Protecting Schools from Cyberthreats

Ottawa-Carleton
District School Board

THE ISSUE

School boards have a legal and ethical obligation to protect private student and employee data and financial systems. Provincial funding to safeguard this vital data is not keeping pace with the growing cyberthreat.

The rising cost of cybersecurity has been well documented in recent years. For Ontario school districts, cyberthreats and incidents have become more sophisticated and prevalent.

The rise in cost for school districts in Ontario to maintain secure and functional technology systems is not just limited to initial investments in security measures. School districts must also allocate resources to address and prevent potential cybersecurity incidents. This can include upgrading technology infrastructure, conducting regular security assessments to identify vulnerabilities, recruiting and training staff to detect and prevent cyber threats, investing in incident response plans, hiring third-party security experts to assist in investigations, and covering the cost of any downtime during the recovery process.

School boards have an obligation to take appropriate measures to protect confidential and sensitive student and employee data and financial systems. The cost of a cyber attack can be substantial. In addition to data loss and privacy implications, the costs include financial loss, as well as learning loss while systems are down, and damage to the district's reputation and the trust of students and their families. As such, school boards must continuously allocate resources towards cyber security to stay ahead of evolving threats. Moreover, with the increase in the number of cybersecurity related attacks across the sector, insurance policies are becoming more expensive.

It is essential that the provincial budget recognize the importance of proper funding of school districts and other public sector organizations to protect against cyberattacks.

$1.4M+

The amount the OCDSB currently spends for monitoring software and security staff to monitor the network and ensure we maintain an environment that is secure from cyberthreats.

RECOMMENDATIONS

In response to this growing threat, the OCDSB recommends:

1. Increased funding specifically directed to support school districts in strengthening and protecting technological infrastructure against cyberattacks.
2. Provincial taskforce and strategy to address growing threat of cyberattacks on educational institutions.

LAST UPDATED: February 2024

MORE INFORMATION

Cybersecurity is much more than an IT issue. School boards are responsible for safeguarding a wide range of important data, including student academic records, personal details, medical information, financial records and employee data. Recent cyberattacks targetting school boards in Ontario have put the personal information of thousands of students, parents/ caregivers and staff at risk.

From a student learning and well-being perspective, it's important to underscore the pivotal role of fostering digital citizenship and maintaining a strong cybersecurity infrastructure to mitigate cyberbullying. Cybersecurity tools are essential to ensure safe online activities, prevent malicious acts and attacks, and investigate and respond to incidents of cyberbullying. Practical security measures, such as fortifying passwords and enabling two-factor authentication, reinforces these practices on social media and email platforms, and act as frontline defences, thwarting unauthorized access to accounts and preventing the dissemination of harmful content.

Responding to an attack requires considerable costs to restore systems and possibly recover stolen data. This may include third party technical consultants and legal experts. Shutting down information systems may lead to further indirect costs and complications at the district and school level.

The OCDSB has in place a policy concerning information technology security. This is underlined by the guiding principle that strong, reliable, and secure information technology infrastructure is essential to ensuring an effective working and learning environment. A secure infrastructure includes effective long-term contingency and incident management planning to prevent, manage and quickly recover from a security threat or any incident and reduce risk to the organization.

We work to ensure all users of the District network are responsible for its safety and security. In addition, students are taught best practices regarding the appropriate use of technology and safeguarding personal information.

In recent years, there have been more school boards in North America targetted with cyberattacks.

Research cited by Gartner in 2022 notes that when a business is attacked:

24 days

average days of business interruption

61%

average amount of data recovered

4%

of organizations recovered all data.