TTC did not have reasonable security measures

The IPC found that the TTC did not have reasonable security measures in place to prevent the unauthorized access to personal information on its systems. In particular, the TTC was found to have failed to implement an available security patch that was publicly known and available at the time of the incident. This patching failure was contrary to the TTC's own internal policies surrounding patching, which required critical patches to be deployed within 72 hours.

Notably, the IPC did not blame the TTC for its employee clicking the malicious link in the email. The employee had taken a mandatory cybersecurity training one month before the incident, which covered phishing and common email red flags. The IPC noted that this phishing attack was pernicious and difficult to spot, as it came from a trusted third party whose system was compromised. With that said, for strict adherence with IPC best practices, the employee should have hovered over and reviewed the hyperlink URL before clicking it, which may have avoided the incident.

Finding #2: The TTC's breach response procedure was sufficient

The IPC was generally satisfied with the TTC's breach response. The TTC responded promptly to identify the attack, shut down employee access to TTC devices, and scanned and cleaned its devices in order of priority. It promptly engaged forensic investigators as part of its security protocols to further investigate the breach.

In terms of notification, the TTC issued multiple waves of notifications to employees, including letters to affected employees setting out the information that had been impacted by the attack.

In terms of remediation, the TTC engaged industry-leading information technology experts to assist in the restoration of its systems. It procured penetration testing and vulnerability assessments. It also developed new policies and updated its patching standard to clearly set out required steps in identifying, implementing and testing required security patches. A new vulnerability management policy provides clearer guidance on who is responsible for patching the TTC network.

The only gap the IPC found in the TTC's remediation efforts, as compared with established IPC guidance, was a lack of encryption protocols for personal information stored on the TTC's systems. The IPC recommended that the TTC implement encryption as the default on all documents, devices and databases containing personal information.

Takeaways

This decision presents several notable takeaways for organizations of all types. We have divided these

takeaways into two categories: data security and incident response.

Takeaways for Data Security

1. **Accountability, accountability, accountability**: While policies are important, they need to be carefully implemented to be effective. Organizations should clearly specify what team members are responsible for what actions under what timelines to ensure its policies are effectively applied. In this case, the TTC's patch standards would have prevented the incident, but they were not effectively implemented.
2. **Regular Employee Training is Essential**: Even with cybersecurity training in place, employees may still fall victim to sophisticated phishing attacks. Continuous training and awareness programs are necessary to help employees recognize and respond to security threats effectively.
3. **Patch Management**: A robust patch management policy and procedure is essential. Failure to implement available security patches, especially for known vulnerabilities, can leave systems vulnerable to attacks and organizations exposed to potential liability.
4. **Encryption**: Evaluate the need for encryption protocols, especially for sensitive personal information. Implementing encryption as the default for all documents containing personal information can provide an additional layer of protection against unauthorized access.
5. L**earn from Regulatory Guidance**: Pay attention to regulatory guidance and recommendations, such as those provided by the IPC or Canada's other privacy regulators. Cybersecurity practices should be routinely reviewed and updated to ensure alignment with established standards to demonstrate compliance and reduce legal risks.

Takeaways for Incident Response

1. **Response Time Matters**: Prompt detection and response to security incidents is critical. It is important to establish clear protocols and procedures for identifying, containing, and mitigating the impact of breaches to minimize damage and prevent further compromise.
2. **Engage Forensic Experts**: Depending on the severity of a security incident, forensic investigators may need to be engaged to conduct a thorough analysis. Their expertise can help uncover the extent of the breach, identify vulnerabilities, and provide recommendations for improvement.
3. **Effective Communication**: Privacy regulators encourage timely open and transparent communication with affected parties.

Cybersecurity is an ongoing process that requires continuous improvement and adaptation. Organizations should regularly assess their security posture, identify areas for improvement, and implement measures to address emerging threats and vulnerabilities.

Members of McMillan's Privacy and Data Protection team are available to assist organizations with aligning their data security and breach response strategies, policies and procedures with legal and regulatory standards.

[1] Ontario Information and Privacy Commissioner, *Privacy Complaint MR21-00114* (April 5, 2024), available here. This investigation was carried out pursuant to Ontario's municipal privacy law, the *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56. [**MFIPPA**]
[2] General Regulation to MFIPPA, RRO 1990, Reg 823, section 3(3).

by Mitch Koczerginski and Robbie Grant

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.