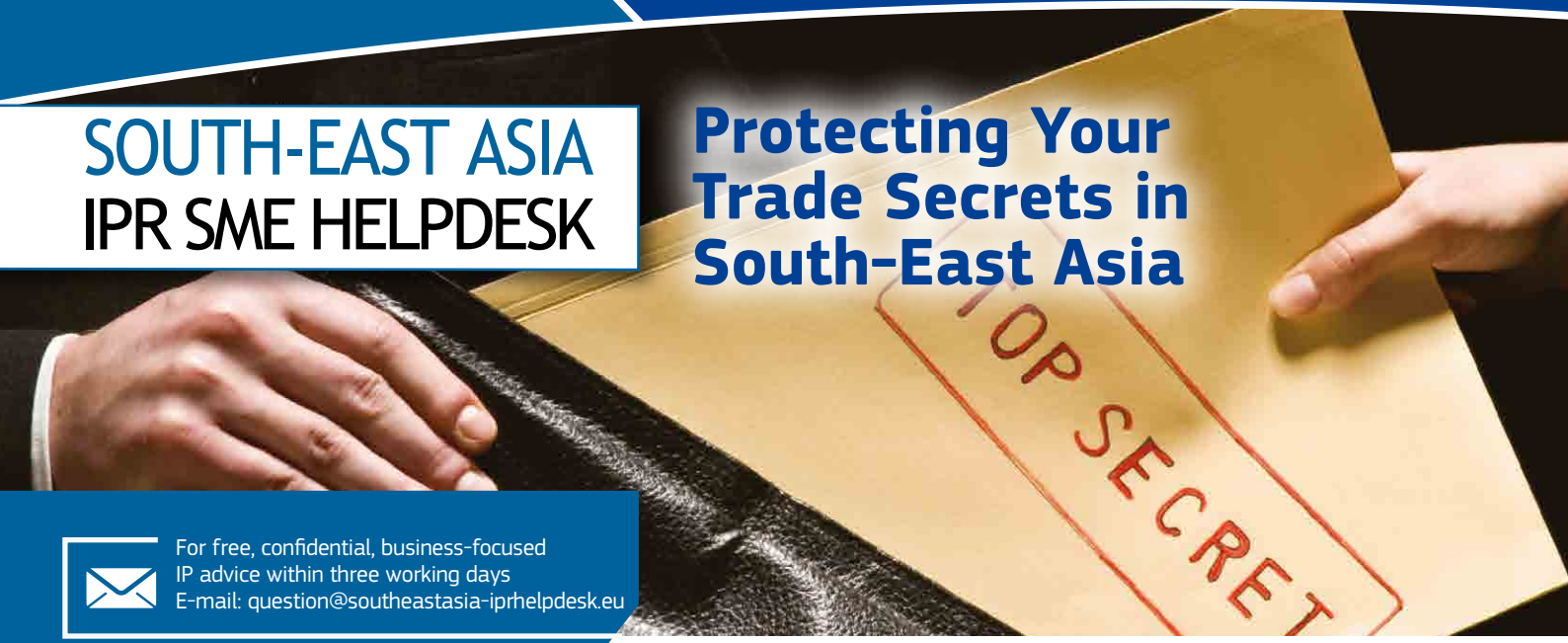
European Commission

SOUTH-EAST ASIA
IPR SME HELPDESK

Protecting Your Trade Secrets in South-East Asia



For free, confidential, business-focused
IP advice within three working days
E-mail: question@southeastasia-iprhelpdesk.eu

1 What is a 'Trade Secret'?
2 Keep it Secret!
3 If it's a Secret, Why do we Need a Law?
4 Duration of Trade Secret Protection
5 Managing your Trade Secrets : Physical, Technical and Contractual Barriers
6 Employee Management
7 Trade Secrets and Other Forms of IP
8 Trade Secrets in Different South-East Asia Member Countries (including brief country-by-country guides)
9 Case Studies
10 Take-Away Messages
11 Your Trade Secret Checklist

1. What is a 'Trade Secret'?

Nearly all businesses in all industries and sectors possess trade secrets. Trade secrets are a highly valuable and useful form of intellectual property right (IP). According to the World Intellectual Property Organization (WIPO), any confidential business information (for example sales methods, distribution methods, consumer profiles, advertising strategies, lists of suppliers and clients, manufacturing processes, etc.) which can be of considerable commercial value to businesses and which provides an enterprise with a competitive edge, may be considered a trade secret. Trade secrets encompass manufacturing and industrial secrets as well as commercial secrets, and may include technical know-how, new products or business models, business operation manuals, recipes and formulae, customer and supplier information, or special techniques uniquely and confidentially employed by a business in the development of a product or service, all of which are closely guarded by the companies in question.

Typically three general standards exist (which are referred to in Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)), and a trade secret is usually defined as information that:

(a) is not generally known to the public (kept as confidential);

(b) confers some sort of economic benefit on its holder (where this benefit must derive specifically from the information not being generally known, not just from the value of the information itself – in other words: it must have commercial value because it is a secret); and

(c) is the subject of reasonable efforts by the rightful holder of the information to maintain its secrecy (e.g., through confidentiality agreements).

Internal Market, Industry, Entrepreneurship and SMEs

The competitive edge of many companies is based on keeping information confidential. The unauthorised use of such information by anyone other than the owner is regarded as an unfair practice and a violation of the trade secret. However the conditions for protection guaranteed by a trade secret may vary from country to country. Depending on the national legal regime, trade secrets are subject to the protection provided for in unfair competition laws or other specific provisions (like the provisions of labour law, criminal law, civil law, invention law, or IP law), as well as to rules developed in case law relating to secret information protection. However, no matter which jurisdiction your business operates in, it is vital that your company takes the appropriate steps to protect your trade secrets in order to maintain a competitive advantage over your rivals.

You can protect your trade secrets as long as you do not allow the confidential information to flow into the public domain. To be protectable, information must be kept confidential. Protection from misuse of trade secrets might include a court injunction to contain abuse or disclosure, in addition to damages incurred. One of the world's best kept trade secrets is the recipe for Coca-Cola, a formula which has been closely guarded for decades. Had CocaCola patented the formula when it was first invented, it would have entered the public domain as soon as the patent expired (most patents last a maximum of 20 years). This is arguably the most famous example of the long-term benefits of a well-protected trade secret.

2. Keep it Secret!

The very nature of a trade secret is that you own it by virtue of not disclosing the information that is to be protected. Simply calling something a trade secret is not enough. In order for the information to be considered a trade secret, it must meet the basic requirements as outlined previously, namely it must (a) be non-public not known to your competitors; (b) have actual or potential commercial value; and (c) be safeguarded by confidentiality measures including clauses in employee contracts and nondisclosure agreements. These three elements are essential for a business to protect its trade secrets.

3. If it's a Secret, Why do we Need a Law?

Trade secrets are created by developing something new and of economic value in a confidential environment where those with access to the information must be under the obligation of confidentiality. The law is targeted at those entrusted with trade secrets and those who employ illegal methods to obtain trade secrets. These laws are aimed at prohibiting perpetrators from illegally acquiring the trade secrets of other companies, or benefiting from the fruits of trade secret misuse.

Once a trade secret is known to the public, it is no longer protected.

Once a trade secret is known to the public, it is no longer protected. It is therefore important to take proactive action to prevent leaks and be quick in addressing trade secret theft.

4. Duration of Trade Secret Protection

There is no form of registration applicable to trade secrets and therefore there is no time limit in the protection of any trade secret provided that it is kept from the public domain. Unlike other forms of IP rights such as patents and copyrights that have a finite term, trade secrets can theoretically enjoy an infinite term of protection so long as the trade secret remains just that – a secret.

5. Managing your Trade Secrets

Most laws require trade secret owners to show that they have put measures in place to safeguard the confidentiality of the information. This might include a system of: identification of information intended to be kept confidential such as marking and storage; procedures in place on how to handle such information to preserve its confidentiality; and rules that confidential information can only be accessed by selected staff.

It is important to remember that once trade secrets become publicly known, they can no longer be protected as trade secrets. Ways in which a trade secret can be disclosed would include publication, disclosure of technical information by your engineer during a seminar, disclosure of information or documents during negotiations and other business dealings with third parties without a non-disclosure agreement, conversations, accidental disclosure by misdirected E-mails or other correspondence, etc.

Trade secrets differ from other valuables in that they are not always in a tangible form, but as with anything of value, it is important to keep them secret and safe. Trade secrets may be stored in printed documents, CDs or DVDs, computer files and hard drives, USB drives, or even in your head. As it is not always practical or possible to keep trade secrets locked away, keeping trade secrets safe usually involves using a combination of **physical, technical**, and **contractual barriers.** Although some businesses go to great lengths to protect their trade secrets, any business can and should take simple, sensible precautions.

(a) **Physical barriers** may include simply marking documents 'CONFIDENTIAL', keeping sensitive documents in a safe, undisclosed location, and locking files away after business hours. In addition, access to areas where sensitive business documents are stored should be restricted to certain employees. Limit access and copying rights to the personnel who actually need it. All visitors should be logged, required to sign a non-disclosure agreement before being granted access to sensitive areas of your premises, and should not be left unattended.

(b) **Technical barriers** require the use of information technology (IT) to protect trade secrets stored in electronic files on your computers or data servers. The basic rule in IT security is that the more valuable the information, the harder, more expensive, and more difficult it is to protect. Consulting an IT security specialist can help you to design a cost-effective IT security system. However, even simple, inexpensive means of IT security measures can be used such as employing the proper use of passwords, commercially available encryption, and logging features. In addition, it is important to have a written technology policy in place and to ensure that your employees abide by the technology policy. For example, as it is extremely easy for your employees to E-mail sensitive documents to third parties or to transfer files using USB drives or CD/DVDs, you might want to consider restricting the ability of your employees to use USB drives and burn CD/DVDs. Your employees in Southeast Asia should be given a copy of your technology policy written in both English and the local language where relevant (possibly as an appendix to their employment contract) and be required to sign an agreement stating they received and understand the policy.

(c) **Contractual barriers** generally involve the use of non-disclosure or confidentiality agreements. In fact, such agreements are generally considered as one of the best ways to protect your trade secrets. You should require every existing employee and all new employees to sign an employment contract with non-disclosure or confidentiality provisions. For your employees in South-East Asia member countries, the contract should be in both English and the local language to prevent an employee from claiming that he or she did not understand the confidentiality obligations. Such agreements should also be entered into with suppliers, subcontractors, and business partners who are given any level of access to your trade secrets.

Be sure to document the trade secrets protection measures you take. It is also essential to maintain sufficient records of the flow of information in and out of your company, including keeping records of meetings, discussions, E-mails, written correspondence, and the transfer of electronic files so that you can conduct an investigation and have evidence in case you suspect your trade secrets have been misappropriated.

It is important to have a written technology policy in place and to ensure that your employees abide by the technology policy.

6. Employee Management

Trade secret theft can be extremely difficult to detect and even harder to prove in a court of law. In some cases, victims may even harbour strong suspicions over the loss of certain trade secrets to former employees but, in most circumstances, are unable to take any action to redress losses because of a lack of proof. Courts in Southeast Asia are required to protect a former employee's right to re-deploy his/her existing skills in order to make a living elsewhere, even if those skills were acquired from the previous employer. Courts are also quick to emphasise that there is no proprietary right over one's customers. Therefore, a former employee is free to solicit the business of customers of his/her former employer as long as that employee has not copied confidential information, which may include a list of clients, from that employer. It becomes difficult to distinguish between the individual thoughts of the employee and certain confidential information such as protected customer lists. It is for this reason that common law systems, such as those adopted in Singapore or Malaysia, allow employers to impose restraint of trade or non-compete clauses in employment contracts. The law requires that such clauses be reasonable to the extent that is necessary to protect a legitimate interest. A non-compete or non-solicitation clause limited to Singapore for a six month period is more readily upheld than a six year world-wide provision.

As such, employers in countries such as Singapore and Malaysia are far more likely to enforce non-competition or non-solicitation clauses rather than attempting the somewhat arduous task of proving trade secret theft, assuming that the contracts bear such non-compete or non-solicitation clauses.

Finally, be vigilant in protecting your trade secrets and implementing your trade secrets protection policy. Businesses usually lose their trade secrets because they are too relaxed about keeping the information inside the company. Make sure your management is informed. Trade secrets are a double-edged sword – your staff and workers must be told not only to protect your trade secrets, but also not to obtain or utilise the trade secrets of others. Designating a person to be in charge of ensuring compliance with your trade secrets protection policy may be a useful option to consider.

When dealing with external parties it is advisable to request the signing of a Non-Disclosure Agreement (NDA) before divulging any confidential information. NDAs are crucial parts of a programme to protect trade secrets and SMEs shall become familiar with this type of legal documents and include them in their management activities. The duty of confidentiality extends to third party recipients who are reasonably expected to have knowledge of the confidential nature of the information in question.

As there is no formal registration process for trade secrets, they are often referred to as 'unregistered rights'. In theory, trade secrets will last forever as long as the information does not enter the public domain.

Modern informal collaborations, particularly in respect of internet and e-commerce start-ups often do not put a proper focus on intellectual property rights, putting at risk patents, ideas and IP ownership. SMEs shall be aware of the risks of informal collaborations where such matters are not defined in writing and therefore difficult to be proved.

7. Trade Secrets and Other Forms of IP

It is not always obvious when to keep your information secret rather than patenting your know-how. Patenting entails comprehensive disclosure to the public of valuable information before patent protection can be granted. Moreover, patent protection is only for a limited duration of twenty (20) years. After patenting their original formula in 1893, the owners of Coca-Cola chose not to patent the new formula and instead chose to use secrecy to protect it until this day. Trade secrecy is only a viable option when reverse engineering (the process of discovering the technological principles of a device, object, or system through analysis of its structure, function, and operation) is impossible and the business in question practices a regime that establishes and maintains secrecy over confidential information. Where reverse engineering can be easily carried out, it might be more beneficial for the company to use patent protection to protect its IP even if voluntary disclosure to the state is necessary for a protection period of twenty years. SMEs shall be aware and carefully analyse advantages and disadvantages whether to keep information secret of protect them under patents.

As there is no formal registration process for trade secrets, they are often referred to as 'unregistered rights'.

8. Trade Secrets in Different South-East Asia Member Countries

Legal systems in certain South-East Asia countries are relatively underdeveloped in terms of protecting trade secrets. One reason for this is because judges often encounter difficulties when dealing with 'unregistered' IP rights. In such countries, cyber-crime laws (if available) might be the more effective solution.

(a) **In South-East Asia, as is the case in most parts of the world, the protection of trade secrets can only be achieved when the following criteria are met:**

(i) The information must not be available to the public.
(ii) The information must offer real or potential advantages to the business in question.
(iii) You must be able to prove that you took measures to protect the confidentiality of the information (confidentiality clauses, password protection, restricted access to important information/buildings, etc.). The internal regulations of businesses should also stipulate how the trade secret is kept and who is responsible for its secrecy.

(b) How long does legal protection last in South-East Asia countries?

In theory, trade secrets will last forever as long as the information does not enter the public domain. Despite being classified as 'unregistered rights' in some South-East Asia countries, trade secrets are recognised in most South-East Asia countries (see country-by-country guide below for exceptions) and can therefore be enforced provided that you can prove that the trade secrets are not known to the public, the abuse of which is to the detriment of your business, and you have taken measures to protect their confidentiality.

Watch-Out: Unauthorised access to computer systems

South-East Asia countries such as Singapore, Thailand, Malaysia, the Philippines, and Indonesia have laws that protect unauthorised access to computer systems. Such laws can add to combatting the theft of protected information. Advances in computer forensics have also made it harder to avoid all traces of improper computer access by, amongst others, departing employees. In Singapore for example, several ex-employees of a bank were prosecuted for downloading customer information prior to joining a competitor bank (see Case Study 1 below for more details of the case).

Here is your brief South-East Asia country-by-country guide:

(i) Brunei

Trade secrets are not regulated by any specific legislation in Brunei. Provision does however exist in common law as the protection of trade secrets are usually provided for in a contract; for instance a contract of employment will provide that an employee leaving employment is contractually bound to protect the trade secrets of the employer for a specific number of years.

(ii) Cambodia

Cambodia has not yet adopted a specific law on trade secrets. However, a draft law is currently being negotiated. Until Cambodia has adopted the 'Law on Trade Secrets and Undisclosed Information', trade secrets may be protected under other laws. For example, to maintain information in employment or other contractual relationships, a non-disclosure agreement may be used and enforced pursuant to the Contract Law of 1998.

(iii) Indonesia

With regards to trade secrets in Indonesia, it is necessary to prove that the trade secret has been unlawfully obtained by the suspected party. Proving this may be difficult as the litigation procedure is not equipped with a discovery procedure to uncover relevant evidence of the suspected party. It may help if you can prove that the local company had some form of relationship previously with you (the victim company) OR was previously given access to the trade secret.

(iv) Laos

Until the IP Law was enacted in 2011, trade secrets did not enjoy protection in Laos. The IP Law sets out the conditions for information to be considered a trade secret: the information must be useful for operating a business or service, it must be information not widely known to the general public, and it must be information not yet accessible by persons who are normally connected with it (Article 20).

Information not eligible for protection as trade secrets includes personal secrets, secrets of the state and state administration, and other non-business related secret information.

(v) Malaysia

Trade secrets are recognised in Malaysia and qualify for IP protection as long as the criteria in section 7 (a) of this guide are satisfied. It is advisable to incorporate confidentiality terms in employment contracts to protect your trade secrets. This 'confidential information' should be defined in sufficiently broad terms to include information created by employees during the term of their employment.

Despite being classified as unregistered rights, trade secrets in Malaysia are recognised and can be enforced, with the provision of sufficient evidence that the trade secrets are not known to the general public, the abuse of which is to the detriment of your business, and you have adopted sufficient safeguards to ensure their confidentiality.

(vi) Myanmar

There is no law on trade secrets in Myanmar. Protection for confidential information arises solely from the law of contract, so there is no means of protection where no contractual relationship exists. The secret know-how will only be protected on the basis of a mutual legal relation created by agreements (non-disclosure or confidentiality agreements/ clauses) signed with subcontractors, licensees, etc., obliging them to keep the information confidential, as well as agreements signed with employees under which they have a duty not to disclose the confidential information, both during the term of their employment and after its termination, and also obliging them (contractors, licensees, employees, etc.) not to use it for competition purposes.

(vii) The Philippines

While the Filipino IP Code includes 'protection of undisclosed information' as one of the intellectual property rights, it does not define it. At present, there is no law that defines trade secrets but the Supreme Court (in the case of Air Philippines Corp. v. Pennswell Inc. G.R. 172835, 13 December 2007) adopted the definition of the term from Black's Law Dictionary:

There are laws that prohibit revelation of trade secrets (such as the Article 40 (e) of RA 7394 of the Consumer Protection act and Article 292 of the Revised Penal Code), however, these laws are rarely cited for enforcement.

SMEs should take internal steps to protect any trade secrets by inserting confidentiality clauses into employee contracts, internally restricting access to sensitive information, and ensuring that confidential information is only revealed on a need-to-know basis. Given that laws on trade secrets are rarely brought to court in the Philippines, in the event that a criminal case is filed for violation of these laws, the Regional Trial Courts (RTC) the highest trial courts in the Philippines are unlikely to be familiar with this issue.

In practice, parties tend to stipulate contractual obligations on trade secrets and, in the case of violations, resort to civil action for breach of contract and damages.

(viii) Singapore

Trade secrets are protected under Singaporean law. They must however, be confidential and not widely available to the public. You must also be able to clearly demonstrate an obligation of confidence towards third parties, for example, by signing nondisclosure agreements or having a confidentiality clause included within agreements with other parties.

Another useful tool to be aware of is the Singapore Misuse of Computer Act. The relatively wide definition of computer misuse makes it an offence if a person gains unauthorised access to the employer's computers to retrieve or download information.

The Computer Misuse Act is relevant to the protection of trade secrets as most confidential information now tends to be stored in company computers. Complaints under the Misuse of Computer Act are often a cheap and effective way of protecting trade secrets since investigation and prosecution are carried out by the police and state prosecutor. The employer's only outlay might be in engaging a local consultant to undertake computer forensics in order to collect any evidence deemed relevant in order for the police to take the case further.

(ix) Thailand

The protection of trade secrets was incorporated into Thai law in 2002, and is currently under review by the Thai Parliament. As trade secrets are classified as 'unregistered rights', there is no formal registration system. Trade secrets can be voluntarily recorded with the Thai Department of Intellectual Property (DIP).

Only basic information is required for this and efficient recording strategies can be set up without actually disclosing essential contents of the trade secret. Recording with the DIP can be advantageous as it provides clear evidence in any possible legal dispute.

Thai law does not yet grant data 'exclusivity', which would guarantee additional market protection for originator pharmaceutical companies. This means that authorities in Thailand, such as health authorities or generic drug applicants, are not prohibited from using data to approve generic versions of the original product.

(x) Vietnam

Trade secrets are protected upon creation without any registration, provided that reasonable measures have been taken to ensure secrecy. It is worth noting that, as trade secrets are a relatively new addition to Vietnamese IP law, the authorities have not dealt with many infringement cases relating to trade secrets.

The following information may not be protected as trade secrets: 1) personal status secrets; 2) state management secrets; 3) other confidential information which is not relevant to business.

For more information on the protection of trade secrets in any South-East Asia country, please contact our free confidential helpline on *question@southeastasia-iprhelpdesk.eu or +84 8 3825 8116.*

9. SME Case Studies

Case Study 1: Tracking electronic data in Singapore

In 2010, several relationship managers of a bank in Singapore left en masse to a rival bank. Prior to leaving the bank, they emailed data from the bank's computer system to their own personal email accounts; they also accessed and printed confidential company data. These employees were subsequently charged in a Singaporean court for the unauthorised access of confidential client data. While the practice of poaching customers from a former employer is prevalent in this area of business, these bank employees may have been unaware of the gravity of their actions. It is much more difficult to cover one's tracks when information accessed by such means can easily be gathered from system logs. Recent advances in computer forensics have made it easier to retrieve deleted files at the operator terminal end. Prior to this case, two lawyers were also fined for downloading legal document (precedents) from a former employer's computer system.

Case Study 2: Inexperience of Indonesian courts with trade secret cases

In contrast, Indonesian courts seem to be less comfortable with the protection of trade secrets. This could be due to the fact that they are indoctrinated with the notion that IP rights ought to be registered in order to be recognised and protectable. The following case demonstrates how Indonesian courts struggle with the protection of trade secrets.

In an on-going case, an engineering firm filed a claim against a large construction company in Indonesia and several other parties for the misuse of its secret know-how in boiler construction. PT Basuki claimed that its secret boiler design know-how was used by the defendant to develop similar products. PT Basuki's claim was summarily dismissed by the Bekasi District Court. The judges reasoned that the Commercial Court rather than the District Court ought to have jurisdiction over the case because the case concerned intellectual property, and the Commercial Court had previously heard a related industrial design case between the same parties. However, the Supreme Court upheld the plaintiff's appeal against the case dismissal. The case was sent back to the Bekasi court to be retried and is still on-going.

The Supreme Court ruling confirms what the law has already stipulated the case was correctly brought before the district court in Bekasi. The initial rejection of the case by the District Court was incorrect and can only be explained by their difficulty with, and lack of experience in, handling trade secret issues. This is a common problem in developing IP jurisdictions in South-East Asia countries where trade secret issues are seldom brought before the courts despite the fact that the law may provide for it.

The new Indonesian Electronic and Information Technology Law also contains provisions against unauthorised access to computer systems. However, an actual application of these provisions has yet to be seen.

Case Study 3: Trade Secrets protection in Thailand

Important amounts of investment are made in research and development to improve designs, techniques, and processes by SMEs to reduce production costs and increase sales. Trade secrets disputes often arise against employees or former employees and business partners and is a frequent issue affecting SMEs. However, in relation to Thailand, the Central Intellectual Property and International Trade Court (IP&IT Court), has published that only 66 trade secret cases were brought to the IP&IT Court between 2004 and 2014. Of this limited number of cases, the majority had unfortunately no positive outcome for trade secrets' owners, with the main reason for the court to dismiss a plaintiff's claim, being the absence of appropriate measures to maintain trade secrets. Key grounds to support a claim of trade secrets theft is indeed represented by the proofs of the existence of a trade secret by demonstrating that the information is protected by measures to maintain its secrecy. Failing to provide certain evidence in this respect, will lead to lose the case.

For example, in Supreme Court Judgment 10217/2553, the Court determined that a general non-disclosure and non-compete clause inserted in an employment agreement was not an appropriate measure to maintain the secrecy of the trade information, and it consequently dismissed the plaintiff's claim. There are several other Supreme Court decisions in which plaintiffs' claims have been dismissed for a similar reason. In fact, it was not possible to prove which specific documents containing trade secrets where subject to confidentiality.

On the other hand, records shows that if a trade secret owner is able to demonstrate that appropriate measures were taken to maintain secrecy over a trade secret, the IP&IT Court is more likely to render a decision in its favor including payment of damages.

10. Take-Away Messages

- **Prevention is the key to protection.** More often than not, once a trade secret is disclosed, the damage is already done, and it is often very difficult to recover its value, even if you succeed in litigation.
- **Establish an internal management system for trade secrets.** Training and clear written guidelines are essential. As your employees may not have the same understanding of proprietary information and intellectual property rights as you might have, it is important to educate them on what can or cannot be disclosed. Adopt appropriate measures to mark and store confidential documents whether such documents are in electronic or paper format.
- **Put in place appropriate measures to keep secrecy and confidentiality.** Make sure that you will put in place appropriate measures to keep secrecy and confidentiality of your information and that you will be able to unequivocally prove that those measure have been breached by your employees, former employees or business partners.
- **Require all employees to sign an employment agreement with strict confidentiality provisions.** To win a theft of trade secrets claim, you must show that the information stolen is (1) not publicly known, (2) has commercial value, and (3) that you took measures to keep it secret. When a current or former employee steals your trade secrets, having an employment agreement with confidentiality provisions is essential to show that you took measures to keep it secret.
- It is very important for businesses to familiarise themselves with the relevant laws in relation to trade secrets in the countries where they are operating or trading in. Know the local rules and consult with local experts would increase the possibility of SMEs to take IP informed decisions in relation to the protection of their trade secrets.

11. Your Trade Secret Checklist

(i) Identify and catalogue your trade secrets.
(ii) Use a combination of physical, technical, and contractual barriers.
(iii) Document trade secret protection measures you take, in case of a dispute later on.
(iv) Implement a trade secret protection policy within your company, making sure your employees understand your expectations.
(v) Consider non-disclosure agreements (NDAs) before entering negotiations with third parties.

EA-03-19-406-EN-N

Free South-East Asia IP advice for European SMEs

> **For more information and to discuss how we can work together, please contact us:**

Tel: +84 28 3825 8116 | Tel: +32 2 663 30 51
Email: question@southeastasia-iprhelpdesk.eu
Online: www.ipr-hub.eu

> **If you have a question about protecting intellectual property in any South-East Asia country, please contact our free confidential helpline at:**

question@southeastasia-iprhelpdesk.eu

Download guide:

A initiative of the European Commission

European Commission

Project implemented by:

PRACSIS PUBLIC RELATIONS COMMUNICATION STRATEGY SPRL

EURICE EUROPEAN RESEARCH AND PROJECT OFFICE GMBH

spi Sociedade Portuguesa de Inovação

EUROCHAM European Chamber of Commerce in Vietnam

ISBN 978-92-9202-511-3
doi:10.2826/421648