FASKEN

BULLETIN

Cybersecurity Risks for Directors and Officers

READING TIME
6 MINUTE READ

Overview

Privacy and Cybersecurity Bulletin

APRIL 26, 2018

Directors and officers in Canada face increased risk of personal liability and threats to job security in relation to cybersecurity. Data breaches and other cybersecurity events often cause companies to suffer staggering costs and losses, severe adverse reputational impacts and third party litigation and liability, among other consequences.

In a growing number of cases, affected stakeholders are seeking to hold directors and officers personally liable and a number of officers have been ousted in the wake of data breaches.[i] In this short bulletin, we highlight a number of key developments and considerations for directors and officers in relation to these matters.

Claims against directors and officers

Directors and officers in Canada generally face limited risk of personal liability. However, they may be liable in scenarios where, for example, they breach their fiduciary duties or their duty to exercise the care, diligence, and skill of a reasonably prudent person in comparable circumstances. Given the complexity that can be associated with the oversight of cybersecurity risks in particular, the lack of clear legal standards in the area, and significant consequences of breaches, the field is ripe for affected stakeholders to test claims that directors and officers have failed to discharge their duties.

In recent years, a number of derivative and securities claims against directors and officers have been brought in the United States in relation to cybersecurity incidents. Plaintiffs typically allege that directors and officers failed to adequately oversee the organization's cybersecurity before a breach and/or failed to appropriately oversee the organization's disclosure, investigation, and remediation efforts after the breach.[ii] While these lawsuits have not advanced for a variety of technical and procedural reasons, such claims are expected to continue, particularly as plaintiffs' counsel learn from their mistakes and find creative new ways to frame their claims.

Canada has not yet witnessed the advent of high-profile lawsuits against directors and officers in relation to cybersecurity, although anecdotally demands have been made in some cases. However, directors and officers should not take comfort that such claims will not be made in Canada and nor should they take comfort that they will be able to invoke the technical and procedural defences that have been successful in the United States in a number of cases to date. Many would consider that it is more likely that similar claims could be more readily advanced in Canada, as compared to the United States. In addition, strict liability may be imposed for breach of a fiduciary duty, which may lead to a successful claim even if a plaintiff is unable to demonstrate compensable damages.

Directors and officers of public companies may also face claims in relation to securities disclosure obligations. Such claims have been advanced in the United States to date. In Canada, the Canadian Securities Administrators ("CSA") expects to see material risk disclosed in a detailed and entity-specific manner.[iii] Directors and officers may be liable for misrepresenting their cybersecurity measures, failing to disclose a material cybersecurity risk, or failing to disclose a material cyber breach in a timely manner. Materiality will depend on the circumstances of the issuer as well as the type of attack and the extent of its consequences. Even relatively minor cyber attacks may be viewed as being material if they are frequent or numerous.

Impact of evolving standards and risks

The discharge of directors' and officers' duties in respect of cybersecurity must be continually reassessed and is evolving along with the changing landscape of standards and risks.

While in the past there has been a relative paucity of concrete guidance in respect of cybersecurity risk oversight, in recent years we have witnessed the emergence of specific guidance for directors and officers[iv], sector-specific directives and initiatives[v], regulatory guidance of general application[vi] and landmark changes in the legal landscape.[vii] Each of these developments would be expected to inform the steps that a reasonably prudent person would take in addressing cybersecurity risk. Directors and officers must ensure that they have regularly updated knowledge not only of the risks faced by their organizations but also of the evolving context in which their actions may be scrutinized.

New privacy regulations in Canada require organizations to: (a) notify individuals about privacy breaches, (b) report privacy breaches to the Office of the Privacy Commissioner of Canada (and others in certain circumstances), and (c) keep certain records of privacy breaches.[viii] These requirements create the potential for increased risk of cybersecurity regulatory investigations and litigation, and in turn increased scrutiny of director and officer actions and potential liability.

With respect to how the evolving threat landscape may influence director and officer risk, it is notable that in at least one action in the U.S., it was alleged that similar attacks on major retailers should have caused the directors and officers to identify an increased risk that the company would be attacked. In the current environment, it could be asserted that with the prevalence of phishing and ransomware attacks (to name two extremely common risks) on organizations of all types and sizes, directors and officers must be particularly alive to controls and reporting for those well-known risks, in addition to considering any risks unique to their industry.

Key steps to consider

In seeking to discharge their duties and to mitigate the risk of personal liability arising from cybersecurity, directors and officers should consider the full range of questions for management, and steps appropriate to their organization and industry. Some of the key steps that typically should be considered include:

- Ensuring that cybersecurity and privacy, and the resources allocated to those areas, are regularly discussed at board meetings;
- Ensuring that officers with expertise of cybersecurity and privacy in the organization give regular presentations to the board and that knowledge is enhanced in other ways;
- Designating a committee of the board, or the audit committee, to have primary oversight of cybersecurity and regular discussion of the topic;
- Baselining current risks using independent frameworks and analysis to identify priorities for management;
- Utilizing third party experts to help assess cybersecurity program effectiveness and improvements (and documenting remediation steps);
- Ensuring that an enterprise-wide cybersecurity framework is implemented, including training programs and vendor management;
- Understanding how the organization is measuring the effectiveness of its cybersecurity program;
- Regularly reassessing risks to track progress in mitigating risks;
- Ensuring that an incident response team, plan and resources are implemented and updated to effectively respond to incidents (in conjunction with a disaster recovery/continuity plan); and
- Identifying risk transfer considerations, including through cyber insurance.

Conclusions

Canadian courts have yet to provide specific direction about director and officer duties in relation to cybersecurity. Certainly the bulk of responsibility for a cybersecurity program will be the task of management and, in its oversight role, the board plainly will not be expected or required to serve as the company's cybersecurity experts. However, there is no question that in recent years the risk for directors and officers in relation to cybersecurity has emerged as a crucial concern. There also seems no question that this key concern will continue and evolve, which will require a concerted ongoing focus.

---

[i] For example, see Forbes.com, Target CEO Gregg Steinhafel Resigns In Data Breach Fallout.

[ii] See e.g. *Collier v. Steinhafel*, Case No. 14–00266 (D. Minn. Jan. 29, 2014)

[iii] CSA Staff Notice 33-321, Cyber Security and Social Media, October 19, 2017

[iv] See e.g. National Association of Corporate Directors' Director's Handbook on Cyber-Risk Oversight (January 2017); World Economic Forum's Advancing Cyber Resilience Principles and Tools for Boards (January 2017).

[v] See e.g. IIROC Cybersecurity Best Practices Guide and the Cyber Incident Management Planning Guide.

[vi] See Privacy and Cybersecurity Bulletin, *Evolving Cybersecurity Regulatory Guidance – Key Finding from Privacy Commissioner of Canada*, Fasken, February 2018. See e.g. IIROC Cybersecurity Best Practices Guide and the Cyber Incident Management Planning Guide.

[vii] Privacy and Cybersecurity Bulletin, *Important New Rules for Mandatory Privacy Breach Notification, Reporting and Record Keeping in Canada*.

[viii] Ibid.

Related Solutions

Practices

Privacy and Cybersecurity

Authors

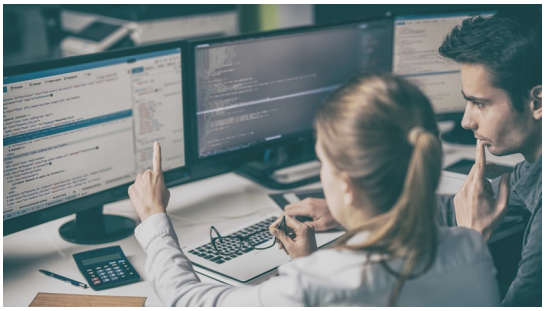
Alex Cameron
PARTNER

Toronto, ON

Daanish Samadmoten
ASSOCIATE

Toronto, ON

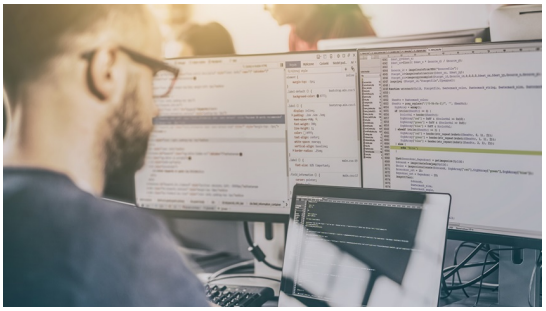
You might be interested in...



BULLETIN FEBRUARY 1, 2018

Evolving Cybersecurity Regulatory Guidance – Key Finding from Privacy Commissioner of Canada

READ MORE >



BULLETIN JANUARY 16, 2018

Artificial Intelligence and the Protection of Personal Information in Canada: The Priority for 2018

READ MORE >

BULLETIN DECEMBER 13, 2017

Mitigating Cyber Security Risks Arising From Open Source Software

READ MORE >