Audit Committee **17 February 2021**

Report 21-018

Business and Learning Technologies Updates

Key Contact: Shawn Lehman, Superintendent of Instruction, ext. 8391

PURPOSE:

1. This report provides the committee with updates to the work Business and Learning Technologies has undergone to improve the cybersecurity posture for the District.

CONTEXT:

2. In Fall 2019, Business and Learning Technologies embarked on a three year technology plan, Transforming How We Learn and Work, centered around four themes. Attached as Appendix A. These four themes will focus the work of Business and Learning Technologies until 2022. The four themes that are the pillars of the plan include:
    - Modern Learning;
    - Seamless and Innovative Technologies;
    - Privacy and Security; and
    - Digital Transformation.

KEY CONSIDERATIONS:

3. The theme of privacy and security is key to ensuring the staff and students in the District have an understanding of the need to keep data confidential and secure. The desired outcomes in the Technology Plan will be achieved

through a comprehensive cybersecurity framework. This is an overview of the work Business and Learning Technologies has undertaken over the last year in the area of security but is not an exhaustive list of the work being carried out in areas of Privacy and Security.

4. **Security and Identity Team**

In January 2020, Business and Learning Technologies adjusted the organizational structure in the department to place greater emphasis on security and identity. Namely a Security and Identity team headed by a Team Manager to oversee cybersecurity and identity management was recommended. In the Summer of 2020, the Team Manager was hired, and by October 2020 the team was formed which included 7 members to oversee both security and accounts in the department. These members included 3 positions from the area of accounts and 2 positions from the Network and Infrastructure team who had responsibilities for network security. The Team Lead position was added through the 2020/21 budget process.

The team's work plan is grounded in the three year technology plan. It's mission is to "*Provide security leadership, identity governance and management in order to create a culture of privacy and information security in order to safeguard the board's digital assets and information in a cost effective and innovative approach*." In the first year their initial focus will be on:

- Developing and implementing a Security awareness training program for all staff;
- Establishing a Vulnerability Management Framework; and
- Conducting a Security Gap and Maturity Assessment which involves reviewing the current state of gaps and progress towards remediation and map them against an industry standard framework.

5. **Security Awareness Framework**

To achieve our goal of 100% of our staff participating in security and privacy training, our Security and Identity team have developed a Security Awareness Framework comprised of three phases.

Phase 1 - Communicate to staff the expectations and importance of training including timing and cadence.

Phase 2 - Provide role based training to staff to match roles and responsibilities i.e., Finance staff would have specific training regarding awareness of spoofed invoices, phishing etc.

Phase 3 - Security Awareness Testing and monitoring of completion i.e., phishing simulations to test efficacy of the program.

Our goal is to implement phase 1 by the end of June 2021 with Phase 3 being completed by December 2021.

6. **Establishing a Vulnerability Management Framework**

The Security and Identity Team established and implemented a vulnerability framework to run scheduled scans on our network to detect any potential malware or threats that could compromise the District's assets. There are two phases in the framework:

1. Network Discovery; and
2. Vulnerability Assessment.

The network discovery phase is conducted to discover live hosts on the target network. The vulnerability assessment uses data gathered during the first phase to generate a final report. The team then makes recommendations based on the findings in the assessment.

7. **Conducting a Security Gap and Maturity Assessment**

The Security Gap and Maturity Assessment will enable the goals outlined within the Business and Learning Technology Plan to be achieved. By baselining existing capabilities against an industry standard framework we will understand areas for improvement and assess the capabilities (people, process and technology) to support the overall control objective. Ratings will range from Not Implemented to Fully Implemented. Recommendations to be prioritized based on:

- Overall risk;
- Strategic objectives outlined within the Technology Plan; and
- Aligned to target state maturity level.

8. **Email Removal Process**

In November 2020, Business and Learning Technologies reviewed and formalized the process for removal emails from inboxes. The process of removing emails from staff and student inboxes was put in place to mitigate risk to the District. Emails can be removed from the inboxes of staff or students when authorized by designated staff when they meet one of the following criteria:

1. Email content is malicious or poses a threat to the user or the District e.g., phishing attack;
2. Email contains sensitive information that was inadvertently sent to the wrong individuals i.e., confidential student information sent to the wrong individuals;
3. Email content is injurious to the moral tone of the school/District or to the physical or mental well-being of others; or
4. Email that may be libelous or where the further dissemination of the email may expose the District to liability.

Over the past year 81% of the email removals were due to security risk, 16% were due to privacy breaches and 3% were removed because the content was injurious to the moral tone of the District/school or to the physical/well being of others.

9. **Privacy and Security**

Privacy and security have a reciprocal relationship. The Security and Identity Team work collaboratively with the Privacy Officer to ensure we are in alignment with our practices.

10. **Software/Applications Vetting**

With the increase in availability of third party applications for educational use, teachers are being asked to interpret privacy agreements and terms and conditions before sharing student data. This has been a challenge for educators and it is clear they are in need of guidance and support in this area. The District has created a software catalogue committee that is curating, overseeing and recommending applications in schools from a pedagogical, technological and privacy and security perspective. The District has procured the services of an Application Vetting Service through the Educational Computing Network of Ontario (ECNO) to provide consistency to the process as most districts will be using this service. The software catalogue and process for vetting applications has been shared with staff in a variety of ways including a system memo.

11. **Operational and Security Steering Committee**

In Fall 2019 the Operational Security Committee and the Security Steering Committee were struck to establish governance in the area of cybersecurity for the District. The Operational Security Committee consists of members of Business and Learning Technologies staff as well Risk Management. They discuss issues relating to cybersecurity and make recommendations to the Security Steering Committee. Since that time both committees have made recommendations around password policies, account retention, security awareness training and implementation of a multifactor authentication protocol.

12. **ECNO Partnership**

The Educational Computing Network of Ontario (ECNO) offers Shared Services to school boards across Ontario. The services of a Regional Information Security Analyst (RISA) is a service that school boards are able to purchase on a consultative basis. The District has purchased this service which offers us the opportunity to collaborate with other school boards in Eastern Ontario on matters of cybersecurity as well as use the resources developed by the RISA.

RESOURCE IMPLICATIONS:

13. The resources required to carry out this work will be part of the Business and Learning Technologies department budget.

COMMUNICATION/CONSULTATION ISSUES:

14. Ongoing consultation has been occurring with other districts through the Ontario Association of School Business Officials (OASBO), Educational Computing Network of Ontario (ECNO) and the Eastern IT Managers (EOIT). A communication plan will be developed in collaboration with Human Resources on the Security Awareness Training Plan once the timelines have been established. Staff were advised of the software vetting process through a system memo in November 2020.

STRATEGIC LINKS:

15. This work is aligned with a Culture of Caring through championing and nurturing a safe, caring and respectful workplace.

GUIDING QUESTIONS:

16. The following questions are provided to support the discussion of this item by the Committee.
    - Does the report reflect the privacy and security outcomes in Transforming How We Learn and Work?
    - Does the work outlined in the report serve to mitigate the privacy and security challenges that school boards are or may encounter?
    - Does the security awareness framework as noted in the report move the District to a more robust security posture?

_____	_____
Shawn Lehman	Camille Williams-Taylor
Superintendent of Instruction	Director of Education
	Secretary to the Board

Attached: Appendix A - Transforming How We Learn And Work Technology Plan - Fall 2019- Fall 2021