Province releases cyber incident response standard for Ontario school boards

April 20, 2023

The Ontario Ministry of Education has released a draft of its new Cyber Incident Response Standard to establish expectations for the management of cyber incidents that can potentially impact Ontario school boards. This article summarizes the most important elements of this draft standard and offers our thoughts on how school boards should approach this new and important initiative.

The draft standard

The Ministry has been engaging with sectoral stakeholders over the past year. It has now released the draft standard with the express stipulation that it is "aspirational" while in draft. Should the standard be released in a binding form, school boards would have 36 months to comply with mandatory requirements. At that time, the standard would require school boards to implement a cyber incident response plan.

Required content for the plan includes:

- A scope statement.
- Role and responsibility definition.
- An incident classification scheme and severity model, tied to an activation plan.
- Documentation of potential cyber threats as determined through a threat landscape risk assessment.
- A communication plan that addresses stakeholder communications and the means of communicating "out-of-band."
- Requirements for reporting to the Ministry and provincial Cyber Security Division.
- A chain of custody process.
- Playbooks to address specific threats, to be reviewed and updated on a biannual basis.
- A plan for documenting incidents.
- A glossary and certain appendices.
- Details regarding storage, distribution, auditing and updating of the plan.

The Ministry says that the plan should set out phases and workflow based on industry standard models, preferably those published by the National Institute of Standard and Technology or the Centre for Internet Security (CIS) .

School boards must develop their own plans based on the standard's requirements, which are framed generally except for the requirement to classify incidents.

Incidents must be classified as one of four types and rated for severity on a scale from one to four. The incident types (as defined by the Ministry) are as follows:

- **Non-declared cyber incident** – A cyber incident that is simple in nature and can be handled by the board utilizing their standard IT incident management process. These incidents do not have any data loss and do not present a significant probability of compromising business operations.
- **Declared cyber incident** – A cyber incident that presents a significant probability of compromising the availability, integrity or confidentiality of board systems or data. Remediation of these incidents requires more resources or time than accounted for by the board's IT incident management process.
- **Cyber safety incident** – A cyber incident that has an online student safety component. These incidents are generally concerns regarding student safety and well-being that manifest online and are typically handled through the board's safe school process, where board IT may play a supporting role.
- **Security tool generated cyber incident** – If a board is using advanced cyber security incident detect and response capabilities, some cyber incidents may be automatically identified and cyber incident records may be generated by a security tool. These automatically generated incidents can include early indicators of anomalous activity or deviation from pre-established policies in the board's IT environment that usually require timely action to prevent escalation to a declared incident.

The standard requires a board to identify the types of incidents that will lead them to activate their plan. We expect most will link plan activation to the "declared cyber incident" definition.

Along with the standard, the Ministry has provided a template plan, which provides a structure, instructions and example text.

Comment

Public sector cyber incident response is challenging and requires preparation. The Ministry is rightly encouraging school boards to engage in cyber incident response planning, and the draft standard is a good document that identifies all the significant planning issues. Its general framing should also leave boards with ample room to develop plans that are tailored to meet school board-specific interests and best practices.

There has been much discussion about Ministry reporting. The draft standard says that declared cyber incidents should be reported "as an incident occurs and include the date of the incident, threat type, indicators of compromise, potential bad actors, business impact, affected systems, time to containment and time to remediation." In our view, this is suitably flexible and aligned with best practice.

School boards should embrace the Ministry's invitation to planning without delay. However, they should not do so by simply taking the Ministry's template and modifying it

for their use, which will not support cyber readiness. As we often tell our clients, the written incident response plan is best understood as a living document and a means to an end – having a strong understanding within IT and senior management of the most relevant cyber threats, their potential impact, and the means of minimizing the potential impact.

In responding to the draft standard, school board IT departments should pause and consider whether senior management is sufficiently knowledgeable and engaged in cyber security matters. If not, they should use the draft standard to build common understanding and engagement.

The authors would be pleased to assist with that task by briefing school board senior management on current cyber threat and incident response best practice and helping them develop a deep and critical understanding of the incident response practices presented by the Ministry.

By

Daniel J. Michaluk, Eric S. Charleston

Expertise

Cybersecurity, Privacy & Data Protection, Information Technology, Education, Government & Public Sector, School Boards and Independent Schools

---