New Cybersecurity Regulations Coming Soon: What you Need to Know

By John Sanche, Chelsea Nimmo, Mardi McNaughton & Sadhna Mathrani

On May 31, 2025, the Government of Alberta's ***Security Management for Critical Infrastructure Regulation*** (the **Regulation**),[1] under the ***Responsible Energy Development Act*** (the **Act**),[2] will come into force.[3] The Regulation targets "critical" facilities in the province, such as pipelines and processing plants. A key goal of the Regulation is the prevention and management of cybersecurity attacks on critical infrastructure. These attacks are on the rise and can have devastating consequences on businesses, such as the temporary shutdown of critical services, which can cost millions of dollars. Below, we outline what you need to know about the upcoming Regulation.

Which facilities does the Regulation apply to?

The Regulation will apply to "critical" facilities as categorized by the Alberta Energy Regulator (**AER**). The AER will be responsible for determining whether a facility qualifies as a "critical facility", and in doing so, it will consider numerous factors, including the size of the facility, its proximity to people, and how it interacts with other infrastructure.[4] The AER will be required to maintain a list of critical facilities – the "critical infrastructure list" – and will be required to inform those whose facilities are on the list.[5] The critical infrastructure list will be confidential.[6]

What does the Regulation require?

The Regulation will require all critical facilities to have both security and cybersecurity measures in place that accord with CSA Z246.1 (the **CSA Standard**) – a Canadian standard related to security management for petroleum and natural gas industry systems.[7] The CSA Standard sets out general requirements for organizations (e.g. creating security incident management programs), but provides organization with some discretion in certain areas to consider which software and cybersecurity practices make the most sense for their business. Generally speaking, the CSA Standard uses "security" and "cybersecurity" interchangeably, but organizations should note that there may be both physical and non-physical elements to their cybersecurity. For example, organizations may be required to have certain technology and infrastructure in place (physical elements), while also maintaining specific data protection software on their electronic devices (non-physical elements). These components all work in tandem to bolster an organization's cybersecurity.

The CSA Standard requires organizations to:

- develop a security incident management program that addresses how operators will acknowledge security threats, respond to them, and report them;[8]

---

[1] *Security Management for Critical Infrastructure Regulation*, Alta Reg 84/2024 [**Regulation**].
[2] *Responsible Energy Development Act*, SA 2012, c R-17.3 [**Act**].
[3] Regulation at s 6.
[4] Regulation at s 2(2).
[5] Regulation at ss 2(1) and 2(3).
[6] Regulation at s 2(4).
[7] Regulation at s 3(1).
[8] CSA Group, "Security management for petroleum and natural gas industry standards" (February 2021) online (pdf): <CSA Z246.1:21 | Product | CSA Group> at s 10.2.

- name individuals who are responsible for, and trained in, security management governance;[9] and

- document decisions made in respect of the implementation of cybersecurity measures, and to consider whether various cybersecurity-related procedures and processes should be implemented.[10]

What are the powers of the AER under the Regulation?

The AER will have the power to require a licensee to file with the AER all or specified information in relation to the security management of a critical facility, and to audit security management programs.[11] If the AER finds that a critical facility has not established a proper security management program, it may order that one be established, or, in some cases, it may order the shut down of a critical facility.[12]

What can organizations do to prepare?

If you expect to be added to the AER's critical infrastructure list, some suggestions on how to prepare are:

- **Review cybersecurity protocols**: Organizations should review their policies, including any IT-related policies, to assess whether they comply with the CSA Standard. This includes developing an incident response plan so that your organization can contain and address a potential cybersecurity breach quickly. An incident response plan should be made with input from both Information Technology (**IT**) and Operational Technology (**OT**) personnel. It should include a checklist of how to identify a breach early on, what steps should be taken in a cybersecurity breach, who is responsible for each step, and where to access corresponding information. These plans should be shared organization-wide to ensure all personnel are alert to potential threats and can respond quickly and effectively.

- **Establish an approach that starts from the organization's C-Suite**: Organizations should ensure that management emphasizes the need for strong cybersecurity policies and processes. There is currently a gap in many energy industry organizations between IT and OT teams. Cyber attackers are aware of this and often leverage this gap to carry out attacks on organizations. As such, it is recommended that IT and OT personnel work together to integrate their systems to strengthen cyber protection.

For assistance on navigating the Regulation, the CSA Standard or cybersecurity generally, feel free to contact any of the authors.

[9] CSA Group, "Security management for petroleum and natural gas industry standards" (February 2021) online (pdf): <CSA Z246.1:21 | Product | CSA Group> at s 4.2.
[10] CSA Group, "Security management for petroleum and natural gas industry standards" (February 2021) online (pdf): <CSA Z246.1:21 | Product | CSA Group> at s 7.2.1 & 7.2.2.
[11] Regulation at ss 3(3) and 3(5).
[12] Regulation at s 3(2).