By Noel Courage

Sell products globally, but keep trade secrets local

Critical product information should be on a 'need-to-know' basis.

It has never been more important for Canadian companies to identify and protect their trade secrets. We often initially visualize an intruder or a hacker when picturing a trade secret thief. Consider the risk of a thief handing over your stolen trade secrets to his or her business partner.

All of your company's custom-developed, secret software is now theirs. Soon, it will be shared with other companies that are more than willing to also take and misuse the software. Next, your company loses a bid on a major project to the thief's company — after all, it is easy to underbid your company by more than 10 per cent, since the new competitor has spent no money or time on research and development.

The above example is based on a true story that happened in Canada. Who was this thief? It is easier to picture what the thief looks like than you think. He was not an intruder or a hacker. The thief was one of the company's software engineers. He didn't break any locks to get the software — he kept a copy at home. For months, he went to work each day at the company he stole from, while working at night on his own company's projects.

This is a dramatic example of a trade secret theft in Canada. However, trade secrets are more often lost in a more mundane manner, such as by a former employee trying to impress a new company by improperly sharing secrets with the new employer. For example, a highly skilled employee that worked on processes for making high levels of the blockbuster drug lovastatin resigned his position to go work for a competing pharma company. He worked on the exact same drug and springboarded his new company's R&D program ahead so it could also make the drug on a commercial scale.

There is also risk to your company trade secrets when a business partnership goes off the rails. The Clamato brand, its formula (recipe) and manufacturing processes were licensed to a juice manufacturer, who made and sold the product. The Clamato beverage includes tomato juice, clam juice and dry ingredients. After the trade secret owner was acquired in a merger, the licence was terminated. The former licensee was free to compete with the secret owner, and it did so with a new product with different levels of salt, pH and soluble solids. However, the formula and process information of Clamato was used to derive the different new product, described by the court as a virtual copy without clams. It would have taken about a year to develop the new product from scratch without misappropriating the secret.

If it is a trade secret, treat it like one — identify and protect trade secrets. Trade secrets are recognized by Canadian courts as a type of property. However, the secret must be treated as confidential by the owner and communicated to others only on a confidential basis. If this is not done, the rights in the trade secret may be lost. Companies should take time to specifically identify their trade secrets. Make sure they are well documented and kept securely confidential. Intellectual property counsel can advise on best practices, and whether a particular knowledge asset can qualify as a trade secret. To maintain confidentiality, the owner must carefully control the trade secret. Companies should limit access to trade secrets on a need-to-know basis. Written policies should restrict use and possession of trade secrets. Employees and business partners should sign confidentiality agreements. Security measures should be used to protect against nosy employees, business partners, intruders and hackers. When employment and business relationships end, the confidential information must be returned to the owner and use stopped.

Quick action is required once there has been a misappropriation. In Canada, injunctions and Anton Piller orders are good options. Damages and disgorgement of profits may also be requested. There may be more options for remedies in other countries if your business is global, depending on where and how the misappropriation occurred. Some misappropriations may also attract criminal liability.

In the real case of the software engineer thief, an Anton Piller order was used to obtain stolen information and evidence of the theft. The court awarded damages for theft and misuse of confidential information and trade secrets. The court also ordered disgorgement of profits, punitive damages and costs.

Once the secret is out, a lot of time, money and company resources are required to chase down the thief and prevent damage. No award of monetary damages fully restores the hit that an innovative company takes when its trade secrets are lost. Proactively identifying and securing trade secrets is a necessity. **IH**

Noel Courage is a partner at Bereskin & Parr LLP.