KOFFMAN KALEF LLP
BUSINESS LAWYERS

MEMORANDUM

TO: British Columbia Association of School Business Officials

FROM: Koffman Kalef LLP

RE: Cyber-Attacks

DATE: May 21, 2026

1. Introduction

This memorandum discusses cyber attacks in the context of school boards and the legal responsibilities relating thereto, with particular focus on obligations under the *Freedom of Information and Protection of Privacy Act* (the "**Act**").

One of the main purposes of the Act is to protect personal information from unauthorized collection, use, or disclosure by public bodies. As part of this purpose, the Act imposes certain obligations on public bodies in the context of a privacy breach, including certain notification obligations, which may be applicable if there was a cyber attack. These notification obligations were added to the Act fairly recently, in 2023.

2. Has there been a "privacy breach"

In the context of a cyber attack on a school board, the first question to ask is whether there has been a privacy breach, which would trigger notification pursuant to the Act.

The Act defines “privacy breach” in Section 36.3(1) very broadly, as the theft or loss, or the collection, use or disclosure that is not authorized by the Act, of personal information in the custody or under the control of a public body.

As the definition of "privacy breach" includes personal information in a school board's custody or under its control, this would include information held directly by a school board, as well as personal information held by a service provider on behalf of the school board. So a privacy breach could occur even where the school board is not the party that is subject to the cyber attack. As a result, all contracts with service providers which involve personal information should include appropriate language regarding privacy breaches, including an obligation on the service provider to notify the school board of the breach so the school board can ensure it is performing its obligations under the Act.

3. Is notification required

Just because personal information is exposed as part of a cyber attack, does not necessarily trigger a notification obligation. An obligation to notify is only triggered if there is a privacy breach involving personal information that could reasonably be expected to result in significant harm to an individual.

“significant harm” is very broadly defined in section 36.3(2) of the Act, including identity theft, significant bodily harm, significant humiliation, significant damage to reputation or relationships, significant loss of employment, business or professional opportunities, significant financial loss, significant negative impact on a credit record, and significant damage to, or loss of, property.

This is not an exhaustive list, so there may be other situations that trigger notification other than what is listed in the Act itself.

The BC government has published guidelines, which are helpful in determining whether significant harm has occurred. This will be a contextual analysis in each case, considering the sensitivity of the information, the amount of information disclosed, the types of individuals whose information was exposed, the type of person who obtained the information, or if there is a possibility that the information would be used for malicious purposes. If the person who obtained the information is unknown, which likely would be the case in a cyber attack, then this may increase the argument for notification.

Also a school board should take into consideration its ability to contain the breach. The guidelines provide the example of a misdirected email (where the school board could ask the recipient to delete and confirm deletion), which would be very different than a cyber attack, where the information may be hard to contain as you are dealing with a third party who is actively trying to acquire the information.

Notification is not required when it could reasonably be expected to result in immediate and grave harm to the individual’s safety or physical or mental health or threaten another individual’s safety or physical or mental health. So there is a cost benefit analysis component to the requirements.

4. Who must be notified and how

If a privacy breach is reasonably expected to result in significant harm to an individual, section 36.3 of the Act requires public bodies to notify the affected individual and the Information and Privacy Commissioner (the "**Commissioner**").

Usually the privacy breach notifications would be provided in writing directly to each affected individual, and must include prescribed information about the privacy breach. This is set out in section 11.1 of the *Freedom of Information and Protection of Privacy Regulation*, which should include, the name of the public body, the date the breach came to the school board's attention, a description of the personal information involved, contact information, steps take to mitigate the risk, and further steps the individual could take.

In certain cases, indirect privacy breach notifications may be allowed, where the school board does not have up to date contact information, direct notice would unreasonably interfere with the public body's operations or the notification would come to the attention of the public body quicker through public

communication. The school board must have a reasonable belief that this would be the case in order to rely on an indirect notification.

The notification to the Commissioner should be in writing and include certain prescribed information, similar to what is in the notice to the individual.

The notification must be completed “without unreasonable delay”. This time requirement may vary depending on the type of breach. If there are concerns for safety then the notification should be given sooner than if there is not.

5. Notification by employees and officers

Pursuant to section 30.5 of the Act, an employee, officer or director of a public body, or an employee or associate of a service provider, who knows that there has been an unauthorized disclosure of personal information in the custody or under the control of the public body must immediately notify the head of the public body.

6. Privacy offences and penalties

Further, pursuant to Section 65.4 of the Act, failure to notify the head of the public body of an unauthorized disclosure of personal information could result in fines of up to $50,000 for individuals and up to $500,000 for corporations.

So it is important that all unauthorized disclosures of personal information be reported as a matter of course to the head of the public body to avoid liability under the Act, and to ensure that the head of the public body can then make a determination as to whether a privacy breach has occurred.

7. Privacy Management Programs

In addition, as of 2023, pursuant to the Act, each public body must have a privacy management program in place. In the context of a cyber attack, this document can be consulted to determine the process for responding to privacy breaches, so it would be a useful place to look as a first step, or if it is unclear what needs to be done.

The Minister of Citizens' Services has issued a direction to the heads of public bodies, which provides a framework for public bodies on the key components of a privacy management program, which includes:

1. The designation of an individual who is responsible for privacy matters and compliance with the Act;
2. A process for completing and documenting privacy impact assessment and information-sharing agreements;
3. A process for responding to privacy complaints and privacy breaches;
4. Privacy awareness and education for employees;
5. Privacy policies and processes;
6. Methods to ensure that third-party service providers are informed of their privacy obligations; and

7. A process for regularly monitoring and updating the privacy management program.

8. Contractual considerations

In the context of a cyber attack, beyond the scope of the requirements under the Act, the school board will also want to consider any contractual exposure that exists, as well as any contractual notification obligations it may have (for instance, under the confidentiality provisions under any contracts), to ensure that it is fulfilling its contractual obligations. There could also be certain contractual indemnities and remedies available to the school board if the cyber attack occurred through a service provider.

9. Legislation

Privacy management programs

36.2 *The head of a public body must develop a privacy management program for the public body and must do so in accordance with the directions of the minister responsible for this Act.*

Privacy breach notifications

36.3 *(1)In this section, **"privacy breach"** means the theft or loss, or the collection, use or disclosure that is not authorized by this Part, of personal information in the custody or under the control of a public body.*

(2)Subject to subsection (5), if a privacy breach involving personal information in the custody or under the control of a public body occurs, the head of the public body must, without unreasonable delay,

(a)notify an affected individual if the privacy breach could reasonably be expected to result in significant harm to the individual, including identity theft or significant

(i)bodily harm,

(ii)humiliation,

(iii)damage to reputation or relationships,

(iv)loss of employment, business or professional opportunities,

(v)financial loss,

(vi)negative impact on a credit record, or

(vii)damage to, or loss of, property, and

(b)notify the commissioner if the privacy breach could reasonably be expected to result in significant harm referred to in paragraph (a).

(3)The head of a public body is not required to notify an affected individual under subsection (2) if notification could reasonably be expected to

(a)result in immediate and grave harm to the individual's safety or physical or mental health, or

(b)threaten another individual's safety or physical or mental health.

(4)If notified under subsection (2) (b), the commissioner may notify an affected individual.

(5)A notification under subsection (2) (a) or (b) must be made in the prescribed manner.

Notification of unauthorized disclosure

30.5 (1)[Repealed 2021-39-17.]

(2)An employee, officer or director of a public body, or an employee or associate of a service provider, who knows that there has been an unauthorized disclosure of personal information that is in the custody or under the control of the public body must immediately notify the head of the public body.

Privacy offences

65.4 (1)An individual, other than an individual who is a service provider or an employee or associate of a service provider, who wilfully does any of the following commits an offence:

….

(d)fails to notify the head of a public body of unauthorized disclosure as required by Part 3.

(2)A service provider or an employee or associate of a service provider who does any of the following commits an offence:

…..

(d)fails to notify the head of a public body of unauthorized disclosure as required by Part 3;

Penalties

65.6 (1)A person who commits an offence under section 65.2 is liable on conviction to a fine of up to $50 000.

(2)A person who commits an offence under section 65.3 or 65.4 is liable on conviction,

(a)in the case of an individual, other than an individual who is a service provider, to a fine of up to $50 000,

(b)subject to paragraph (c), in the case of a service provider, including a partnership that or an individual who is a service provider, to a fine of up to $50 000, and

(c)in the case of a corporation, to a fine of up to $500 000.