What's The Secret to Protecting Trade Secrets?

In technical terms, a trade secret is a form of intellectual property pertaining to information that is commercially valuable. Why? Well, by virtue of the fact that it's secret.

Valuable, secret information can take many forms. For example: the formula for Coca Cola's signature beverage, or the fabled "Original Recipe" of Kentucky Fried Chicken (KFC). It could apply to anything, really, including a manufacturing process, a method for doing business, research projects, business plans, source codes, and even algorithms. The list is potentially endless.

In order to maintain inherent value in the information, the secret has to be safeguarded and reasonable IP security measures need to be taken. How does one do that? Unlike other forms of IP, such as patents, trademarks, designs, or copyright, there is no searchable registry of trade secrets. Although many countries have laws outlining how misappropriation of trade secrets is a crime, enforcement can be a long and costly process.

Further, unless one can quickly identify a misappropriation and contain it, the secret is often, well, no longer secret. Although certain technology allows for the tracking and identification of potential security breaches, it can also facilitate the speedy transmission (including inter-jurisdiction transmission) of information.

Legal enforcement

Criminal provisions in Canada

Recent amendments to section 391 of the *Canadian Criminal Code* have made it an offence to "knowingly obtain, communicate or make available a trade secret" by deceit, falsehood, or other fraudulent means[1] or does so knowing that it was obtained by deceit, falsehood or other fraudulent means.[2] The *Criminal Code* defines "trade secret" as any information that: (a) is not generally known in the trade or business that uses or may use that information; (b) has economic value from not being generally known; and (c) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[3]

However, the *Criminal Code* excludes as an offence situations where the trade secret

was obtained through independent research and development, or by reverse engineering.[4] Charges can proceed on an indictable or summary offence basis. If convicted as an indictable offence, one could be subject to imprisonment of up to 14 years. On summary conviction, maximum sentencing would be two years less a day and/or a fine of up to $5000 CDN.

Under the *Criminal Code*, law enforcement will bear the burden of investigating and charging those involved in trade secret offences, while the Crown will bear the responsibility of proving beyond a reasonable doubt that an offence was committed. Practically, the owner of the trade secret is in the best position to provide supporting evidence for any conviction, primarily through their systems, policies, and operations. Some law enforcement agencies also have tools and networks that may facilitate identification, tracking, containment, deterrence, and enforcement. Of course, criminal proceedings do not preclude civil proceedings.

Civil remedies in Canada

Remedies for the misappropriation of trade secrets (otherwise known as confidential information) are available in Canada. A handful of landmark Supreme Court of Canada decisions have set the following legal requirements that must be established on the balance of probabilities:

i. The information conveyed was confidential;
ii. The information was communicated in confidence; and
iii. The information was misused by the party to whom it was communicated.

Canadian courts have recognized that it is often hard to quantify the harm suffered as a result of misappropriation of a trade secret. As a result, many have taken an approach geared toward finding a broadly equitable result. This has often led to significant monetary awards.

In addition to monetary awards, a Canadian court may issue an injunction. When there is a serious issue to be tried, there will often be irreparable harm, and the balance of convenience favours granting an injunction. Recently, the Supreme Court confirmed a lower court decision granting an extraterritorial injunction, recognizing that the "internet has no borders."

The secret of maintaining trade secret value

1. Develop a trade secret policy and operational systems in order to:

i. Identify information that is a trade secret (that lends itself to being a trade secret and has value);
ii. Maintain the secret; and
iii. Provide evidence in support for criminal/civil proceedings.

2. Components of trade secret policy

Many components of a good trade secret policy support broader business planning, IP strategy, and data privacy/confidentiality compliance objectives, and may include:

i. A method for identifying and reporting on information that is valuable and ideally kept as a trade secret (as opposed to other forms of IP). What information provides a business with a commercial edge? What information would impact the value of the business if known by others?
ii. Ensuring proper agreement/relationship management, such as standard confidentiality clauses and, to the extent permissible, non-compete provisions

(see below). Also, identifying trade secret information obtained from third parties, isolating it, and limiting access and use in accordance with the agreement.

iii. Adopting proper document management, including labelling/classifying documents, establishing access/permission levels (limiting access to trade secrets or parts of them to certain employees/consultants, etc.), tracking and recording access, encryption, password protection, and physical lock and key methods (including limiting location for access, limiting downloading, printing, and the creation of copies).

iv. Training employees (as well as consultants and third-party partners, as applicable) on appropriate measures to keep trade secrets safe; professionally remind departing employees and applicable third parties of their continuing confidentiality obligations.

v. Ensuring physical security: sign-in/sign-out procedures, security officers, physical security systems.

Last, policies and procedures should not be static. Laws change, so business and commercialization plans and priorities need to change, too, along with the technology used to protect trade secrets. It's imperative for businesses to review the aforementioned on a regular basis..

3. Employment law

Until recently, Canadian employers were able to utilize non-compete clauses in employment contracts as a tool to limit the disclosure of trade secrets. However, in November 2021, Ontario passed Bill 27, *Working for Workers Act*, which prohibits the use of non-compete clauses in Ontario through an amendment to the *Ontario Employment Standards Act*. This prohibition does not apply to "executives[5]" nor in situations relating to a condition of purchase or sale of a business or part of a business, and the seller thereafter becomes an employee of the purchaser.

Although non-compete clauses are generally unenforceable in Ontario, they may be in other jurisdictions across Canada and internationally. Lawyers in the applicable jurisdictions should be consulted for clarification. Further, a non-compete clause does not preclude an employment contract that has continuing confidentiality obligations that survive the terms of employment. Conversely, as a hiring entity, it also does not preclude provisions that prevent an employee or contractor from using third-party confidential information or trade secrets.

When it comes to protecting trade secrets, investing in good policies, procedures, and security measures should be seen as not just the cost of doing business, but an investment in a valuable asset. That asset can ultimately help distinguish the unique products and services of a business, and should be closely monitored, guarded, and contained.

Do you need help with your trade secrets protection, either in Canada or around the globe? Explore our Trade Secrets Law page to learn more about our service offerings and cross-disciplinary team.

---

[1] *Criminal Code* (R.S.C., 1985, c. C-46) , section 391(1)

[2] *Criminal Code* (R.S.C., 1985, c. C-46) , section 391(2)

[3] *Criminal Code* (R.S.C., 1985, c. C-46) , section 391(5)

[4] *Criminal Code* (R.S.C., 1985, c. C-46) , section 391(4)

[5] “executive” means any person who holds the office of chief executive officer, president, chief administrative officer, chief operating officer, chief financial officer, chief information officer, chief legal officer, chief human resources officer or chief corporate development officer, or holds any other chief executive position.

Source: Gowling WLG