CSE report stresses cyber threat to Canada's energy sector

November 27, 2020

Pursuant to the Ontario Energy Board's Ontario Cyber Security Framework (see our analysis of the framework), electricity utilities are required to perform an Inherent Risk Profile Tool and a related Self-Assessment Questionnaire.

But keeping up with cybersecurity developments can be challenging.

Below we highlight two threats recently identified by the Communications Security Establishment in its national threat assessment report, along with other relevant publications and developments.

The CSE report

The Communications Security Establishment is Canada's signals intelligence agency. On November 18 it published its second national threat assessment report, which sets out general expectations about the Canadian cyber threat landscape over the next two years.

The value in the CSE report is that it is forward-looking, and published by an organization well-suited to make predictive judgements about cyber threats. The CSE cites exclusively public sources of information, but, as it makes clear, its judgement is based on public and classified information.

The CSE highlights two threats to the energy sector:

Ransomware

The CSE identifies critical infrastructure as a key target for threat actors using ransomware: "We assess that ransomware directed against Canada in the next two years will almost certainly continue to target large enterprises and critical infrastructure providers," the report states. It also believes that increased targeting of poorly segmented industrial control systems is likely in the next two years, as threat actors "attempt to place increased pressure on critical infrastructure and heavy industry victims to promptly accede to ransom demands."

State sponsored intelligence gathering

Although the CSE makes clear that it does not anticipate nation state attacks targeting operational technology in the absence of international hostilities, it nonetheless judges such attacks as the most pressing threat to the physical safety of Canadians. In doing so, the CSE refers specifically to operational technology used to control "dam openings, boiler activities, electricity conduction, and pipeline operations." And while physical safety risks are currently remote, the CSE says, "Nevertheless, cyber threat actors may target critical Canadian organizations to collect information, pre-position for future activities, or as a form of intimidation."

Other recent publications and developments

Regulators outside Canada have recently released three reports on major cybersecurity incents.

- On October 15, the New York Department of Financial Services issued a report on the compromise of Twitter's account management system that occurred earlier this year. The DFS report is a highly relevant resource on controlling the risks of remote access and remote work. For example, the DFS comments on the varying quality of different means of multi-factor authentication, reflective of a warning recently issued by Microsoft.
- On October 30, the (UK) Information Commissioner's Office issued a report on a major hospitality sector incident in which threat actors gained access to a company's systems and undertook significant malicious activity over a two-year period before finally triggering an alert. The ICO makes prescriptions on monitoring and other network layer controls.
- On November 13, the (UK) Information Commissioner's Office issued a report on a major 2018 incident in which threat actors compromised a third-party "chat bot" script to scrape payment card and other data from a company's online payment form. The ICO makes a number of prescriptions about managing supply chain risks, particularly in respect of application development.

Also of note, on November 4, ransomware recovery company Coveware published its quarterly ransomware report. The report includes a significant indication that it is starting to see a "fraying" of threat actor promises to delete stolen data. Holding data for ransom and threatening publication on leak sites has become common in 2020. If one accepts Coveware's report, the payment option is significantly less appealing.

The regulatory environment is also on the verge of major change. The federal government has introduced Bill C-11, which will replace PIPEDA with a new act called the *Consumer Privacy Protection Act* and, in particular, bring in a strict new enforcement regime. The greatest impact will be on local distribution companies. See our comprehensive analysis of Bill C-11 to learn more.

Takeaway

The threats outlined in the CSE report will not be new to some clients. Other clients should consider the CSE input and adjust their processes accordingly. Bill C-11 reinforces the ongoing pressure to be ready for cyber incidents of all kinds. Clients

should view their incident response polices as living documents, ones that are subject to continuous testing and refinement.

We would be pleased to assist with any such matters. Please reach out to your BLG lawyer or any of the key contacts below.

By

Daniel J. Michaluk, John A.D. Vellone

Expertise

Cybersecurity, Privacy & Data Protection, Privacy & Security Breaches, Energy – Power

---

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

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2024 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.