

Directors' and Officers' Liability

Emerging Risks and Risk Control Considerations

Directors' and officers' (D&O) liability insurance coverage is a critical risk-financing tool that is often used to pay legal costs if someone sues your organization for directors' or officers' negligence, and can also cover the costs associated with third party liability exposures.

TYPES OF D&O LIABILITY CLAIMS

Depending on the specific coverage terms:

- Derivative shareholder claims
- Investor claims
- Employer-related (employment practices) liability claims
- Regulatory non compliance allegations
- Other miscellaneous claims including customer claims against the company or directors and officers and, competitor claims against directors and officers.

EMERGING RISKS

Directors and officers need to consider the best interests of the corporation, which includes the interests of shareholders, creditors and consumers. It's critical to work with an experienced insurance professional who can help navigate terms of your policies and advise on other potentially applicable coverage.

Data and cyber security breaches have increased in frequency and severity over the past two years, and directors and officers can be held liable if they fail to meet their duty of care to the company. Directors and officers can be held personally liable and fined if they fail to comply with Canada's anti-spam legislation.



Cryptocurrency and blockchain losses will likely lead to future claims against directors and officers. Currently, very few claims are related to cryptocurrency and blockchain, however, this emerging technology has yet to be fully integrated into that Canadian electric commerce environment.

DUTIES OF DIRECTORS

In general, directors have these duties:

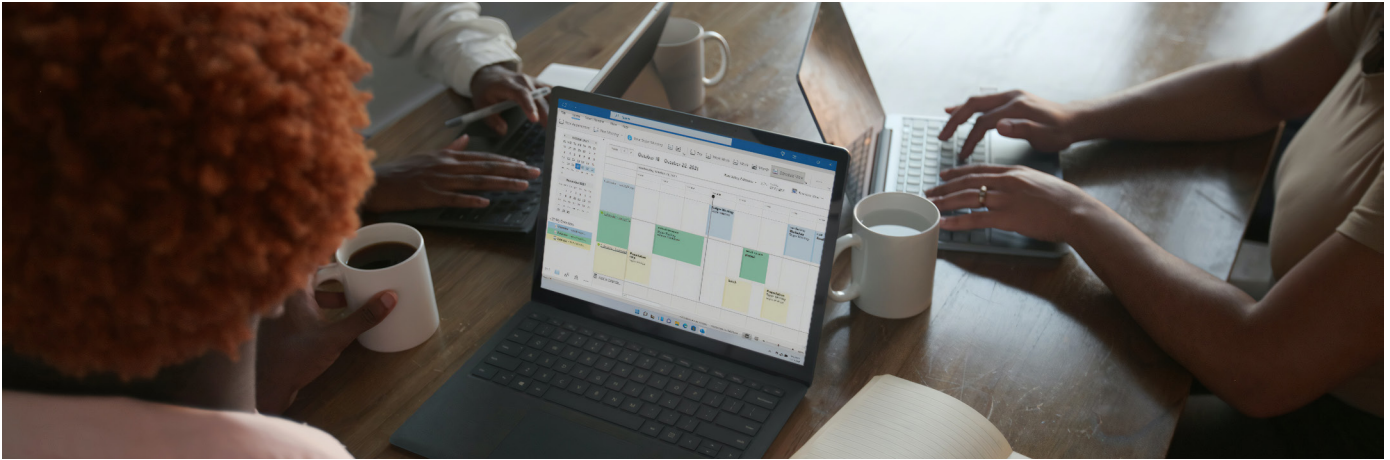
- **Duty to Manage** – While day-to-day management may be delegated to professional managers, led by the corporate officers, the corporation's directors need to supervise and provide oversight for the decisions of the officers and managers.
- **Fiduciary Duty (Duty of Loyalty)** – Directors must act in good faith, placing the interests of the Corporation above their own interests.
- **Duty of Care** – Directors are required to exercise the care, diligence and skill that a reasonably prudent individual would exercise in comparable circumstances.
- **Duty of Compliance** – Directors must comply with applicable corporation statutes and associated regulations, unanimous shareholder agreements, and corporation articles and by-laws.

MEASURES TO TAKE

To mitigate risk and use best practices for management, your organization should:

1. Provide all directors and officers with awareness training with respect to their duties and obligations and update the training every six months to reflect emerging risks. The Institute of Corporate Directors offers excellent training on these topics.
2. In particular, an organization should ensure directors are aware of the nature of the business operations:
 - a) The risks associated with being a director and officer of the organization
 - b) Statutory and civil liabilities
 - c) The importance of general financial literacy
 - d) They have an understanding of the corporate General by law

They have an understanding of the scope and nature of both the statutory and corporate indemnities that may be applicable to them



3. Ensure there is no conflict between the duty owed to the organization and a director's self-interest, and if one exists to disclose it to the other Directors. Directors should:
 - a) Avoid outside employment or business that may compromise the organization's best interests
 - b) Handle confidential and sensitive information carefully (prevent leaks of information)
 - c) Follow guidelines on the appropriateness of public statements (i.e., what information can be released and when)
 - d) Not accept gifts, favours or services relating to company duties.
4. Ensure directors are aware of the organization's operations and affairs.
5. Encrypt all confidential electronic materials
6. Ensure only those with passwords have access and require that passwords be changed frequently
7. Implement firewalls to prevent hackers from accessing information
8. Perform penetration testing once per year to ensure data systems are protected against the latest threats.
9. Create a human resources policy. Prepare formal job descriptions for all employees and document required experience and training, as well as specific aspects of unacceptable employee performance.
5. Ensure all employees, visitors, customers, clients and other stakeholders are protected from reasonably anticipated harm.

ORGANIZATION OVERSIGHT AND RISK MANAGEMENT:

The organization should:

- a) Implement a financial management policy and establish clear financial reporting guidelines
- b) Properly store confidential materials and sensitive information and do the following:
 - Determine who has access

6. Establish a formal information reporting system. Directors and officers are accountable for ensuring that the information that they are receiving from management is accurate. In some circumstances directors and officers are entitled to rely in good faith on the accuracy of expert reports and opinions. All decisions of directors should be documented in meeting minutes and any dissenting opinions should be clearly recorded.

7. Ensure directors work closely with legal representatives in making decisions. Providing full disclosure to counsel, requesting counsel's advice about the legality of a proposed action, receiving advice that the action would be lawful and following the advice may demonstrate that the director acted with due care.
8. Implement a whistleblower policy that is communicated to staff and volunteers. Let employees and others know which board member or representative they should inform about any situation they feel the board should be aware of.
9. Implement a comprehensive director's indemnification policy that clearly states the rights and obligations of directors and what protection the organization provides to them.
10. Ensure directors' and officers' experience and backgrounds are relevant and diverse.
11. Develop an incident response system to identify, record and report incidents to appropriate internal officers, staff, or external regulators.
12. Purchase a comprehensive D&O insurance policy with limits that are adequate to provide a defence and indemnity to the types of claims that may foreseeably arise as a result of the business operations of the Corporation within its current and emerging social economic environment.

QUESTIONS TO ASK YOUR BROKER:

What is Side A (D&O Liability Coverage), Side B (Corporate Reimbursement Coverage) and Side C (Entity Coverage) insurance?

Who is covered by D&O insurance? How can committee members be covered?

What is the purpose of a run-off period? Why is it important?

What are the impacts of insolvency and the D&O insurance policy?

What are the reporting timelines and obligations?

What are the exclusions to the policy?

What is the difference between a "claims made" and an "occurrence" policy?

We are here to help.

IBC has insurance professionals to help businesses navigate the insurance marketplace. Contact IBC's Business Insurance Helpline at **1-844-2ask-IBC** (1-844-227-5422) if you need help obtaining affordable insurance coverage.

