INSTITUT C.D. HOWE INSTITUTE
Trusted Policy Intelligence | Conseils de politiques dignes de confiance

Intelligence MEMOS

March 19, 2026

From: Gary Edwards

To: Federal and provincial securities regulators; Treasury Board; Canadian Securities Administrators; self-regulatory organization leaders

Re: PARITY IN CYBERSECURITY PRACTICE FOR REGULATORS AND SELF-REGULATORY ORGANIZATIONS

Regulators and self-regulatory organizations (SROs) set expectations for disclosure, incident management, and stewardship of sensitive information. These bodies also compel data collection and exercise delegated authority.

For that reason, there is a strong case for codifying and publicly articulating cybersecurity and privacy practices for regulators and SROs that reflect the transparency and governance expectations they apply to regulated entities. Consistent practice can improve clarity, provide predictability for institutions, and reinforce confidence in supervisory frameworks.

This alignment matters most when incidents occur. Today, authority-to-authority reporting in Canada is generally well defined (dealer members need to report to their SRO within three and 30 days; federal institutions report material privacy breaches to privacy and treasury authorities within seven days of determining materiality). By contrast, there is no uniform cross-sector baseline prescribing the cadence and minimum content of public notices by regulators and SROs, nor a consistent expectation for independent assurance following material incidents.

A short public-facing baseline would clarify expectations while respecting existing legal frameworks. It would also clarify an important distinction: In parts of the public sector, breach-management expectations are formalized for government institutions yet comparable public-facing expectations are not applied consistently across regulators and SROs that compel sensitive information and set standards for others.

Some recent examples illustrate the challenges with public disclosure practices and constructive steps to improve incident transparency. In 2025-26, the Canadian Investment Regulatory Organization (CIRO) disclosed a cybersecurity breach in stages, with public communications unfolding over several months. Initial notices focused on operational continuity and the possibility that personal information had been affected. Later updates confirmed impacts to registration information for member firms and registered individuals, and subsequent disclosure indicated that many investors were also affected. Although this example not an assessment of the adequacy of CIRO's response, which available information suggests was robust, the sequence of public communications illustrates the challenge: Expectations regarding the cadence, minimum content, or explanatory context for regulators and SROs are not clearly articulated.

Other jurisdictions are doing better. In the United Kingdom, financial supervisors have consulted on standardized operational-incident reporting to improve consistency and timeliness across firms. Separately, the UK Electoral Commission published accessible post-incident materials describing affected systems and data categories. While contexts differ, these examples illustrate practical steps for oversight bodies: Consult on structured reporting requirements and publish clear, plain language post-incident information.

Here are several recommendations that should be part of a broader set of discussions on establishing a public-facing baseline.

1. **Public incident disclosure**. Retain statutory reporting as the floor. Once materiality is confirmed, publish: (i) an initial plain-language notice within 72 hours; (ii) weekly public updates until containment; and (iii) a close-out summary describing root cause, affected data categories (a non-trivial task), and remediation. Define when the clock starts, the minimum facts required at each stage, and where notices will appear. Require notices to state, at minimum, what is known, what is not yet known, what affected individuals should do, and when the next update will be provided. Cybersecurity challenges may cause issues with fixed short-term timelines, and those issues ought to be articulated in regular updates.
2. **Independent assurance**. Following any material incident, commission an external review and publish an executive summary with dated remediation milestones. Ensure the review assesses governance, technical controls, third-party exposure, and incident handling. Require periodic public updates on remediation progress. In addition, publish an annual public attestation that the cybersecurity and privacy program aligns with recognized frameworks (e.g., OSFI Guideline B-13; relevant ISO standards).
3. **Control baseline**. Adopt the Canadian Centre for Cyber Security control sets as a minimum. Publish a small set of practical indicators that reflect implementation and resilience, such as privileged-access management and logging, network segmentation and identity boundaries, endpoint detection and response coverage, immutable backups and restoration testing, tested recovery times objectives and recovery point objectives, and third-party and supply-chain risk management. This reporting should be simple and comparable year over year. The objective is transparency on control maturity, not operational detail that would increase risk.
4. **Data minimization and retention**. Reduce breach impact by holding less sensitive information for less time. Publish an inventory of compelled data fields, justify each field with reference to regulatory purpose, and encrypt data at rest and in transit. Establish retention periods that are justified by regulatory purpose and minimize long-term exposure. Where feasible, use tokenization, pseudonymization, and segregation of high-risk data sets.
5. **Coordination**. Align the baseline with the federal critical-cyber-systems framework as it advances and with provincial privacy regimes to promote consistency of terminology and expectation. Use consistent terminology for materiality, affected data categories, notification triggers, and public update cadence. The goal is not duplication, but harmonized expectations and clearer public communication.
6. **No-fault incident learning mechanism**. As an optional enhancement, Canada could establish a no-fault cyber incident review board as a post-incident learning mechanism, similar in concept to models used in other jurisdictions, such as the US Cyber Safety Review Board. Its role would be to publish anonymized, cross-case lessons derived from independent reviews without assigning blame or imposing sanctions. This would support continuous improvement.

Treasury Board should issue guidance for federal regulators and Crown entities that codifies the commitments outlined above.

The Canadian Securities Administrators should require self-regulatory organizations and securities commissions to publish annual cyber and privacy attestations and to meet explicit public-disclosure timelines for material incidents.

The Canadian Centre for Cyber Security should maintain the control baseline, develop sector profiles, and manage an anonymized lessons-learned repository drawing on findings from independent reviews. If adopted, a no-fault cyber incident review board could support this work.

Aligning regulator and SRO practices this way can strengthen trust, improve predictability, and support learning after incidents. A short, uniform public-facing baseline, paired with independent assurance and optional cross-case learning, offers a practical approach that complements existing reporting and can be adapted across sectors.

Gary Edwards is Co-Founder and Principal of Golfdale Consulting, and an advisor to the Cyber Security Global Alliance.

*To send a comment or leave feedback, click **here**.*