Information lock down

Michael Ellis and **Donna Trysburg** of Ellis IP discuss how to manage trade secrets and when such confidential information cannot be protected

Picture: Ba

We see high profile examples of trade secrets whose existence and the publicity surrounding them is as much about branding as it is about secret technology. Coca-Cola's 'famous' secret ingredient has been the mainstay of its apparent uniqueness for over 120 years. KFC's secret 'blend of 11 herbs and spices' is a key element of its marketing message. The recipe for Irn Bru is also a closely guarded secret.

But how do trade secrets apply to our own organisations and what are they?

What are trade secrets?

Trade secrets are typically the most neglected form of intellectual property; the poorer cousins of registered rights such as patents, design registrations and registered trademarks. A trade secret can be any item of knowledge or information known only by your organisation and that has a perceived value.

There is very little harmonisation at international level for trade secrets. The Trade Related Aspects of Intellectual Property Rights Agreement (TRIPS) contains an obligation on Member States to protect "undisclosed information", framed within the wider policy against unfair competition. Article 39(2) states that natural and legal persons shall be able to prevent information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices, as long as: (a) the information is not generally known; (b) the information has commercial value because it is secret; and (c) the owner has taken reasonable steps to keep the information a secret.

The US approach appears to largely follow TRIPS. The Economic Espionage Act 1996 makes the theft of a trade secret a felony. Section 1839(3) of the US Code provides a useful definition:

> "Trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information whether or how stored if:
>
> - The owner thereof has taken reasonable measures to keep such information secret; and
> - The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

As this is a criminal law, perpetrators are liable to face fines and incarceration. Civil law action can be taken in the US under the Uniform Trade Secrets Act 1985 (applicable in most states). The definition of a trade secret is essentially the same as that under the criminal code.

By contrast, in the UK, there is no specific legislation which protects trade secrets, or any universally accepted legal definition. Trade secrets disputes are dealt with via contract law or the action for breach of confidence. Contractual obligations of confidentiality can be imposed in a wide range of circumstances, for example, in standalone confidentiality agreements or non-disclosure agreements (NDAs) or confidentiality clauses in pre-joint venture memorandums of understanding (MoUs), terms of business, or employment contracts. In addition, an action for breach of confidence is available in which the claimant must prove that (a) the information has the necessary quality of confidence about it, (b) the information was communicated in circumstances importing an obligation of confidence and (c) there was unauthorised use of the information to the detriment of the party communicating it, following *Coco v AN Clark* (1968).

The case centred round a moped manufactured by mast-making business AN Clark (Engineers) Limited. The innovation in the power unit of the moped was not Clark's, instead it was devised by *Mr Coco*, who had been in discussions with Clark's for several months before being informed that his design caused unacceptable wear to the rear tyre and would not be used. By the time the machine appeared on the market, it was realised that the power unit was closely related to the Coco design. Mr Coco sued for breach of confidence. The case remains a fundamental statement of the principles of law in this area, despite not going to trial as the defendants paid 5 shillings per engine as compensation.

How to keep a trade secret

There are certain actions one can take to maintain a trade secret:

Contracts of employment

- A Confidentiality clause; or
- Restrictive covenants to prevent certain key employees with access to special information from taking up equivalent posts with competitors. These must be reasonable and proportionate.

NDAs

- When negotiating with partners or potential partners, or when securing manufacturing or distribution agreements, ensure that a non-disclosure agreement is in place to oblige the third-party to keep the information secret and to use it only for the identified purpose; and
- Only provide necessary documentation to support purpose.

Document the trade secret

- Some countries require a trade secret to be documented before it can be categorised as a trade secret and action taken; and
- Documentation provides an improved form of evidence.

Security provisions

- Limit access to a need-to-know basis. Optionally, ensure that the number of people who know the secret in its entirety are limited.
- Control distribution.
- Use encryption and computer passwords. In the case of software, consider providing the solution as a service over a secure server.

Take swift enforcement action against breaches and former employees

- Such a clear signal highlighting the importance your organisation places on trade secret information may deter others from doing the same.

Mistakes with trade secrets

Let it walk out the door

Even with NDAs or employment contract confidentiality terms in place, something you regard as company know-how or a trade secret can unknowingly walk out the door. The knowledge your employees have of proprietary information can provide a commercial advantage, even if it is negative information.

In *Faccenda Chicken Ltd v Fowler* (1986), the UK Court of Appeal found that an ex-employee may use confidential information acquired during the course of his previous employment (short of memorising and recording such information during his employment). Confidential information short of a trade secret is not protected. In considering whether information is a trade secret, the court should have regard to the nature of the employment and status of employee within the organisation, the nature of the information, whether the employer had stressed the confidentiality of the information to the employee and whether the information could be isolated from other knowledge and non-confidential information.

Thus, a simple clause in a contract cannot necessarily be relied upon. Confidential information in the possession of an employee should best be recorded and categorised as confidential or a trade secret if it is deemed valuable, and the duty of confidence the employee has in relation to that information should be clarified.

Reverse engineering

If products are available to the public, the information deducible from them is also. This is explicitly set out in the US Uniform Trade Secrets Act 1985 and established by case law in the UK. *Mars UK v Teknowledge* (2000) indicates that a breach of confidence action will not be successful for reverse engineering[1]. Ownership of an item includes an entitlement to dismantle and see how it works; therefore the information does not have the necessary quality of confidence. Encryption measures do not imply an obligation of confidence.

Telling too many people

Even under NDAs, by revealing your trade secret to multiple third parties, you substantially increase the risk of that secret being lost. Once it is the public domain, there can be no recovery and identifying the responsible party will be challenging.

Is a trade secret the right form of protection for us?

Trade secrets and/or patents may be appropriate protection for a product or method depending upon the circumstances.

A patent may be more appropriate where:

- Reverse engineering would reveal a trade secret;
- Absolute protection is required. A patent can prevent others from working the patented invention, copied or not;
- Licensing is desirable eg, for manufacture or franchising purposes patents are easier to manage, exploit, license and franchise because the subject matter is already disclosed; and
- There is a risk to the business. Damages for breach of confidence would not be a sufficient remedy if the secret were disclosed.

A trade secret may be more appropriate where:

- Longevity is desirable. Patents last for only 20 years, whereas a trade secret will last as long as you can keep it a secret;
- Changes are likely. Trade secrets can accommodate change and product development more easily, whereas patents will only protect the claims applied for;
- Multiple concepts make widespread patent protection cost prohibitive; and
- The 'need to know' basis only extends to a select few individuals.

What should my organisation be doing?

The proper protection of trade secrets requires a good deal of effort and should always be undertaken in an informed manner as part of a broader approach to IP management.

Develop an IP policy

An IP policy sets out the company's approach to management of intellectual property. Responsibility for IP matters should be at a senior level. It should provide general guidance on what and how certain types of IP are to be protected, including new patentable ideas and key valuable information, processes and methods.

A risk register and IP capture process

A risk register is an effective way to identify at a high level the intangible assets of your organisation. Capturing information may require some probing, as people harbouring information often under-value it and may not offer it up when asked directly. The risk register should include analysis of a) the likelihood and b) the consequence of losing that IP. Highly rated risks may represent IP that needs effective protection. The risk register may also indicate how certain IP links together with other IP for a single product and how to protect it. An idea/information capture process should be the responsibility of a designated person. The risk register should be a living entity, regularly updated and reviewed.

Enforce appropriate protection

On establishing the relative value of IP assets, the form of protection should be chosen in accordance with the IP policy, taking into account the type of IP and the business model (eg, a product or service model).

Establish secure processes and methodologies for trade secrets

Once a valuable trade secret has been identified, a set of security procedures relative to the importance of the secret should be implemented. This should include:

- Documentation as essential evidence for the future and for defining as a form of trade secret control of distribution (eg, only to key individuals);
- Establishing security measures such as secure documentation storage, careful document destruction, encryption, minimal memory stick use and passwords on laptops;
- Confidentiality measures – for relevant staff, suppliers, contractors, commercial partners and outsourced manufacturers;
- Ensuring knowledge/expertise of key staff is shared and plan for staff departures; and
- Planning for recovery in case of loss

Trade secret protection is not a concern exclusive to large international organisations. By properly managing IP and applying a dose of commercial sense with carefully managed procedures, valuable trade secrets can be identified, documented and effectively protected by any organisation.

Footnote

[1] In its simplest terms, reverse engineering is taking a product and dissembling it to figure out how it works. It is legal as long as the object is obtained legitimately.

Authors

Michael Ellis is a patent attorney and IP consultant at Ellis IP, a full service intellectual property consultancy based in Edinburgh. Its consultants advise on and help implement business-focused intellectual property protection and commercialisation strategies for small and large companies in a broad range of sectors.

Donna Trysburg is an IP analyst, also at Ellis IP.