Trade Secrets – What They Are And How To Protect Them

What is a trade secret?

A 'trade secret' is information which: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

In practice, information that you actively keep out of the public domain because it gives you a competitive edge, either now or in the future, is a trade secret. A trade secret does not expire as long as it is kept secret and it therefore maintains its value, potentially indefinitely. However, once the information is in the public domain, reverse engineered or independently derived, the information loses value. So it is crucial that robust policies and procedures are in place to prevent disclosure or theft. Having such protections in place maximises the chance of trade secrets remaining as such and will provide evidence to help you recover damages, should one of your trade secrets be stolen.

This is not to say that trade secrets are not transferable. If appropriate measures are in place, and now that trade secret legislation is becoming well-established, trade secrets can be transferred by agreement.

Should unauthorised acquisition, use or disclosure of a trade secret occur in the UK, this is considered unlawful (under the Trade Secrets (Enforcement, etc.) Regulations 2018 (SI 2018/597)). This applies not only to the original acquirer of the information, but also to any other person who later obtains the trade secret directly or indirectly and who knew (i.e. a subjective test) or ought to have known (i.e. an objective test) that the trade secret had been acquired unlawfully. Unlawful use of a trade secret includes producing, offering or placing on the market infringing goods, and importing, exporting or storing infringing goods for those purposes.

Does your company hold trade secrets?

Yes, your company certainly has trade secrets. Instead, you should be asking whether you are *recognising* and *treating* your trade secrets appropriately. Examples of the type of information which can qualify as a trade secret if kept confidential includes commercial data, technological information or product information. Commercial data include customer or supplier information, business plans and market strategies.

Technological or product information includes recipes, techniques and know how. Clearly, these types of information have little value if widely known but potentially considerable value if known only to one or very few persons in the relevant market. Famous examples include the recipe for Coca-Cola® or for WD40®, details of upcoming Apple® product launches, and the Google® search algorithm. All of these examples are hugely valuable as long as they remain secret but would be worthless if widely known.

Of course, in many instances you may decide to protect technical information with a patent. However, information which is not patent eligible – including negative test data or failed prototypes – may be valuable as a trade secret. Usefully, unlike a patent, trade secrets can evolve over time and are not time-limited. Sometimes you might decide not to apply for a patent to an invention or to withdraw a priority application before it publishes, and instead treat the information as a trade secret. In such cases, take care to take the appropriate active steps to catalogue and protect the subject matter as a trade secret.

There is absolutely no requirement that a trade secret must be technical. A more prosaic example is your company's customer profile. This is valuable to your company because it gives you an informational edge over your competitors, but if your competitors have the same information then it is less valuable.

How do you keep them secret?

1 Knowledge

You can only control secrets that you know about. The first step of a company trade secret policy is to appoint a manager of trade secrets. The manager should conduct an audit of all information believed to be secret and commercially valuable.

Assemble the information and then analyse it to assess whether it is confidential to the company, and whether it has value as a result of that confidentiality. Assuming there are some trade secrets, then put in place policies to protect them (see below).

From then on, you should maintain a catalogue of key metadata relating to the trade secret, for example including identifying information such as the title, owner, creation date, creator, location, access information and protection mechanisms. You may also consider recording the estimated value of a trade secret, any expected publication date (if appropriate), information of who they have been shared with and when (including copies of any agreements and contracts used), and a dated audit trail of any changes occurring. This information can be leveraged (for example to investors, or to reassure a potential collaborator) without divulging the trade secret itself. Similarly, you may wish to know that a collaborator has equivalent processes in place before sharing your own trade secrets with them.

Most companies continue to research, innovate and improve their processes and products and therefore are likely to continue to generate information which could potentially qualify as trade secret. Accordingly, your company's ongoing trade secret policy should ensure that any new trade secret is recognised as such and falls within the framework set up to protect the existing trade secrets.

Not all trade secrets remain secret and commercially valuable forever, and information no longer considered a trade secret need not be subject to the same protections. It is useful to review the designated trade secrets periodically so that any information which is no longer valuable (e.g. the business plan for 2010) or no longer secret (because it was either deliberately or accidentally disclosed) can be re-designated and resources diverted away from protecting it.

2 Policies

The key points to guide your company's policy are 1) the fewer people who know a secret, the less likely it is to be disclosed; and 2) a court will look at what effort a company has expended in protecting information as part of its assessment of whether that information qualifies as a trade secret.

The number of people who need access to a trade secret will depend on the size and sophistication of your business. However, as a general rule, access to a trade secret should be on a need-to-know basis.

2.1 Internally within the company

Staff in different departments need to know different things: sales staff need to know about customers but not the recipe, whereas manufacturing staff need to know the recipe but not the customers. Accordingly, try to minimise the number of staff privy to specific information. Restrict access to information physically, electronically and legally to those staff who need to know it in order to discharge their duties.

Put in place procedures regarding the handling of trade secrets, sharing and governance of trade secrets and what to do in the event of inadvertent disclosure. These policies will likely require input from HR and IT personnel. Ensure that staff are educated and up-to-date on these policies, and reminded of their duty of secrecy at exit interviews.

2.2 Physically/Electronically

R&D laboratories should be accessible only to the relevant researchers, and documents detailing trade secrets should be marked as confidential and kept in a safe place (e.g. a safe).

Electronic documents should be protected by passwords and computers should be protected from hacking (we don't pretend to be IT security experts – your IT consultants will give you best practice on this).

2.3 Legally

There are three phases to the legal aspect: when staff join, while they are employed, and when they leave.

When staff join it is important to ensure that employment contracts for relevant staff include confidentiality provisions (and possibly non-compete and non-solicitation provisions).

While they are employed it is important to educate staff about what a trade secret is (so they can identify new ones), what the company considers to be trade secret, and the consequences of the secret no longer being secret. The company should monitor compliance with the physical and electronic procedures put in place to protect the trade secrets. There is little purpose in having rules which are not observed.

When staff leave they should be given an exit interview to remind them of their obligation of confidence. In addition, they should return all company property and sign a statement confirming that they have returned all confidential information (physically and electronically).

2.4 Externally with contractors

The same basic rules apply to relations with external contractors. A company should protect its confidential information physically, electronically and legally.

In physical and electronic terms, this means much the same as for internally within the company: use physical and digital means to restrict access to the information.

In legal terms, this means that companies should always sign non-disclosure agreements (NDAs) before disclosing any confidential information (even if the information does not qualify as a trade secret because it has no commercial value, it might one day become commercially valuable). NDAs should be drafted in as specific terms as possible in relation to what information is disclosed and to whom it is disclosed (i.e. specific individuals), and they should be appropriate for the jurisdiction (i.e. enforceable where the receiver of the trade secret is based).

When the collaboration comes to an end it is vital to ensure that all documents (physical and electronic) containing confidential information are returned or destroyed, and ensure that the NDA continues to be enforceable in relation to information that the collaborators might remember.

2.5 From the general public

The basic principles of restricting access physically and electronically apply. If the general public is permitted onto the premises, then it should be only into areas where there is no risk of any confidential information being accidentally disclosed.

Remember, also, that in addition to restricting access by the general public, it is important to prevent staff accidentally releasing confidential information into the public domain. Any documents which contain confidential information should be shredded when disposed of, staff should not work on confidential documents in public spaces, and care taken with electronic access, USB sticks and suchlike.

What should you do if a trade secret has been stolen from you?

One of the most useful remedies available in the UK to a trade secret holder is an interim injunction. This is an Order from the Court, obtainable on very short notice, that the person alleged to have stolen the trade secret may not disclose nor use the trade secret until the case has been decided at trial (which might take a year or more to be completed).

Interim injunctions may be awarded by the court as long as there is an arguable case that a trade secret has been stolen by the defendant, and that monetary compensation would not be adequate to compensate the trade secret holder. The interim injunction will remain in place until trial, at which point it will

either be converted into a permanent injunction (if the judge holds that the information did qualify as a trade secret and that it was unlawfully acquired) or it will be lifted (if the judge decides that the information did not qualify as a trade secret or it was lawfully acquired). If lifted then the claimant will be liable to the defendant for damage caused to the defendant by the interim injunction.

In order to obtain an interim injunction, especially to prevent further disclosure of the trade secret, a trade secret holder will need to apply to court as quickly as possible. The process will run more smoothly if the trade secret holder is ready with important information easily accessible. For example, it will be important to produce details of the information that the putative defendant was exposed to; a copy of the relevant confidentiality contract (i.e. the employment contract or NDA); details of the policies the company has in place to keep the information secret; the likely value of the information they might have stolen; and the possible damage that the company could suffer if the information is disclosed further.

What remedies are available for theft of a trade secret?

As discussed above, it is possible to obtain an injunction to prevent the defendant disclosing the trade secret to third parties, and to prevent the use of the trade secret and/or the sale of infringing products.

In addition, the Court can order the defendant to pay damages. In the UK damages are intended to be compensatory. In the case of trade secrets that means that damages are intended to put the claimant in the position it would have been had the trade secret theft not occurred. This can be calculated as the trade secret holder's lost profit, or account of the defendant's profits.

The same policies and procedures that reduce the likelihood of trade secret theft in the first place (as described above) will assist with establishing a legal case, if required.

Is it possible to licence trade secrets to third parties?

Yes. It is important to take care to ensure confidentiality is maintained but, in principle, it is possible to licence trade secrets as know-how. The licence should compel the licensee to take steps equivalent to those taken by the owner of the trade secrets to protect the confidentiality (i.e. all the points discussed above), and could include provision for the trade secret owner to be able to conduct spot checks on the licensee to ensure that those policies are being enforced. Further, the licensee should be under an obligation to report full details of any suspected breaches of confidence as swiftly as possible to the trade secret owner in order to enable prompt legal action to be taken.

Summary

Companies should know what their trade secrets are on an ongoing basis and take steps to maintain their confidentiality. Prompt action should be taken if it is suspected that a trade secret has been stolen.

For more information, please contact:

Martin Jackson — mjackson@jakemp.com

Josephine Pepper — jpepper@jakemp.com