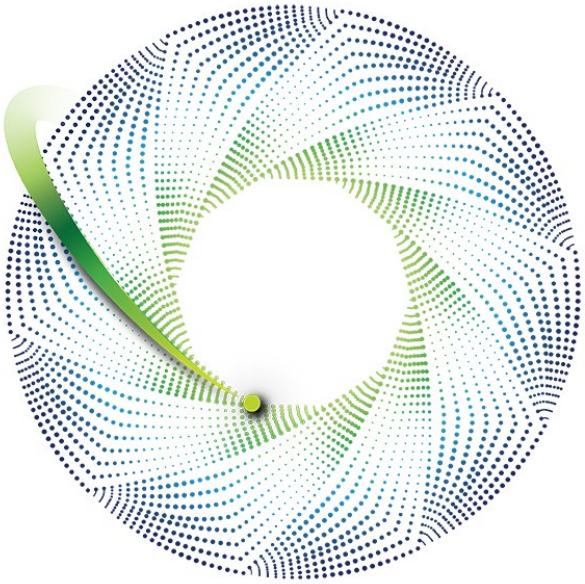
Deloitte.



Canadian Tax & Legal Alert

Cyberthreats in the energy sector and beyond

Why and how your organization should address cybersecurity vulnerabilities

November 3, 2021

Executive summary

As cybercriminals are targeting more diverse data sources, there has been a surge in recent years in the prevalence and destructiveness of cyberattacks in the energy sector worldwide. This article examines the specific legal risks faced by both organizations and directors and officers and outlines a number of recommendations for mitigating such liability.

Key considerations

The energy sector's current cybersecurity environment

Ransomware attacks in this sector have grown in scope and significance, including the recent incident involving Colonial Pipeline Co., which forced the company to pay a ransom of nearly US$5 million in digital currency and, in the interim, shut down nearly 9,000 km of pipelines, causing panic buying at gas stations across the eastern United States. What is more, this incident highlighted just how vulnerable some public and private organizations are, including those in the energy industry, to even basic attacks on computer networks.

While many have speculated about the reasons underlying the increasing prevalence of such attacks, our research as well as our own observations from working with utility companies on similar breach incidents has led us to identify the following factors:

1. An increase in the number of threats as well as threat actors targeting utility companies

A recent assessment performed by the Canadian Centre for Cyber Security (Canadian Cyber Centre) noted that it is not only **cybercriminals** initiating attacks in the energy sector in order to obtain ransom payments, business fraud spoils and intellectual property, but also **nation-state actors** seeking to achieve geopolitical goals and "**hacktivists**" looking to publicize their agendas and/or their opposition to certain utilities' projects.

Many of these threat actors are viewed by government intelligence as highly sophisticated and motivated to target the supply chain and managed service providers for two purposes: (i) to obtain intellectual property and information about the industrial control systems (ICS) of a utility; and (ii) as an indirect route to access the networks of electricity utilities.

The Canadian Cyber Centre also notes that the "likelihood of a cyberattack impacting the Canadian electricity sector is **higher** than it otherwise might be because of the **connections between US and Canadian grids**: cyber threat actors likely view Canada as an intermediate target through which they can impact the US electricity sector, and the increased levels of threat activity against US grids could result in an event that impacts the Canadian electricity sector."

2. The particular vulnerability of electric power and gas companies to cyberattacks

Over the past two years, ransomware attacks with the potential to affect industrial processes have become more frequent in Canada and around the world. Since January 2019, for example, at least seven ransomware variants have contained instructions to terminate ICS processes that would normally run on industrial control workstations.[1]

One potential cause of this increase may be the utilities' ever-expanding attack surface, arising from their geographic and organizational complexity. The largely decentralized nature of such organizations' cybersecurity leadership and the electric power sector's unique interdependencies between physical and cyber infrastructure may also contribute to these companies' particular vulnerability to cyberattacks. Finally, as noted by the Canadian Cyber Centre, cyber threat actors are adapting their activities to new opportunities provided by the transition of companies in the energy sector to smart grid technology.

Examples of such attacks range from the appropriation of operational technology (OT) systems by cybercriminals through the internet to billing fraud via wireless smart meters and physical destruction.

Contacts:

Helene Deschamps Marquis
National data privacy and cybersecurity law practice leader
Partner, Deloitte Legal Canada
Tel.: 514-393-8300

Claire Feltrin
Senior Associate, Data privacy and cybersecurity law practice
Deloitte Legal Canada
Tel.: 416-885-9446

Related links:

Deloitte Tax Services

Deloitte Legal Canada LLP

[1] Andy Greenberg, "Mysterious New Ransomware Targets Industrial Control Systems," *Wired*, February 3, 2020; Nathan Brubaker *et. al.*, "Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families," FireEye Threat Research Blog, July 15, 2020.

Repercussions for organizations and officers/directors

1. Organizations

Under Canada's current federal private sector privacy legislation (the *Personal Information Protection and Electronic Documents Act* or PIPEDA), organizations are required to:

- Report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals;
- Notify affected individuals about those breaches; and
- Keep records of all breaches.

Any organization that knowingly contravenes PIPEDA's reporting, notification, and record-keeping requirements relating to breaches of security safeguards could be subject to fines. Furthermore, proposed amendments to this legislation via Bill C-11, the *Digital Charter Implementation Act* (DCIA), seek to introduce (i) administrative monetary penalties for organizations that contravene the new legislation of up to the greater of $10,000,000 and 3% of the organization's gross global revenue; and (ii) fines of up to the greater of $25,000,000 and 5% of the organization's gross global revenue where organizations *knowingly* commit certain offences under the new regime.

Organizations in the energy sector should also be aware of the North American Electric Reliability Corporation (NERC), which has developed standards relating to cyber security incidents and dictates that security incidents be reported to the NERC within certain prescribed periods of time depending on the particular incident at hand (in addition to any reports made to the Office of the Privacy Commissioner of Canada under PIPEDA).[2] Failure to report such incidents may result in fines and other sanctions. Further, organizations subject to the United States' Transportation Security Administration must abide by stringent requirements relating to the implementation of cybersecurity software updates and patches in the context of security incidents.[3]

Beyond these statutory fines and penalties and the threat posed to national security inherent to energy sector cyberattacks, organizations in the energy sector targeted by cybersecurity incidents face other unique risks, including significant business interruption to critical infrastructure arising from distributed denial of service (DDoS) attacks, reputational risk stemming from post-incident consumer mistrust, and potential class action litigation.

2. Officers and directors

While potential personal liability of officers and directors for cybersecurity failures remains a developing area in Canadian law, it is clear such individuals would be well advised to play an intentional role in cybersecurity risk management to fulfill their obligations to the company.

For instance, directors and officers have statutory as well as Canadian common law obligations to exercise reasonable care and diligence in the operating of the company. They must, for example, proactively identify cybersecurity gaps, regularly address

[2] See NERC standard CIP-008-6, *Cyber security – Incident Reporting and Response Planning*, at page 14.
[3] Pipeline Security Guidelines.

cybersecurity issues at board and related meetings, and ensure that critical security incidents are addressed in a timely manner and disclosed to appropriate individuals. Further, under Canadian federal and provincial privacy legislation, directors and officers can be held liable for regulatory penalties. In Québec, for example, directors and officers who authorize a corporate act or omission which violates privacy law may be named as parties and liable to penalties.

While the scope of civil liability for directors and officers in the context of cybersecurity class actions has not yet been tested, American investor class action litigation provides some hints with respect to the extent to which Canadian officers and directors may eventually face liability when it comes to organizational cybersecurity incidents. In particular, these cases indicate that a company's shareholders may have special statutory remedies against officers and directors (*e.g.*, where such individuals intentionally withhold information about cybersecurity vulnerabilities from the public market or by simply failing to prevent data breaches). Similar statutory remedies currently exist in Canada and proposed amendments to Canada's federal privacy law seek to introduce new penalties and a private right of action following a finding of non-compliance with the law. These amendments, if passed into law, may increase exposure of directors and officers to liability to the extent that they fail to fulfill their responsibilities to address cybersecurity risk.

Deloitte's perspective

How to mitigate liability through a wholistic approach to cybersecurity

In order to proactively combat the ever-increasing cyberthreats in the energy sector, organizations must remain vigilant to cybersecurity risks, ensure appropriate privacy and cybersecurity controls are in place, and take action to remedy any relevant shortcomings. To achieve these goals (and mitigate their own liability), officers and directors in particular should consider taking some of the following steps to mitigate risk and liability when it comes to cybersecurity, and ensuring that:

- Cybersecurity risk is a regular agenda item at board and other meetings;
- Directors and officers are aware of and trained on material cybersecurity risks affecting the organization;
- Directors and officers are asking the right questions to the right stakeholders and hiring external cybersecurity experts, as necessary;
- Directors and officers verify whether the organization has appropriate:
    - cybersecurity controls (people, process, technology);
    - breach response capabilities (playbooks, retainers);
    - personal data processing practices (compliance with privacy laws);
- Major incidents are escalated to the board and that directors have a diligent response strategy that is regularly put to the test (*e.g.*, through crisis simulations).

While electric power and gas companies are especially vulnerable to cyberattacks, a **wholistic** approach to addressing cybersecurity vulnerabilities can **significantly reduce** organizational and officer/director's liability. In order to address the immense legal, geographic, organizational, and technical issues unique to organizations in this sector, a

wholistic, **multidisciplinary**, and **innovative** approach would offer organizations in the energy sector the following tools and advice to guard against and address cyberthreats:

- wholistic cybersecurity maturity assessments to evaluate current cybersecurity maturity, benchmark capabilities against industry peers, and identify opportunities to build a strong cybersecurity operating model;
- incident readiness and preparation (including the development of privacy and cybersecurity policies, incident response plans and protocols, reviewing and negotiating data-related agreements (*e.g.*, data protection addenda, outsourcing agreements, etc.);
- incident response (including acting as a breach coach, coordinating privacy and regulatory notifications/reports, engaging forensic teams, leading post-mortem reviews and recommending privacy/cyber improvement programs, and handling regulatory investigations); and
- legal advice on a variety of other data-related matters (including, but not limited to, privacy and data security assessments and compliance audits, privacy and cybersecurity due diligence in the context of corporate and other transactions, employee privacy training and awareness, data governance, and information consent practices).

How can Deloitte help you?

Our multidisciplinary team of professionals from Deloitte LLP and Deloitte Legal Canada LLP can help you understand the cybersecurity vulnerabilities that may impact your organization and how to address them.

If you have questions on any of the above, please reach out to your Deloitte advisor or any of the individuals noted on this alert.

Deloitte LLP
Bay Adelaide Centre, East Tower
8 Adelaide Street West, Suite 200
Toronto ON M5H 0A9
Canada