Office of the Auditor General of Ontario
Bureau de la vérificatrice générale de l'Ontario

Information Technology (IT) Systems and Cybersecurity at Metrolinx

2020 Value-for-Money Audit

Why We Did This Audit

- Information Technology (IT) systems at Metrolinx play a vital role in managing day-to-day public transit operations, which provided over 76 million passenger trips in the 2019/20 fiscal year.
- With the evolution of technology in the transportation industry, cybersecurity is a growing concern due to the increase in cyberattacks that have increased with the growth of technology.

Why It Matters

- Interruptions caused due to IT issues can negatively affect customers' experience with train delays and cancellations, fare payments and potentially reduce provincial revenue.
- Cybersecurity is a critical measure to protect Metrolinx from cyberattacks, privacy breaches and unauthorized access to IT infrastructure.

What We Found

- Critical transit operations have experienced IT-related incidents—such as network connectivity issues, system malfunctions, and software and hardware issues—resulting in train delays and cancellations. We noted that from January 2015 to January 2020 there were nearly 4,500 GO train and UP Express delays and cancellations resulting from IT software and hardware issues.
- Although Metrolinx has the technology and necessary data to automatically refund customers who qualify for the Service Guarantee Program, Metrolinx does not do this. In the last five years, of the 4,500 train delays and cancellations due to IT incidents, only 23% of the eligible customers applied to the Program for a total refund of about $450,000, with another approximately $2.2 million of applicable refunds going unclaimed.
- PRESTO's IT system sometimes charged customers twice and charged regular adult fares instead of reduced fares to students and seniors. In addition, funds were not always added to customers' PRESTO cards on time, resulting in PRESTO customers' cards being declined due to insufficient funds.
- Metrolinx does not assess whether it has sufficient staffing resources or should hire full-time employees prior to contracting staff at much higher rates. We noted that contractors are assigned key management positions and decision-making roles, including hiring and supervising other contractors. Metrolinx relies heavily on external contractors for IT operations and services and has paid approximately $157 million to IT contractors in the last five years, which is 2.5 times higher than the salaries and benefits paid for its full-time staff in the same period.
- With the exception of PRESTO's IT system, Metrolinx has not performed regular security scans, such as penetration tests, and does not always review software code for security weakness. There have been two significant security breaches at Metrolinx in the last five years that resulted in disclosure of customers' personal information. Metrolinx does not consistently safeguard its customers' personal information by applying security controls such as encryption. In addition, Metrolinx does not have a disaster recovery strategy, and has not tested its ability to recover its operations in an event of an actual disaster such as a major cybersecurity attack, software issues from unplanned changes or power outages.
- Metrolinx has not taken a centralized approach to procuring IT systems and websites. We found that different departments procured their own IT systems and websites, resulting in a number of redundant IT systems. duplicating functions that already existed in other Metrolinx departments.

..../2

Conclusions

- Metrolinx does not always have systems and processes in place to manage its IT operations effectively, efficiently or with due regard for economy. Critical transit operations, including PRESTO, have been impacted by IT system-related issues.
- Metrolinx is overreliant on IT contractors for day-to-day operations of IT systems and services. Metrolinx spends more for IT contract staff than it would have for regular full-time staff, and does not always ensure that contract staff provide better value for money when making hiring decisions.
- Metrolinx's cybersecurity functions need improvement. With the exception of PRESTO's IT system, the personal information of Metrolinx employees and customers, as well as sensitive corporate information, needs to be more secure. Metrolinx also does not have an overall IT strategy, which has resulted in redundant IT systems and websites.

Read the report at www.auditor.on.ca