NANAIMO LADYSMITH PUBLIC SCHOOLS
STRATEGIC DIRECTIONS COMMITTEE
PUBLIC MEETING
INFORMATION SHEET

DATE: January 29, 2025
TO: Strategic Directions Committee
FROM: Mark Walsh, Secretary-Treasurer and
Zeyad Merchant, Director of Information Technology
SUBJECT: Updates and Progress on Cybersecurity

Background

This information sheet provides an update on cybersecurity measures being undertaken by the District following the October 2024 Business Committee presentation (attached as Appendix A) on the District's state of cybersecurity risk and the need to continue and accelerate efforts to enhance our threat preparedness, awareness, and response. These updates reflect the District's progress in addressing vulnerabilities and goals highlighted in the October discussion.

Discussion

1. Multi-Factor Authentication (MFA) Implementation

- **Status:** MFA implementation is in its final preparation stages and directly addresses vulnerabilities identified in October, such as the need for stronger authentication mechanisms to reduce account compromises.
- **Testing:** Various MFA methods (authentication apps, SMS codes, phone calls, hardware tokens) and conditional access policies are being tested on different devices and in different scenarios (e.g. on internal vs external networks).
- **Support Resources:** Documentation and support resources are being developed for staff to ensure a smooth transition.
- **Engagement with Stakeholders:** Meetings with HR and labour stakeholders are underway to secure support and inform staff about this critical initiative.
- **Rollout Plan:**
    - IT are the first group to have MFA policies enforced (underway)
    - Following this, enforcement will occur in a phased, site-by-site approach to ensure manageable scaling.
    - District-wide enforcement is scheduled for Spring Break 2025 or shortly thereafter.

2. Incident Response Retainer

- **Partnership:** The District has signed up for an incident response retainer with professional security consulting firms through a master services agreement negotiated by Focused Education.
- **Funding:** The retainer is funded by the BC Digital Services Board. Services consumed in the event of an incident will be borne by the district.
- **Benefits:**
    - Pre-arranged access to expert consultants in case of a major cybersecurity incident.

    - Onboarding ensures the consultants are familiar with district systems, enabling faster and more predictable recovery during incidents.
- **Alignment with October cybersecurity discussion:** This retainer directly addresses the need for improved incident response capabilities, as emphasized in the discussion of operational and reputational risks.

3. DNS Firewall Implementation

- **Service:** The District has subscribed to a DNS firewall service to add an additional layer of protection against known malicious websites from user web browsing while on the district network, as well as from user-browsing off the network from district-issued computers.
- **Activation:** The service will be activated on all district networks by Spring Break 2025.
- **Purpose:** This service will complement the existing Internet security and filtering tools, enhancing the district's ability to protect staff and students from malicious online activities.
- **Direct Response to Risks:** The October report highlighted phishing and malicious websites as key threats. The DNS Firewall addresses these risks by enhancing the prevention of access to such sites.

4. Cybersecurity Awareness Program

- **Launch Plan:** The District will roll out a cybersecurity training and awareness program in 2025. The program selected has consists of content curated for the Canadian K-12 sector.
- **Content:** The program will include:
    - General cybersecurity best practices.
    - K-12-specific scenarios to enhance staff awareness and proactive defense.
- **Alignment with the October cybersecurity discussion:** This program directly tackles the concern over the risk from a lack of cybersecurity awareness and the critical need for a vigilant and informed user population, as highlighted in the October discussion.

5. IT Department Review

- **Objective:** The IT department is conducting a comprehensive review of its structure and capacity to address gaps in expertise and resources related to cybersecurity.
- **Rationale:**
    - Legacy IT systems and processes were designed for a less complex environment. Today's interconnected, cloud-based systems require newer sets of tools, resources, and expertise to manage cybersecurity effectively.
    - The October report identified the increasing sophistication and frequency of attacks as a significant risk. Addressing these risks requires adequately skilled personnel and sufficient resources.
- **Focus Areas:**
    - Proactive cybersecurity measures.
    - Enhanced response capabilities for modern threats.
    - Alignment of tools, resources, and personnel to meet current and future challenges.

Action: The current gaps in in-house expertise and available personnel-hours for cybersecurity planning and operations represent a significant risk area that needs attention and resourcing. Investments in staff and training are critical to closing this gap.

Appendix A: October 2024 Information Sheet