

Cyber Risk

School for New Trustees
January 2025



Session Description

This session will review the report developed by the 2023 Cyber Risk Working Advisory Group, focusing on governance and risk management of cyber vulnerabilities commonly faced by school divisions.

Cyber Risk and the School Division

- Potential threats and vulnerabilities that can compromise the confidentiality, integrity, and availability of digital systems and data within educational institutions.
- Schools rely heavily on technology for teaching, learning, and administrative operations, and they face risks such as data breaches, ransomware attacks, and phishing scams. These threats can expose sensitive information about students, staff, and finances, disrupt educational activities, business activities and incur significant costs.
- Addressing Cyber Risk requires school divisions to adopt proactive measures, including robust cybersecurity policies, staff training, secure network infrastructure, and regular risk assessments, to safeguard their digital environments.

Background and Challenge

- Background
- Deliverables
- Committee representatives

Background

- In 2021 multiple conversations were begun with school division leadership amongst the SSBA membership on the topic of cyber risk in education.
- In that same year 2021, the GIP unsuccessfully searched for group purchase options for cyber insurance and several school divisions then purchased individual policies.
- The 2021 SSBA Comprehensive Services Survey conducted by the SSBA Executive called for the development of new supports for cyber security insurance services.

Challenge

- All SSBA member Boards acknowledge their cyber security risk. The early risk responses were generally to mitigate at a division level with technology and / or transference to the insurance market.
- Over the past several years and going forward, this risk is increasing in both likelihood and impact for all school divisions.
- In general, data and security breaches in our world are becoming more frequent and more destructive.
- School divisions have not been immune to breaches, and we have seen several within Saskatchewan over the past three years.

Deliverable

- In March 2022 the SSBA Executive approved the organization of a Cyber Risk Working Advisory Group to
 - identify and assess Cyber Risk as it pertains to school divisions, and
 - research and recommend a Cyber Risk mitigation strategy to the SSBA membership.

Engagement Strategy

- Representative WAG developed 2022
 - key decision makers
- 3 meetings 2022 - 2023
 - Roundtable Discussions
 - Consultant Presentations
 - Commercial Presentations
- Development of recommendation January 2024

Governance / Board Role

What is the role of the Board in the area of cyber risk management?

- The Board has ultimate responsibility for risk in the school division.
- The role of the Board is to provide governance oversight of the Enterprise Risk Management program, which will include strategies for the management of cyber risks.
- Understand the risk and how it impacts the achievement of your strategic objectives.

Risk Identification and Assessment

Cyber Risk is not an IT risk, it is an Enterprise Risk

Risks / Vulnerabilities:

- Organizational Culture
- Resourcing: Financial / Human
- Technology and Process
- Access to Breach Response

Organizational Culture Risk

- Social engineering is the most prevalent and successful attack method
- This involves tricking employees into granting access or providing credentials that allow attackers to infiltrate systems.

Resourcing Risk

- Resourcing for cyber security protections and tools was rated as the second highest cyber risk vulnerability for a school division.
- Under-resourcing human resource, professional development and technology budgets creates this vulnerability, including talent retention in a fiercely competitive industry.

Technology and Process Risk

- The Technology and Process risk
 - the absence or lack of a common standard in the technologies and processes used to protect against cyber threats.
 - In the current state, school divisions vary widely in their capacity and resources to mitigate Cyber Risk
 - a shared resource model may work better for dealing with the infrequent, but impactful cyber-attack event, prevention of such events is more manageable at a local level.

Access to Breach Response

- Following a cyber incident, poor or no access to breach response resources such as communications or legal support sustains the school division's vulnerability until an adequate response is made.
- These resources generally are not available in-house and is in fact one of the main attractions of cyber risk insurance – to be able to access a “breach coach” for the post-breach journey.

Recommendation to SSBA Executive

- Shared Resources
- Autonomy of School Divisions
- That the SSBA Executive develops a membership-driven, cyber security standing committee to oversee the development, implementation and maintenance of a commercial contract and services provided by a commercial partner. The committee should be supported by a third-party consultant to conduct a Request for Proposal to provide services.

Governance / Board Role Review

What is the role of the Board in the area of Cyber Risk management?

- The Board provides governance oversight of the Enterprise Risk Management program, which should include identification, assessment and mitigation strategies for the management of Cyber Risk.
- Understand the risk and how it impacts the achievement of your strategic objectives.

When your administration says you have Cyber Risk – believe them.

Thank You



www.saskschoolboards.ca