Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

April 25, 2025

SENT BY EMAIL

Jennifer Saville
Freedom of Information Coordinator (Acting)
Toronto District School Board
050 Yonge Street, 5th Floor
Toronto, ON M2N 5N8

Email Address: jennifer.saville@tdsb.on.ca

Dear Jennifer Saville:

RE: Complaint MR24-00071

On June 11, 2024, Toronto District School Board (TDSB or the school board) reported a breach to the Office of the Information and Privacy Commissioner of Ontario (IPC or this office) pursuant to the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act* or MFIPPA). File MR24-00071 was opened to deal with this matter.

The circumstances of the breach involved a cyberattack that resulted in the compromise of TDSB's data. A threat actor accessed TDSB's test lab environment (test environment), which contained the personal information of an estimated 280,000 individuals.

BACKGROUND:

TDSB explains that its test environment is a separate system used to evaluate new technologies and applications before deployment in the live production environment. TDSB acknowledged that a subset of real production data, including student and staff personal information, was used in this test environment. TDSB explained that the intended purpose of using production data in this environment was to facilitate realistic testing of new technologies and changes to applications, prior to applying them in the production environment.

On May 27, 2024, TDSB discovered a Lockbit 3.0 ransomware note from a threat actor stating, "your data is stolen and encrypted." This cyberattack resulted in the encryption of 16 systems associated with the TDSB's test environment. The test environment was subsequently taken offline.

TDSB reported that the incident was contained immediately after it was discovered on May 27, 2024. On June 12, 2024, TDSB issued a pre-emptive notification to TDSB staff members and to parents/guardians with respect to this incident. TDSB informed the affected individuals of the circumstances of the breach, that the breach affected TDSB's test environment, and that TDSB notified the Toronto Police Service of this breach.

TDSB further communicated that it was in the process of conducting a thorough investigation to understand the nature of the incident, any impact on its network, and if any personal information may have been affected by the incident.

To investigate the incident, TDSB immediately implemented its Cyber Security Incident plan and Privacy Breach Protocol, along with engaging its core incident response team. TDSB partnered with cybersecurity experts to assist with the containment, investigation, remediation and to conduct a forensic investigation into the cybersecurity incident. Additionally, the Toronto Police Service, the Canadian Centre for Cyber Security, and the Canadian Security Intelligence Services were all immediately informed.

The Personal Information at Issue:

TDSB engaged a third party to analyze the records affected and found that the test environment contained the information of 42,000 employees and personal information 238,000 students.

The business-related information relating approximately 42,000 current employees of TDSB includes the following:

- Full name
- Employee number
- TDSB department
- TDSB position/title
- TDSB phone number
- TDSB email address
- TDSB full business address (e.g. school location)

The personal information relating to approximately 238,000 TDSB students includes the following:

- Full name
- school name
- grade
- TDSB e-mail address
- TDSB student number
- Day and month of student birthday

ISSUES:

Institutions, when confronted with a breach of personal information, must take appropriate steps in response. These steps include identification of the scope of the breach, containment of the personal information involved, notification of those affected, and investigation and remediation of the breach. The IPC guidance to institutions on these steps is set out in *Privacy Breaches:*

Guidelines for Public Sector Organizations.[1]

There is no dispute that TDSB is an institution, or that personal information, as defined by section 2(1) of the *Act,* was contained in the TDSB's test lab environment that was inappropriately accessed.

The following issues were identified during the review of this breach file at the Early Resolution stage:

1) Did TDSB have reasonable measures in place to prevent unauthorized access to personal information within its systems in accordance with section 3(1) of Regulation 823 of the *Act*?
2) Did TDSB take adequate steps to contain the breach?
3) Did TDSB take adequate steps to notify individuals who were affected by the breach?
4) Did TDSB take reasonable remedial measures that will likely prevent similar breaches in the future?

DISCUSSION:

Issue 1: Did TDSB have reasonable measures in place to prevent unauthorized access to personal information within its systems in accordance with section 3(1) of Regulation 823 to the *Act*?

Section 3(1) of Regulation 823 of the *Act* states:

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

In Privacy Complaint Report PR16-40, Investigator Lucy Costa (refers to the equivalent regulation under the *FIPPA*) stated that there is no mandate for a "one size fits all" approach, noting:

> ...It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions. [2]

[1] privacy-breach-protocol-e.pdf
[2] See paras. 72 of Privacy Complaint Report PR16-40.

Measures in Place at the Time of the Incident

In answering the IPC's questions regarding the security measures in place at the time of the attack, TDSB submitted that its test environment systems did not have any form of antivirus protection, or real-time monitoring software. It is important to note however, that TDSB's network segmentation separates its Test Environment from its Production environments.

In the affected test environment, TDSB submitted that the following measures were in place:

- Access and connection methods were controlled based on the user's role via Active Directory ("AD") user accounts;
- Specific AD accounts were assigned to staff members so that they could connect to the test environment via 2 mechanisms:
    1. Virtual Proxy Network
    2. Virtual Desktop Infrastructure gateway
- Staff members were required to contact the Test Environment Administrator to request access to the test environment. The Test Environment Administrator would then configure access to requestors.
- Access rights to systems, data and applications were granted upon request to staff as required for the test cases they were performing.

The above security measures, which were in place prior to the cyberattack, are important because they enforced controlled, role-based access to the test environment through Active Directory, ensuring users only had permissions necessary for their roles. By requiring specific AD accounts and secure connection methods like VPN or Virtual Desktop Infrastructure, access was both traceable and protected. Centralized access approval through a Test Environment Administrator added oversight, while granting access based solely on specific test case needs followed the principle of least privilege. Together, these measures reduced the risk of unauthorized access, enhanced accountability, and limited potential damage in the event of a breach.

Analysis

It is clear that vulnerabilities existed within TDSB's test environment at the time of the incident. TDSB's test environment did not have preventative measures in place to protect against cyberattacks aside from requiring a login name and password to gain entry to the environment. This is especially concerning since TDSB was using live information that included the personal information of staff and students for testing purposes. Furthermore, it was noted that multi-factor authentication (MFA) was not used in the test environment, which made it more susceptible to unauthorized access. Had TDSB taken a more proactive approach to identify, analyze and address the privacy risks involved with its test environment, including improvements to its preventative measures, such as MFA, the likelihood of such an attack succeeding would have been significantly reduced.

Considering that TDSB is a large public-facing organization, it should have up to date and effective security measures in place on all of its systems, and in particular, those that contain the sensitive personal information of children and youth.

Section 3(1) of Regulation 823 of the *Act* requires institutions to ensure security measures to prevent unauthorized access to records are "defined, documented and put in place."[3] Based on the information before me, I find that TDSB did not have reasonable security measures in place, as required under Regulation 823 of the *Act.*

In October 2022, the IPC published a Technology Fact Sheet addressing ransomware attacks, such as the one described above, titled How to Protect Against Ransomware.[4] The Fact Sheet discusses how this type of malicious software is becoming increasingly common and a serious threat to the security of electronic records. Organizations such as TDSB can take proactive steps to reduce the risk of bad actor(s) gaining access to their Information Technology (IT) systems, including the following:

- **Put in place email security controls** to detect and prevent the delivery of emails with suspicious links, malicious attachments, and spoofed sender addresses.
- **Establish a vulnerability management program**
- **Follow system hardening best practices**. Hardening generally involves reducing the number of pathways that an attacker can take to get access to your network.
- **Develop strategies to mitigate risk to systems that are out of date**.
- **Restrict employee access** to suspicious websites.
- **Ensure that all employees receive up-to-date cybersecurity awareness training** that includes content about ransomware attacks and how they occur.
- **Install security tools** on all computers that can prevent malware, quarantine suspicious files, and issue alerts, such as enterprise antivirus tools or endpoint detection and response tools.
- **Use good authentication practices** including effective passwords, password management, strong multi-factor authentication, and limiting password reuse.[5]

Institutions need to regularly address risks identified in all of their systems, including test environments if the information used contains the personal information of its clients, and applications on a regular schedule, rather than waiting for issues to arise. I recommend TDSB review the above-mentioned IPC guidance to ensure it has implemented sufficient preventative measures, make improvements to better adapt to the evolving threats, including ransomware, and take steps to keep its cybersecurity posture up to date.

Issue 2: Did the TDSB take adequate steps to contain the breach?

TDSB discovered the attack on May 27, 2024. To contain it, TDSB engaged cybersecurity experts who began the process of determining the scope of the breach with a digital analysis. TDSB submitted that its production environment was not affected by this breach and remained active.

TDSB submits that, upon discovering the cyberattack, it immediately took the following steps to contain the breach:

---

[3] RRO 1990, Reg 823 | General | CanLII
[4] See IPC Fact Sheet: fs-tech-how-to-protect-against-ransomware.pdf (ipc.on.ca)
[5] See IPC Fact Sheet: fs-tech-how-to-protect-against-ransomware.pdf (ipc.on.ca)

- Shutdown test environment servers to prevent any outside access;
- Shutdown test environment network to prevent any outside access;
- Shutdown Internet connectivity in the test environment network to prevent any outside access;
- Shutdown TDSB test environment between PowerSchool (student information system) and TDSB
- Disabled network drops to the test environment to isolate the affected systems;
- Disabled Azure Cloud for the test environment connection to isolate the affected systems;
- Disconnected all network drops to disable all activity on its test environment; and
- Turned off internet to the test environment to prevent any outside access.
- Notified law enforcement and cyber security authorities to investigate this matter
- TDSB indicated that it has not seen any public disclosure of student and staff data as part of its investigations which included monitoring of the dark web and other online locations. However, TDSB acknowledged that a subset of production data was posted on the dark web. TDSB asserts that this data did not include personal information.

Analysis

While the vulnerabilities present at the time of the attack cannot be fixed retroactively, I find that TDSB took reasonable steps to contain the breach including early isolation of the attack vector to prevent lateral infection, and its frequent monitoring of the dark web for fraudulent use of the stolen data.

Issue 3: Did TDSB take adequate steps to notify individuals who were affected by the breach?

In June 2024, TDSB issued a preemptive notification to TDSB staff members and parents/guardians/caregivers notifying them that a cyber security incident had occurred. The notification informed the affected individuals of the circumstances of the breach, that the breach affected TDSB's test environment, that TDSB notified the Toronto Police Service of this breach, and that the school board was in the process of conducting a thorough investigation to understand the nature of the incident, any impact on its network, and if any personal information may have been affected by the incident.

On August 29, 2024, TDSB issued a follow-up notice to the community detailing the circumstances of the breach. TDSB confirmed in the notice that personal information was present on the test environment when the breach occurred. TDSB emphasized that, according to its cyber security team and external security partners, it was determined that the risk to students in connection with this cyber incident is low. TDSB communicated that it took steps in response to the cyberattack including disconnecting the test environment, strengthening its systems, monitoring the dark web for any unauthorized disclosure of personal information and contacting law enforcement.

The breach notification letter contained the following information:

- The details and extent of the breach;
- The specifics of the personal information at issue;
- The steps that have been taken to address the breach;
- That the IPC was notified of the breach, and referral to the IPC website should the individual want to file a privacy complaint; and
- The contact details of the person within TDSB that the individual should contact if they have questions.

Additionally, TDSB posted a notice on its website which contains all of the above information.

Analysis

At this time, although the *Act* does not require an institution to notify affected individuals of a privacy breach, it is a best practice to notify individuals impacted by a breach. Institutions are encouraged to consider the number of individuals, sensitivity and the potential for abuse of the information at issue when deciding whether to notify.

TDSB data from the test environment was posted to the dark web by the threat actor(s). TDSB asserts that the exfiltrated data did not contain personal information. The reality of personal information being posted or available on the dark web is explained in Privacy Complaint Report MR21-00114[6], by Investigator, Jennifer Olijnyk:

> …once data is stolen, it is beyond the [institution's] control. In such situations, one should assume that it is being used by bad actors and take steps accordingly. While dark web monitoring can be useful in discovering a breach or determining its extent, it doesn't change the fact that institutions cannot remove personal information posted by bad actors.

It is understood that TDSB does not believe that data containing personal information was accessed, exfiltrated or included in the data posted to the dark web. This position is based on two factors:

- A screenshot provided by the threat actor purportedly showing the contents of the exfiltrated files
- TDSB's own review of the data that was publicly disclosed on the dark web.

[6] MR21-00114 - Information and Privacy Commissioner of Ontario

Based on these two factors, TDSB opted not to notify affected individuals. However, while TDSB maintains that there is no evidence that personal information was specifically accessed, exfiltrated, or disclosed by the threat actor, the IPC was not provided with material evidence demonstrating the full scope of the intrusion by the threat actor or how it conducted its data review process.

It is important to note that information supplied by threat actors, such as screenshots or assertions, cannot be considered reliable or verifiable. Threat actors are not credible sources, and their claims should not be relied upon to determine whether notification to affected individuals is appropriate. Based on the information shared with the IPC and the absence of conclusive forensic analysis, in my view, that it remains possible that the threat actor accessed and exfiltrated all information stored in the affected test lab environment.

Going forward, I encourage TDSB to provide potential affected individuals with enough details in its notice and with resources to assist them with protecting their personal information such as the IPC's guidance document Identity Theft: A Crime of Opportunity. This will give affected individuals a reasonable opportunity to take preventative measures should they choose to do so.

Issue 4: Did the TDSB take reasonable remedial measures that will likely prevent similar breaches in the future?

The IPC has published Privacy Breaches: Guidance for Public Sector Organizations (the Privacy Breach Protocol) that outlines best practices for institutions for responding to privacy breaches. It provides steps to take to identify the scope of the breach, how to contain it, and notification expectations. It also emphasizes how to reduce the risk of future privacy breaches, including implementing preventative and remediation measures, such as training.[7]

The Ransomware Attack

TDSB reported that the threat actor(s) accessed its test environment on May 27, 2024, and left a Lockbit 3.0 ransomware note stating, "your data is stolen and encrypted." This cyberattack resulted in the encryption of 16 systems associated with TDSB's test environment and the exfiltration of some of that information.

TDSB advised that during the investigation, the cybersecurity experts discovered that the threat actors posted a subset of TDSB operational data from the test lab environment to the "dark web". TDSB explained that some TDSB information was exfiltrated and posted on the dark web but asserts that personal information was not included.

TDSB reported that the cybersecurity expert's investigation into the root cause of the cyber security incident pointed to a compromised user account in the test environment where the threat actor was able to obtain a username and password. TDSB did not provide the IPC with information to support its position that exfiltrated data did not include personal information or how it came to the conclusion regarding the root cause of the attack.

[7] Privacy Breaches: Guidelines for Public Sector Organizations | Information and Privacy Commissioner of Ontario

The cyberattack on TDSB's test environment highlights significant security lapses. One of the major concerns was the use of production data in a test environment without preventative security measures such as a firewall, antivirus, or monitoring software. While TDSB has taken steps to contain the breach and improve security, the fact that real production data was accessible in an environment without proactive monitoring meant that unauthorized access may have occurred undetected for an extended period and is a major concern. Had additional measures such as MFA and antivirus software been in place, the likelihood of such an attack succeeding would have been significantly reduced. This underscores the importance of ensuring that test environments maintain the same security standards as live environments to prevent similar breaches. Moving forward, security frameworks must be consistently applied across all environments, and proactive monitoring must be prioritized.

Prevention

In this case, it is important that TDSB ensure it has adequate measures in place to prevent unauthorized access to its test environment. To detect, prevent and recover from a ransomware attack, if not already implemented, I suggest implementing the following:

- **Maintain regular backups** of information and systems in an offline environment.
- **Monitor the integrity of records** for irregular changes to large numbers of files or to highly sensitive information.
- **Detect the unauthorized use of tools and application programming interfaces** (APIs) that encrypt data.
- Use data loss prevention tools to log, monitor, and block network traffic of irregular file transfers to untrusted destinations or known file upload websites.
- **Configure computers** (user workstations, servers, and cloud infrastructure) **beyond default settings** to log a wide range of events and information. Actions that will help to ensure breach investigations have access to more detailed information include:

    - Taking steps to prevent logs from being modified, overwritten, or deleted without authorization after they are created.
    - Developing a retention schedule for event logs.

- **Combine event logs** from across your organization's Information Technology (IT) assets (including cloud infrastructure) into a centralized location. Consider using a security information and event management solution to develop a clearer picture of a ransomware attacker's activity.[8]

TDSB stated that it provides ongoing cybersecurity awareness training through simulated phishing campaigns and cyber security quarterly tips, covering a wide variety of topics and its incident response team carries out simulated cyber security incident exercises, facilitated by its security partners for the last 10 years. Additionally, staff members are required to receive privacy training and sign a confidentiality agreement upon hiring and annually thereafter.

[8] See IPC Fact Sheet: fs-tech-how-to-protect-against-ransomware.pdf (ipc.on.ca)

TDSB also stated that it follows the cybersecurity framework of a well regarded leader in cybersecurity standards to guide its security practices. As part of its "protect" phase the organization refers to this organization on key actions like cybersecurity awareness training, managing vulnerabilities and monitoring threats in its production environment.

I recommend that TDSB review its current privacy training program and revise it as necessary to ensure that it also provides adequate and specific privacy protection against unauthorized access to its test environment. The TDSB confirmed that the NIST (National Institute of Standards and Technology) Cyber Security Framework is now in place.

Incident Management

The TDSB partnered with cyber security experts to isolate and conduct an investigation, secure the affected systems, and determine the scope of the breach. The cyber security expert's investigation pointed to a compromised user account in the test environment where the threat actor was able to obtain a username and password. Manual steps and automated system response are in place to manage suspicious and compromised accounts.

Ransomware Attack Remediation Efforts

Following the breach, TDSB committed to implementing a series of security enhancements designed including:

- Ensuring that the production environment's network and production information is segmented from the test environment;
- Updating the test environment's Endpoint Detection and Response;
- Enhancing the test environment's network firewall rules and Indicators of Compromise (IOCs) blocking capabilities;
- Implemented a data anonymization tool for the test lab environment; and Enforcing MFA for all staff accounts including staff members who access TDSB's test environment.

These steps will strengthen TDSB's cybersecurity framework and prevent future incidents in its test environment. One of the most critical changes was the decision to discontinue the use of production data in test environments.

This measure is vital, as test environments often lack the same level of security controls as live systems, making them more vulnerable to cyberattacks. The decision to remove live data from the test environment, along with enhanced security measures, significantly reduces the risk of exposing sensitive personal information.

The Importance of Protecting Personal Information

As Canada's largest school board, the TDSB has a responsibility to protect the personal information of students, teachers, and staff. Educational institutions hold a vast amount of sensitive data, including student records, health information, employment details, and even financial data. Any unauthorized access to this information could result in identity theft, fraud, reputational harm, or other severe consequences.

Under the *Act,* institutions like TDSB are required to implement measures to safeguard personal information and prevent unauthorized access. The duty to protect personal information is not only a legal obligation but also a matter of public trust. Parents, students, and staff must have confidence that their private data is secure.

Educational institutions are also high-value targets for cybercriminals, as student data can be used fraudulently for years before its misuse is detected. Furthermore, the disruption caused by cyberattacks can significantly affect learning environments, delay administrative processes, and erode confidence in the institution's ability to manage its data securely.

Maintaining strict segregation between production and test environments prevents unauthorized access and data leakage. Role-based access controls and the principle of least privilege further reduce the risk of exposing sensitive data to unauthorized users. INVESTIGATION REPORT F10-02[9] underscores these concerns by emphasizing that real data containing personal information of identifiable individuals must never be used outside of a fully secured production system and the potential consequences of failing to do so. By recognizing the importance of these measures, an organization will ensure compliance with privacy regulations and maintain public trust. I recommend for the TDSB to follow these and other industry standard guidelines, so it can better secure their test environments, preventing them from becoming weak points in its overall security architecture.

Analysis

I am satisfied with the remedial steps taken by the TDSB in response to the breach of its test environment. The TDSB demonstrated a commitment to addressing the incident by partnering with cybersecurity experts, isolating and investigating the breach, and enhancing its security controls.

Specifically, the TDSB has addressed key security gaps by discontinuing the use of production data in test environments, strengthening Endpoint Detection and response capabilities, enhancing firewall rules, implementing robust Indicator of Compromise blocking, and enforcing MFA for all staff accounts. Additionally, the TDSB's ongoing cybersecurity awareness training and its adherence to cybersecurity frameworks like NIST reinforce a sustained commitment to cybersecurity best practices, further ensuring the protection of personal and sensitive information against potential breaches.

[9] 2010 BCIPC 13 (CanLII) | Electronic Health Information System (Re) | CanLII

CONCLUSION:

After considering the circumstances of this reported breach and the actions taken by TDSB, I am satisfied that TDSB responded adequately to the breach and that no further review of this matter is required.

Based on the information considered at the early resolution stage, I have reached the following conclusions:

- At the time of the incident, TDSB did not have reasonable security measures in place to protect the personal information as required by section 3(1) of Regulation 823 under the *Act*.

- Upon discovery of the threat actor(s), TDSB adequately determined the scope of the breach and took steps available to contain the breach.

- TDSB is committed to implementing reasonable measures to protect its test environment from cyberattacks as required by section 3(1) of Regulation 823 under the *Act*.

RECOMMENDATIONS:

Using production data in a test environment poses significant breach in security risks particularly when sensitive information such as personal identifiable information is involved. Test environments often lack the same level of security controls as production systems, making them more vulnerable to unauthorized access and potential breaches.

If real production data is used in testing, it increases the likelihood of exposure, whether it's through accidental disclosure, inadequate access controls or cyberattacks. These risks highlight the necessity of implementing strong safeguards in adhering to established best practices.

TDSB announced plans to enhance access controls by implementing multi-factor authentication (MFA) and removing production data from all test environments. These security measures ensure that unauthorized users cannot gain access, even if login credentials are compromised.

Additionally, TDSB has committed to strengthening network segmentation to ensure that test environments are properly isolated from production systems. This step will limit the ability of threat actors to move laterally within the network in the event of a breach. With production data no longer being used in the test environment, the risk of a breach involving personal information is mitigated. Based on these remedial measures, I am satisfied that TDSB has taken reasonable steps to prevent future security breaches in its test environment.

To enhance ongoing protection, I recommend that TDSB continually review and update its cybersecurity practices, aligning them with industry best practices and recognized frameworks. Regular cybersecurity awareness training, updated annually, should specifically address threats relevant to test environments and emphasize the importance of maintaining strict separation between test and live data.

Further, I strongly encourage TDSB to regularly consult the following IPC resources to maintain and enhance its cybersecurity posture:

- Privacy Complaint Report MR21-00114.
- Technology Fact Sheet: How to Protect Against Ransomware, which includes cybersecurity industry frameworks and standards.
- Privacy Breaches: Guidelines for Public Sector Organizations.

These combined efforts will significantly enhance TDSB's capability to safeguard personal information.

Thank you for your cooperation in this matter and commitment to ensure compliance with the *Act*. This letter will serve as confirmation that this file is now closed.

Yours truly,

Aaron Heath
Analyst