# The transparency imperative: Challenges of public sector cyber incident response

**November 17, 2022**

Public sector cyber incident response has unique challenges that counsel and client must appreciate. To demonstrate this point, we presented the following scenario at the Law Society of Ontario's recent Ontario Digital Evidence and eDiscovery Institute.

*You are on day five of an incident as counsel to an Ontario public school board. The Board has been holding off inquires by staff and students with a communication that* refers to a "network disruption." The Board does not know the details of what occurred, *although the Chair of the Board of Trustees has been briefed informally briefed. The threat actor, the Karakurt group, just presented a 500,000+ line file tree with employee data going back 15 years and a hodgepodge of student data, including psycho-*educational reports and individual education plans. They've given the Board five days to pay up or the data will be released on the Karakurt leak site.

Keeping this scenario in mind, here are five reasons why public sector cyber incident response differs from private sector incident response and why, even in the absence of any cyber incident reporting obligations, transparency is the strong norm.

## 1) You are subject to the presumptive right of access in freedom of information legislation

Incident visibility drives transparency. In the above scenario, the incident is visible because it has disrupted IT services. This ought to drive the response strategy from time zero.

Visibility, however, is not always the case. As more institutions deploy technologies that provide for a better view of their networks, institutions are detecting network intrusions before threat actors deploy ransomware. Global password resets are often required in these cases, but can be implemented without raising an alarm.

A private sector organization who is not subject to a cyber incident reporting obligation might opt to manage such an incident quietly. This option is narrower for public sector institutions, whose records are presumptively accessible under freedom of information legislation. If a public sector institution opts to remain quiet, it must be prepared to later explain this decision.

### 2) There is an expectation to act consistently with the public trust

Although organizations generally have no legal duty to protect the public at large, public sector institutions are expected to act responsibly and consistently with the public trust. In incident response, this means reporting to law enforcement early and providing law enforcement with evidence to support its fight against cyber crime. It means sharing threat information with peer institutions. It may even mean reporting early to a privacy commissioner, even before there is any proven unauthorized access to personal information and even in the absence of a statutory duty to report.

While a benefit to the public, this is a potential burden on institutions and their response processes. Ideally, counsel should report for the institution and guard the institution's incident response resources. Counsel should also help outside agencies understand that institutional resources are limited, and that supplementary reports will be provided in due course rather than on demand.

### 3) Government may become involved

Even in the absence of a binding directive, government may expect public sector institutions to report cyber incidents and provide periodic updates. This is the case in the Ontario education sectors, for example.

Government reporting is reasonable to expect, but raises the same resource challenges as reporting to law enforcement, peer institutions and other agencies. Government must also be clear about its objectives. Is it there to help? The institution or the public sector as a whole? Or is its interest in engaging with institutions during the response process rooted in holding them accountable? If so, what are the accountabilities?

### 4) Your governors may also be politicians

Elected members of a school board or municipal council have duties similar to that of any board member of a corporation in the private sector, but this does not make reporting to the governing bodies of school boards and municipalities easy. The will of elected governors can be forceful and difficult to predict, so reporting to them requires careful preparation. Particularly clear and confident messaging will minimize the risk of losing the confidence of governors and bearing the burden of lost confidence through the life of the incident.

### 5) Your workforce is highly unionized

Bargaining agents are often key stakeholders in public sector incident response. They have an exclusive right to bring a claim on behalf of their affected members and can grieve swiftly. Unions must be at the top of counsel's stakeholder list in a public sector incident. Regardless of collective agreement obligations, they should be kept apprised and, if possible, kept onside.

## Takeaways

Unfortunately, the public sector continues to be targeted by ransomware actors and other cyber criminals. Funding problems lie close to the root of the problem and must be addressed. In the interim, public sector institutions must hone their cyber response knowledge and spend what time they can on preparation. These efforts should reflect the unique challenges we have outlined in this short article.

If you have any questions about the potential challenges of public sector cyber incident response for counsel and clients, reach out to the authors or key contacts listed below.

By

Daniel J. Michaluk, Marc Vani

Expertise

Cybersecurity, Privacy & Data Protection

---

## BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

**blg.com**

## BLG Offices


**Calgary**

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

**Ottawa**

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

**Vancouver**

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

**Montréal**

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

**Toronto**

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749