Cyber Incident Response Plan – The Role of Legal Counsel

By Peter Ciechanowski, John Sanche & Mardi McNaughton

In January 2026, the Canadian Centre for Cyber Security released its report assessing the ransomware threat to Canada (the **Report**).[1] The Report highlighted, among other things, that ransomware events in Canada are increasing and will remain a significant threat in the next two years, particularly by threat actors leveraging advancements in artificial intelligence (**AI**).

Legacy information technology (**IT**) and operational technology (**OT**) systems and supply chain dependencies are attractive targets for cyberattacks, and such vulnerabilities remain a top concern within the energy sector. While critical infrastructure and large corporations continue to be prime targets for ransomware threats, no organization is immune to cyber incidents.[2]

The following provides a brief overview of some ways legal counsel serve an integral role for an organization that is preparing for and responding to cyber incidents.

1. Preparing for cyber threat readiness

As explained in our previous article ***What Is an Incident Response Plan and Why Every Business Should Have One***, legal counsel can assist with preparing an incident response plan (**IRP**) and, among other things, conduct tabletop exercises to stress test the IRP under various scenarios. In addition to preparing an IRP, legal counsel can review the organization's contractual and governance documents to ensure compliance with applicable data privacy laws. This review also enables the identification of any regulatory bodies that must be notified in the event of a cyber incident.

2. Establishing Legal privilege

Involving legal counsel in overseeing and implementing protocols during a cyber incident response will facilitate a strong presumption that solicitor-client and/or litigation privilege apply over various types of information.

Solicitor-client privilege protects confidential communications exchanged between a lawyer and client for the purpose of obtaining legal advice. Protection of communications can also extend to vendors retained by legal counsel, such as forensic and crisis management firms, which is useful in protecting reports prepared for legal counsel to assist with providing advice to the organization.

---

[1] CCCS, *Ransomware Threat Outlook 2025 to 2027: An Assessment of the Evolving Ransomware Threat to Canda* (28 January 2026) [***Ransomware Threat Outlook***].
[2] *Ransomware Threat Outlook*, page 10.

Litigation privilege protects communications and documents that are prepared with the dominant purpose of existing or anticipated litigation. If there is a reasonable prospect of litigation (such as contractual disputes, regulatory investigations or class actions), legal counsel can ensure the proper collection and preservation of evidence and implement procedures to help establish a *prima facie* case that litigation privilege applies to such documents.

3. Managing Communications and Notifications to Third Parties

As details are obtained on the type and extent of information that has been compromised as a result of a cyber incident, legal counsel can determine whether any regulatory or contractual requirements are triggered to notify the relevant affected parties. Legal counsel can assist with preparing notices to those third parties and ensure that language does not unnecessarily admit liability. Legal counsel can also assess whether any contractual arrangements with commercial parties may expose the organization to further liabilities.

4. Notifying Regulators and Handling Regulatory Investigations

If the organization collects personal information in the course of its commercial activities a cyber incident may require notifying one or more regulators of the incident. Such notification requirements may be triggered under Canada's *Personal Information Protection and Electronic Documents Act* or Alberta's *Personal Information Protection Act*. Once notified, a regulator may further investigate the circumstances of the cyber incident and may order penalties.

Organizations that conduct commercial activities in certain industry sectors may also have additional notification requirements to those regulators of that specific industry. Federally regulated financial institutions, for instance, must report any material technological or cybersecurity incidents to the Office of the Superintendent of Financial Institutions within 24 hours of the incident. Similarly, organizations that are custodians of personal health information are subject to Alberta's *Health Information Act* and in the event of a cyber incident, may be required to notify affected individuals, the Office of the Information and Privacy Commissioner and the Minister of Health. For cyber incidents that compromise the personal information of persons residing outside of Alberta, applicable regulatory and notification requirements in those jurisdictions must be considered as well.

5. Managing Post-Incident Review and Potential Litigation

After an organization's affected systems are restored, legal counsel can assist with lessons learned from the response to the cyber incident by updating the organization's cyber policies, training and revisiting the IRP. Legal counsel can also assist with assessing and managing the organization's exposure to potential litigation from affected persons or commercial parties.

Conclusion

Organizations in Canada, particularly those in the energy sector, are faced with an increasing threat to their IT and OT systems. Threat actors are also taking advantage of new technologies, such as AI, to implement innovative ways to target organizations. Legal counsel can form an integral part to an organization's resilience to cyberattacks and mitigate legal risks by providing guidance and implementing best practices before, during and after a cyber incident.

If you have questions or would like assistance, please reach out to any member of our **Cybersecurity team**.