NANAIMO LADYSMITH PUBLIC SCHOOLS
BUSINESS COMMITTEE
PUBLIC MEETING
INFORMATION SHEET

DATE:	October 9, 2024
TO:	Business Committee
FROM:	Zeyad Merchant, Director of Information Technology Mark Walsh, Secretary-Treasurer
SUBJECT:	Confronting Today's Real Challenge of Cybersecurity Risk

Background

October is Cyber Security Awareness Month in Canada. This report is to give the Board a high-level overview of the cybersecurity challenges facing our school district, the current state of the District's defenses, and some of the ongoing and planned work to improve security. The report seeks to shine a light on the need for an increased focus on awareness and actions on cybersecurity.

Discussion

Introduction

Over the last 10-15 years, matters of cybersecurity have moved out from the confines of those directly managing and supporting Information Technology into the main stream. Significant and highly publicized and impactful security breaches began catching the attention of the media and public in the last 5-10 years. These incidents have now become frequent and normalized enough and are now regarded as an expected reality of our digital lives. Today, only the most sensational events attract the attention of the public and then only the attention of the local communities in which they take place. Matters of cybersecurity are no longer of interest to IT leadership, they belong in the forefront of risk management activities of public institutions, private enterprise, governments, law enforcement, and indeed of every end-user of digital technology. If you are using or applying technology today, either in your personal or professional life, you are constantly at a real and increasing risk of a cybersecurity breach that threatens aspects of your life, family, business and well being.

Cyber Risk and the Evolving Threat Landscape

Over 15 years ago, cyber criminals were motivated mainly by the value of stolen military, government or corporate secrets for political gain or for trade advantage, and often simply for the thrill of disrupting electronic operations and/or communications.

Today, cybercrime is a major income generator for organized crime and state sponsors. Any organization or individual holding information of value is a potential victim. A ransomware attack is when a criminal gains access to your or your organization's digital data files, locks your access out, threatens to delete, or worse, publicly release the data, with a ransom demand for its release back to you (extortion).

80 percent of schools across 14 nations were the target of ransomware attacks in 2022. K-12 was the single most targeted industry, edging out higher-education, and surpassing government, construction and healthcare.[1] Why? Schools are data-rich environments. Schools and school districts are uniquely susceptible to pressure to bend to ransom demands and are exceptionally vulnerable from their historic under investment in the security of their digital infrastructure.

Present and Increasing Risks

- Data Breaches: Sensitive data like student records, staff information, and financial data are prime targets.
- Ransomware: Increasingly common in schools, where attackers encrypt data and demand a ransom for its release.
- Phishing: A growing threat through deceptive emails that target staff, students, and administrative systems.
- Denial-of-Service (DoS) Attacks: Disrupting access to critical educational platforms and networks.

With the criminal success of attacks against K-12, the criminals are highly motivated. This is evidenced by:

- The rise in sophistication: Cybercriminals are using more advanced tactics like AI-driven attacks and targeted spear-phishing campaigns.
- The increase in frequency: Cyberattacks on educational institutions have spiked in the last few years, exacerbated by remote learning and hybrid working models.
- Criminals leveraging exposure resulting from broader technology adoption: As technology continues to offer digital solutions to age-old problems, continued pressure for their rapid adoption by school districts often leaves security behind as an afterthought, with criminals taking advantage of the gaps - e.g. with the implementation of IoT ('Internet of Things'). IoT are commonly specialized, Internet-connected devices that often replace older, non-networked technology in modern automation tools for facilities maintenance and operations areas, like HVAC, security and cameras in schools, but that also then leave significant security exposure entry points into the local networks.

What's at Stake for NLPS - Our District's Digital Assets

Today, our district spans almost 40 buildings in which users, devices and storage are connected to each other and to internet. There are currently over 15,000 district-owned devices connected to the network, including iPads, laptops, Chromebook, servers, surveillance cameras, phone systems, HVAC, earthquake and vaping sensors and much more. Each day, an additional 7,000 personal (BYOD) devices also connect to our infrastructure. All of these devices carry, transmit, or store some information of value. In its custody, our district holds the personal and sensitive data of today's 16,000 students and 2,200 staff, that of their families, and a vast collection of financial, payroll and HR data. We host multiple websites and dozens of software programs internally. Additionally, due to data retention policies, we hold data on students and staff from the past. Furthermore, we have rapidly adopted 21st century learning and

[1] https://www.forbes.com/sites/frederickhess/2023/09/20/the-top-target-for-ransomware-its-now-k-12-schools/

productivity platforms with dozens of web-based programs that are hosted in the 'cloud', completely eliminating the access boundaries that our previous district's virtual perimeters confined us to. As the region's largest employer, it isn't much of a stretch to speculate we hold the data of more people in our community than almost any other single organization in the region. This makes us a valuable target.

While most school districts make sound emergency preparations for the physical safety of students and staff, e.g. for natural disasters, etc., very little focus is placed on the impact of a cyber event on operations. Victims of cyber events are usually caught off guard on how reliant they are on technology for everything they do. A significant cybersecurity breach event would most likely take every technology system offline, and there would be a number of associated costs or damages:

- Financial:
    - Ransoms (Extortions): Centre for Internet Security (CIS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), which works closely with US school districts, reported that the average ransom demand for K-12 institutions was **typically between US$100,000 and US$1 million**, depending on the district size and attack severity.[2]
    - Incident Response and Forensics: School districts often rely on external cybersecurity vendors for response and forensic investigation. These services typically cost **between $5,000 to $25,000 daily.**
    - Remediation and Infrastructure Hardening: Post-attack remediation often includes system upgrades and hardening, **which could cost $10,000 to $25,000 daily for several days or weeks** as systems are brought back online with enhanced security measures.
    - Downtime and Lost Learning Time: The cost of downtime, especially during school hours, can be significant. Daily costs for K-12 schools could range from **$5,000 to $50,000** for disruptions in learning, teacher productivity, and administrative functions.
    - Communication and Public Relations: Addressing public relations and stakeholder communication often involves specialized teams, **costing $2,000 to $10,000 daily**.
    - The IBM Cost of a Data Breach Report 2024 reported that the average cost of a data breach globally reached **US$4.88 million**, a new record high.[3]
- Disruption to Learning Continuity, affecting students' education and access to critical resources.
- Disruption to families/community/communications.
- Lasting impacts from identity theft and the exposure of private and sensitive info potentially released to the public.
- Disruption to Operations/Administration.
- Impact to the District's reputation in the local and wider community.
- Sanctions from failing to meet FIPPA obligations: FIPPA requires a public body to provide appropriate and reasonable physical and procedural security measures to protect personal information in its custody or under its control by preventing unauthorized access to personal information in its custody or control both from within and outside the public body.

[2] https://www.cisecurity.org/ms-isac

[3] https://www.ibm.com/reports/data-breach

Current State of Cybersecurity in the District [and recent improvements]

The District's digital assets are managed and supported by the IT department with a constant security-forward approach. This culture has been developed more from a collective sense of professional care than from a requirement to comply with cybersecurity standards (there are no such compliance standards that apply today for BC School Districts). These are some examples of worthwhile security practices and proactive defense measures currently in place [recent initiatives highlighted]:

- Latest generation firewalls at every district site with advanced filtering to minimize malware threats attempting to cross into our trusted networks designed for appropriate separation of network traffic (e.g. separating BYOD traffic from internal, trusted networks). [recent reviews and security enhancements made in 2023/24].
- Replacement of end-of-life network equipment at all district sites (a security risk) with new, supported gear and threat reporting and protection capability [ongoing, through NLPS Data Infrastructure Upgrade Project].
- Endpoint security (antimalware and other device protection on devices) [recently upgraded].
- Regular updating and software patching of all our managed devices.
- Controls placed on end-user devices to minimize unauthorized or malicious software installation or system reconfigurations.
- Local data and server backup and restore procedures [recent improvements to resiliency].
- Shared resources locked down to authorized users.
- Adherence to Role Based Access Controls (RBAC) where users (staff, students, contractors) are only given access to systems and files they are authorized to by way of their job title and/or assignment – we strive to apply the Principle of Least Privilege, where a user is given the minimum level of access they need to perform their job duties [work underway to tighten this up further].
- Antimalware and anti-phishing policies and configurations on email systems [recent enhancements added].
- [New mandatory Privacy Impact Assessment practices for any new initiative and program – includes security]
- Cybersecurity awareness, 'Spot the Scam' campaign targeting all staff via email, newsletters and posters.

Next Critical Steps

The most first step today is to bring the awareness and responsibility for the significant threats and risks of Cybersecurity incidents out from the exclusive domain of the IT Department and into each and everyone's portfolio of responsibilities, as a necessary part of living and working in and around technology. Effectively keeping our students, staff, community and assets safe from these real threats starts with Board and Executive sponsorship, support and participation in a district cybersecurity plan and roadmap.

Developing a formal Cybersecurity Plan will be a priority for IT and the District, and a necessary one to ensure we are committing the necessary resources and effort towards measurable and meaningful improvements in our security posture and therefore our ability to fend off -and respond to- cyber events. An established security framework relevant to our sector and region, will be selected to inform our plan

and guide our efforts in the proven most effective ways. The plan will articulate objectives, goals and action items based on objective and ongoing assessments of our strengths, risks and gaps.

Despite the proactive security measures taken thus far, as well as some reactive measures taken in the past in response to previous (relatively minor) cyber attacks in our district, we are keenly aware of some lucrative opportunities that exist today that we will want to tackle immediately.

One of these opportunities is a district-wide roll-out of Multi Factor Authentication (MFA). MFA is now considered a must-have as a basic security control and requires the necessary stakeholder support and change management to carry out.

Another opportunity for quick wins is a launch of a comprehensive cybersecurity awareness and training campaign for all users of technology. Today's sophisticated and well-crafted attacks often target unsuspecting staff possessing a lower level of cybersecurity awareness. An aware and vigilant user population is one of our best defenses against cyber attacks.

As we make the necessary shift to a formalized security-informed approach to managing the digital environment through the development and implementation of a cybersecurity plan, the District will monitor and assess the org/staffing chart to ensure it aligns with today's cybersecurity needs.

Conclusion

This report is to convey, during this Cyber Month, the urgency of the evolving and increasing cyber threat landscape while also justifying the need for increased focus, support and yes, an investment in new and continued cybersecurity resources for the District. Given our close calls and the real instances of serious cyber events in our neighbouring districts demonstrate the clear value of a commitment to a long-term cost savings strategy through proactive investments and attention on cybersecurity as an avoidance to costly data breaches, ransomware payouts, and system and operational downtime. It is critically important to take the preventative approach and build a resilient security culture that acknowledges that cybersecurity is not just an IT issue but requires district-wide commitment, from leadership to staff and students, as well as a technically sound and supported plan to make us well-prepared for the present and future cyber challenges.