



**“REASONABLE STEPS”
TO PROTECT TRADE SECRETS:
Leading Practices in an Evolving Legal Landscape**

AN INTRODUCTION

Every company has trade secrets. For some, these could include customer lists, product strategies or confidential trading information. For others, it could be a formula or sophisticated and complex methodology to make an advanced technology product. For all, trade secrets can represent the lifeblood of an organization, crucial to its ability to sell products, gain competitive advantage and enjoy a reputation of innovation.

By their very nature, trade secrets are ‘secret’ and are not protected in the same way as traditional forms of intellectual property. When there is misappropriation, a company must prove that it has taken “reasonable steps” to prevent trade secret theft or misuse.

In this whitepaper, we review the “reasonable steps” requirement for protecting trade secrets. We look at international, regional and national laws and legislation; consider the types of protections that companies have implemented; and look at court cases that examine “reasonable steps” taken by companies. Finally, this whitepaper provides examples of practical steps that companies can take to put protections in place in the eight categories of an effective trade secret protection program.

The Center for Responsible Enterprise And Trade (CREATe.org) is dedicated to helping companies and their third parties protect intellectual property (IP) and prevent corruption. In our work with companies around the world, we continue to see companies – from the largest, most mature corporations to fast moving start-ups – grappling with how best to manage and protect their trade secrets.

To help guide companies on this issue, we have undertaken this research to present in a concise way how courts are addressing the issue and the law is evolving. Our aim is to help companies to protect their proprietary information more effectively and to enforce their rights more successfully, in order to benefit fully from their trade secrets. Our work has provided us the opportunity to see what is working inside of companies – and importantly, what is not – and we provide in this whitepaper our insights into practical, scalable, cost effective practices that can help companies manage and protect their trade secrets.

This whitepaper builds on CREATe’s other reports on trade secrets. The first addressed the risks associated with working with third parties: Trade Secret Theft: Managing the Growing Threat in Supply Chains (May 2012). The second, a report developed in partnership with PricewaterhouseCoopers (PwC), described how companies can identify, assess and secure trade secrets. It is titled: Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats (February 2014).

All of this work has informed our development of CREATe Leading Practices for Trade Secret Protection, a three-step comprehensive service that includes an online assessment, independent evaluation by CREATe experts, tailored recommendations and a guide to maturing your practices.

To learn more about CREATe, please visit www.CREATe.org.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

I. THE RELEVANCE OF “REASONABLE STEPS” IN PROTECTING TRADE SECRETS

A. TAKING REASONABLE STEPS TO PROTECT TRADE SECRETS TO MAINTAIN REVENUES, COMPETITIVENESS AND REPUTATION

B. INTERNATIONAL AND NATIONAL LAWS REQUIRING COMPANIES TO TAKE “REASONABLE STEPS” TO PROTECT TRADE SECRETS

1. THE TRIPS REQUIREMENT

2. U.S. LEGISLATION

3. COUNTRIES WITH EXISTING “REASONABLE STEPS” REQUIREMENTS

4. PROPOSED EU DIRECTIVE

5. MORE SPECIFIC PROTECTION EFFORTS REQUIRED IN SOME COUNTRIES

6. RELEVANCE OF “REASONABLE STEPS” UNDER OTHER LEGAL REGIMES

II. EXAMPLES OF “REASONABLE STEPS” AND LEADING PRACTICES

A. POLICIES, PROCEDURES AND RECORDS

B. SECURITY AND CONFIDENTIALITY MANAGEMENT

C. RISK MANAGEMENT

D. THIRD PARTY MANAGEMENT

E. INFORMATION PROTECTION TEAM

F. TRAINING AND CAPACITY BUILDING

G. MONITORING AND MEASUREMENT

H. CORRECTIVE ACTIONS AND IMPROVEMENTS

CONCLUSION



EXECUTIVE SUMMARY

Protecting companies' confidential business and technical information – “trade secrets” – is becoming a major priority of the private sector and governments around the world. Trade secrets and other intellectual property and intangible assets represent the bulk of the overall value of many companies. Given the pervasive use of information technology and worldwide supply chains, and the relentless physical and internet exchange of data in every business sector, protecting trade secrets against unauthorized disclosure and use has taken on a vital importance for many companies wanting to protect their business and market value, maintain their reputation, and keep their competitive edge.

International, regional and national trade secrets laws are increasingly focusing on the steps that companies themselves should take to protect their confidential and proprietary information. The definition of a trade secret in the controlling international treaty, the WTO Trade-Related Aspects of Intellectual Property Rights Agreement, and in many countries' national and even state laws, requires that the owner or other controller undertake “reasonable steps” or “reasonable efforts” to protect the secrecy of its information. A “reasonable steps” requirement is also included in the draft EU Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) which, if adopted, would become part of the national legislation in all 28 EU member countries. New legislation proposed at the national level in the U.S. likewise has contained similar requirements.

Aside from the practical usefulness of implementing “reasonable steps” to prevent trade secret theft and misuse, taking such steps can also have crucial legal significance. Where the legal definition of trade secrets includes a “reasonable steps” or similar requirement, a court can find that a company's information is not a trade secret if such

steps are not taken. Failing to take adequate precautions to protect such information can preclude a company from getting any legal redress if the worst happens and an unauthorized disclosure or use of the information takes place.

This whitepaper reviews the evolution and significance of the “reasonable steps” requirement for protecting trade secrets. It also reviews the protections that companies have implemented and that courts in the U.S. and some other countries have examined (and that some national laws have specifically mandated) as “reasonable steps” by the owner or other controller to protect its proprietary information. These examples are organized into eight categories of different protections that companies can implement. The discussion in each category concludes with a checklist of leading practices that companies can use to review and implement their own “reasonable steps” for protecting trade secrets.

I. THE RELEVANCE OF “REASONABLE STEPS” IN PROTECTING TRADE SECRETS

A. TRYING TO PROTECT TRADE SECRETS TO MAINTAIN REVENUES, COMPETITIVENESS AND REPUTATION

In an era when up to 75% of the value of the U.S. Fortune 500 companies is attributable to intangible assets¹ including intellectual property (IP) and trade secrets, protection of such proprietary technical and business information has become an important way to help companies innovate and compete. One only must think about the formula of Coca Cola or the liqueur Chartreuse, the search algorithms and other technical information of companies like Google and Facebook, and the know-how and formulation of Michelin rally tires and many other advanced products, to realize the significance of trade secrets for many companies.

Because trade secrets have such a significant value, they have become a growing target for theft and unauthorized use. A 2013 report by the Commission on the Theft of American Intellectual Property, an independent U.S. research group, estimated that the U.S. economy suffers about \$300 billion in losses annually from trade secret misappropriation.² This Commission concluded that previous assessments of losses had underestimated the true extent of IP and trade secret theft.

A more recent study conducted by PricewaterhouseCoopers (PwC) and the Center for Responsible Enterprise And Trade (CREATe.org) estimated that the value of trade secret theft in the U.S. is approximately 1% - 3% of the U.S. gross domestic product (GDP).³ The report assessed private sector research and development expenditures, and data on other illicit economic activity (including narcotics trafficking, tax evasion and corruption), as proxies for determining the estimated level of trade secret theft. Using such

proxy measures together provided a useful context for the scale of trade secret theft and its relative impact on the U.S. economy.

Trade secret theft and misuse take place for several different reasons, and are carried out by a range of different “threat actors,” including competitors, malicious insiders, organized criminals, “hacktivists” and even nation states.⁴ Although “there is little statistical analysis on trade secrets,”⁵ one of the rare statistical studies that has been done in the U.S. found that “in over 85% of trade secret cases, the alleged misappropriator was someone the trade secret owner knew – either an employee or a business partner.”⁶


Theft and misuse of trade secrets can have devastating effects on a company’s earnings, competitiveness and reputation. High visibility cases of hacking of major companies’ computer networks and theft of competitive data are now reported in the press regularly. This has led to public acknowledgements by companies in their U.S. securities filings that IT security issues, including the possible loss of trade secrets and other proprietary information, are corporate risks that could seriously affect their business.⁷

The Ford Motor Company in its February 2014 10-K filing with the U.S. Securities and Exchange Commission, listed cybertheft of trade secrets as one of its material “risk factors:”

“[C]yber incidents could materially disrupt operational systems; result in loss of trade secrets or other proprietary or competitively sensitive information; compromise personally identifiable information of customers, employees, or others; jeopardize the security of our facilities; and/or affect the performance of in-vehicle systems... an incident could harm our reputation and subject us to regulatory actions or litigation.”⁸

B. INTERNATIONAL AND NATIONAL LAWS REQUIRING COMPANIES TO TAKE “REASONABLE STEPS” TO PROTECT TRADE SECRETS

Trying to protect a company’s trade secrets is also necessary for such confidential and proprietary information to qualify for legal protection under the controlling international trade treaty, under U.S. state and federal legislation, and under the laws of many other countries, and would be required under new legislative proposals under consideration in the U.S. and the EU.



“Theft and misuse of trade secrets can have devastating effects on a company’s earnings, competitiveness and reputation.”

1. THE TRIPS REQUIREMENT

The 1996 World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) was the first international treaty to protect trade secrets and other undisclosed information explicitly. TRIP defines protection of such information as protection against unfair competition,⁹ and requires this be implemented in the laws of all WTO members 161 countries.

TRIPs mandates that companies or individuals that control qualifying information should be protected from unauthorized disclosure, acquisition or use “in a manner contrary to honest commercial practices,” where such information:

- (a) is secret in the sense it is not, as a body or in the precise configuration and assembly of its components known among or readily accessible to persons within the circles that normally deal with the 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.¹⁰

2. U.S. LEGISLATION

The element of “reasonable steps to keep the information secret” is implemented verbatim or in substantially similar terms in the trade secrets laws of several countries. This requirement was derived from model legislation developed for implementation by U.S. states, the Uniform Trade Secrets Act (UTSA), which was drafted by a legal experts group called the National Conference of Commissioners of Uniform State Laws in the 1970s.¹¹ The USTA provided a useful template, which most U.S. states have used to develop their trade secret laws and sanctions.

The USTA specifically includes in the definition of a trade secret the requirement that it be “the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”¹² 48 states and the District of Columbia have enacted a version of the UTSA containing this definition,¹³ making “reasonable efforts” an element to be proved in virtually any trade secrets litigation in the U.S.

Trade secrets protection in the U.S. is still governed primarily by state laws modeled on the UTSA. However, the increasing value of trade secrets to the economy encouraged the U.S. Congress to enact the Economic Espionage Act of 1996 (EEA),¹⁴ which made intentional or knowing theft of a trade secret – for the benefit of a foreign entity or anyone else beside the owner – a federal crime. The definition of trade secrets in the EEA requires that the owner “has taken reasonable measures to keep such information secret.”¹⁵

The case law of the U.S. International Trade Commission has also developed to interpret its controlling statute (which gives it authority to address “unfair methods of competition and unfair acts in the importation of articles ... into the United States”¹⁶) to allow federal import bans on articles produced in violation of a company’s trade secrets.¹⁷ These cases have used state UTSA and common law definitions of trade secrets that require the owner to take “reasonable efforts” to protect its trade secrets.¹⁸

In recent years, the U.S. Congress has been considering whether to adopt legislation to give trade secret owners a full federal civil cause of action against trade secret theft. The proposals under consideration so far would not pre-empt state trade secrets claims, but provide an alternative or parallel right of action for companies wishing to address in a single federal court case any trade secret misappropriation that occurs or has effects in more than one state.¹⁹

Two such bills were considered in the last session of Congress.²⁰ Each of these would have inserted a federal civil cause of action into the EEA, incorporating the EEA’s existing definition of trade secrets including its “reasonable efforts” requirement.²¹

3. COUNTRIES WITH EXISTING “REASONABLE STEPS” REQUIREMENTS

In Europe, the “reasonable steps” requirement is included already in the national legislation of Latvia,²² Lithuania,²³ and Romania,²⁴ and courts have read into Belgium’s more general manufacturing-secrets law a requirement that a litigant claiming misappropriation of a trade secret must establish the “adoption of reasonable steps to keep it secret” in order to commence proceedings under the Criminal Code.²⁵

Quite a few other countries have enacted trade secrets legislation that specifically requires that the owner or other controller of the information undertake “reasonable steps” to keep the information secret. Countries as diverse as Costa Rica,²⁶ El Salvador,²⁷ Ghana,²⁸ Indonesia,²⁹ Jordan,³⁰ Mauritius,³¹ Panama,³² Saudi Arabia,³³ Qatar,³⁴ Thailand,³⁵ Tonga,³⁶ Trinidad & Tobago,³⁷ and Vanuatu³⁸ include such a requirement in their definition of trade secrets.

In China, the 1993 Anti-Unfair Competition Law similarly defines a trade secret as technical or business information that is unknown to the public, can bring economic benefits to the owner, has practical utility, which the *trade secret owner has adopted measures to protect its confidentiality*.³⁹ There has been more trade secrets litigation in China recently, brought by such companies as Eli Lilly, General Motors, E.I. du Pont, Corning and American Superconductor.⁴⁰

4. PROPOSED EU DIRECTIVE

The EU is considering a new Directive to protect trade secrets in a more harmonized way throughout Europe.⁴¹ The draft Directive on Protection of Undisclosed Know-How and Business Information (Trade Secrets)⁴² would adopt a definition of trade secrets that includes a “reasonable steps” requirement, based on the TRIPs Agreement formulation and similar to the laws of the countries described above:

- (1) ‘trade secret’ means information that meets all of the following requirements:
 - (a) is secret in the sense it is not, as a body or in the precise configuration and assembly of its components known among or readily accessible to persons within the circles that normally deal with the information in question;
 - (b) has commercial value because it is secret;
 - (c) *has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.*⁴³

The EU member state governments agreed on a draft of this directive with the European Commission in May 2014.⁴⁴ Various committees of the European Parliament are preparing reports and proposed amendments to this proposal. If these differ from the member states’ “common position,” the Parliament, member states and Commission will engage in a reconciliation process to come up with a final text that can be agreed to by all of these institutions.

A bill was also introduced in the France National Assembly in late 2014 (the proposed Project de loi Macron⁴⁵) that would have protected certain business secrets (*secret des affaires*) that had been the subject of “reasonable measures of protection” (*mesures de protection raisonnables*) to preserve their nonpublic character.⁴⁶ (These provisions were removed from the bill in early 2015.)

5. MORE PROTECTION EFFORTS REQUIRED IN SOME COUNTRIES

A few other countries, notably Russia and Japan, have specified in their legislation or in case law more detailed lists of protection measures that the owner or controller of information must implement for that information to qualify for legal protection as a trade secret.

In Russia, the possessor of such information must implement a “regime” of trade secrecy, which must include defining a list of information constituting commercial secrets, limiting access to that information by establishing a procedure for handling the information and for control over compliance with that

procedure, keeping a record of persons who acquired access and/or to whom that information was furnished or transferred, regulating use by employees on the basis of labor and civil law contracts, and affixing a “commercial secret” stamp specifying the holder of that information.⁴⁷

Japanese law defines trade secrets as “technical or business information useful for commercial activities such as manufacturing or marketing methods that *is kept secret* and that is not publicly known.”⁴⁸ This has proved to be “a much more stringent” standard of secrecy than the more general “reasonable steps” requirement elsewhere. Among other requirements that Japanese courts have read into this standard are that trade secret holders must limit the number of people with access to the information, give clear notice that the subject is secret, and implement physical and electronic access restrictions.⁴⁹

6. RELEVANCE OF “REASONABLE STEPS” UNDER OTHER LEGAL REGIMES

Even in countries that have no specific requirement that the holder of a trade secret undertake reasonable or other particular steps to protect such information, this issue can also arise in other contexts in trade secrets litigation – particularly regarding questions whether the information is actually confidential and under what conditions it has been disclosed.

The United Kingdom and other Commonwealth countries including Canada, Australia, New Zealand, and India, protect proprietary information under the “law of confidence,” which has developed under the common law to protect a broad category of information from a “breach of confidence.” Someone who receives another person’s information cannot use or disclose that information without authorization, if the information has the “necessary quality of confidence about it,” and if the circumstances in which it was acquired or received evidence an objective knowledge or notice that the information was confidential.⁵⁰ The courts in these countries look primarily at evidence on the nature of the information itself, and the facts and circumstances surrounding its initial communication.

Even under this formulation, however, one of the categories of evidence for determining whether sufficient knowledge or notice of confidentiality existed is “the steps taken to preserve or emphasize the secrecy of the information.”⁵¹ As one of the leading cases on the subject in the Commonwealth explained, “If the confider takes strenuous precautions to preserve the confidentiality of information, it is to be expected that the confidant ought to have known that the information was confidential.”⁵²



II. EXAMPLES OF “REASONABLE STEPS” AND LEADING PRACTICES

Companies all over the world have recognized that putting a variety of measures in place to protect trade secrets within their company and among their supply chain and other third parties is necessary to keep their trade secrets from being stolen and misused. To date, companies have implemented various types of protections for their trade secrets, with varying degrees of consistency, comprehensiveness and ongoing oversight.

Reviewing and improving information technology (IT) and physical security, and other systems and practices for protecting trade secrets and other proprietary company data, has now become a high priority for many companies – particularly in light of recent high-profile cyberthefts of corporate data. As the *New York Times* succinctly put it: “Companies across the globe are on high alert to tighten up network security to avoid being the next company brought to its knees by hackers like those that executed the dramatic cyberattack against Sony Pictures Entertainment.”⁵³

The following sections discuss a variety of measures that companies and individuals have put in place to protect their trade secrets, and that courts have examined or that legislation has specifically mentioned as evidence of “reasonable steps” to protect that information. These protections are classified according to the eight categories of leading practices that CREATE.org has developed as part of its systematic and comprehensive approach for evaluating the business processes needed to protect intellectual property and trade secrets specifically.⁵⁴

These measures range from the policies, procedures and agreements and other records needed to establish and document protection; to physical and electronic security and confidentiality measures; to risk-assessment efforts to identify and prioritize trade secret risks; to due diligence and other ongoing third party management; to management oversight and coordination, employee and supplier training, monitoring and measurement, and corrective actions and improvements.

The discussion in each category concludes with a checklist of leading practices that companies may find useful in developing and implementing their own “reasonable steps” to protect trade secrets.

CREATe LEADING PRACTICES FOR TRADE SECRET PROTECTION

Policies, Procedures and Records

Security and Confidentiality Management

Risk Assessment

Third Party Management

Information Protection Team

Training and Capacity Building

Monitoring and Measurement

Corrective Actions and Improvements

A. POLICIES, PROCEDURES AND RECORDS

The policies and procedures that a company has for protecting its trade secrets, including rules and processes for designating, managing and disclosing trade secrets, are vital. The contracts and other documentation that the company uses to implement trade secrets protection in legally binding ways on employees, third parties and others, are also among the most important ways that companies seek to protect their trade secrets.

Nondisclosure and other agreements have been regularly examined in court cases as evidence of “reasonable measures” to protect trade secrets. In *Aetna, Inc. v. Fluegel*, in which Aetna sought to prevent a former high-level employee with access to Aetna’s strategic plans from using Aetna’s confidential information in working for a

competitor, the court noted with approval Aetna’s nondisclosure agreements and related secrecy efforts with its employees: “Aetna ... goes to great lengths to protect its trade secrets. Aetna employees must annually review and agree to nondisclosure requirements. Aetna’s high-level employees, including [the defendant], must sign a non-solicitation, confidentiality and nondisclosure agreement. Aetna marks all appropriate documents as confidential and uses technology including password protection and encryption to limit access to confidential information to only key employees.”⁵⁵

One of the few statistical studies done on trade secrets litigation in the U.S. has found that a court is almost 25 times more likely to find that a trade secret owner has engaged in “reasonable efforts” if it has such agreements with employees that ultimately become the target of trade secret litigation, than if it does not.⁵⁶ Under Commonwealth legal systems, an employee nondisclosure agreement can provide a separate legal basis for addressing trade secret misappropriation under contract law, besides common-law breach of confidence claims.⁵⁷

Courts have also mentioned companies’ overall **corporate policies** for maintaining confidentiality as evidence of “reasonable measures” for protecting trade secrets. Company-wide policies for maintaining confidentiality have been considered as reasonable steps for protecting such diverse information as automotive tire designs,⁵⁸ customer lists,⁵⁹ and pharmaceutical formulas.⁶⁰ A specialty pharmaceutical and medical device company that had no policy or procedures concerning trade secrets or confidential information and that had never asked an employee it later sued to return company information known to be on his home computer, failed in its attempt to have a court determine that the employee had misappropriated a trade secret.⁶¹

Companies also regularly adopt **procedures** to implement particular aspects of their confidentiality policies, such as procedures for marking sensitive documents as confidential,⁶² for conducting exit interviews and seeking return of sensitive materials when employees leave the company,⁶³ or for dividing a collection of confidential information or a confidential process into discrete parts in such a way that no one employee or vendor has access to the whole.⁶⁴

Not that smaller companies necessarily must implement as extensive or as costly policies, procedures and records as large companies. Courts have recognized that what efforts are “reasonable” may look different at a smaller company. One court found, that a small family-run cheese production business had taken sufficient efforts to protect the secrecy of its formula, methods of production, sales to selected customers and other business-related information by limiting access to that collection of information to the family itself

and its outside accountant.⁶⁵

However, when policies, procedures and records have not been implemented adequately or followed consistently, courts have not been reluctant to declare that the company has not engaged in “reasonable steps” sufficient to treat the information as a trade secret. The PatientPoint health-information service brought legal action to prevent a terminated employee from using competitive, sponsor and other information he had access to during his employment. However, the court found that PatientPoint’s policies, procedures and records were inadequate to protect these as trade secrets:

- No non-compete or nondisclosure agreements were requested until a year after the employee began work, and none were requested for other employees.
- The company made an oral request for the employee to return the employee’s company-issued laptop and iPad upon termination, but did not demand the return of these items again until 6 months later.
- The company waited until 6 months after termination to request return of other proprietary information.
- The company accepted a separation agreement with the employee that had no non-compete or nondisclosure provisions. (The original draft separation agreement contained these provisions, but the employee had refused to sign it, and the company accepted a revised version without these provisions.)⁶⁶

▶ LEADING PRACTICES FOR POLICIES, PROCEDURES

AND RECORDS. CREATE.org recommends that companies implement “reasonable steps” to protect trade secrets by implementing company policies, developing procedures to ensure that policies are followed, and keeping records to document protections and compliance. These may include steps in the following areas:

❑ COMPANY, STAFF AND THIRD-PARTY POLICIES.

Develop an overall set of company-wide policies for protection of trade secrets internally and with key third parties, such as the company’s supply chain. (CREATE has prepared a set of model policies for reference.⁶⁷)

❑ TRADE SECRETS PROCEDURES.

Develop procedures for how trade secrets are to be managed in areas relevant to the company. These may include procedures in such areas as employee hiring and termination, trade secrets handling and disclosure, and company computer and personal device usage.

❑ **MARKING AND SEGREGATION PROCEDURES.** Develop procedures for marking, segregation, and storage of trade secrets.

❑ **STANDARD CONFIDENTIALITY AND USAGE PROVISIONS.** Develop and use standard confidentiality clauses in all employee, contractor, and supplier and other relevant third-party agreements.

❑ **STANDARD NDA.** Develop a standard nondisclosure agreement and use it when disclosure of trade secrets is authorized.

❑ **INVENTORY AND OTHER DOCUMENTATION.** Keep written records of all trade secret related activity, including usage, disclosure, and management.

B. SECURITY AND CONFIDENTIALITY MANAGEMENT

Particularly given the current spate of cyberattacks and other headline news involving the theft of corporate information, effective management of a company’s physical and electronic security is important for ensuring that the company is taking “reasonable steps” to protect its trade secrets. Not only courts but also new government regulations are increasingly insisting upon adequate protection measures in these areas.

On physical security measures, one court found that the Valco company had shown that it tried to protect its proprietary materials and manufacturing processes for its valve and glue applicator head in light of testimony:

that Valco’s plant had more than adequate locking devices; there was a receptionist who screened every visitor to the building; that a buzzer lock system on the door to the processing area was operated by the receptionist; that the general public was never taken through the plant; that competitors were never authorized within the plant; that Valco’s drawings were provided to their suppliers only to bid on, or manufacture of certain parts; that the drawings were provided only to the employees with a specific need for them; that all drawings which left the Valco plant had to have a proprietary marking restricting the use and disclosure thereof; and that a shredder was utilized to destroy all computer printouts and old pricing sheets.⁶⁸

It should be noted again here that security and confidentiality management steps need only be “reasonable” under the circumstances to satisfy this element of the definition of a trade secret. The DuPont chemical company was not required

to camouflage its secret process plant against aerial photography during its construction.⁶⁹

Companies increasingly are implementing and using a whole variety of information and other electronic security measures as an important part of their overall programs to protect trade secrets.⁷⁰ When the U.S. government attempted to prosecute a former computer programmer who had worked on developing and improving investment bank Goldman Sachs's proprietary high-frequency trading platform, the trial court noted with approval the multiple electronic-security systems that Goldman had in place to protect this information. These included maintaining a firewall, monitoring employee use of internet sites, blocking access to certain websites, implementing pop-up banners that advised employees logging in to their computers of acceptable and prohibited uses, restricting access to firm computers, and restricting use of USB flash drives to only a few employees with administrative access.⁷¹

In Japan, courts have also examined the information security steps taken by a company in determining whether particular information has been "kept secret." Courts have found that a company must "implement physical and electronic access restrictions" for information to be deemed "kept secret" and protected by Japan's unfair competition rules for trade secrets.⁷²

Governments are increasingly requiring companies to implement electronic security measures of the sort needed to protect trade secrets, as part of broader data security requirements. In Canada, written policies, practices and procedures as part of an "information governance" structure are a key factor considered by national regulatory authorities for determining, in investigations of security breach incidents, whether the organization established reasonable safeguards as required by applicable privacy legislation.⁷³

► **LEADING PRACTICES FOR SECURITY AND CONFIDENTIALITY MANAGEMENT.** CREATE.org recommends that companies consider the following leading practices in implementing their "reasonable steps" to protect trade secrets in security and confidentiality management. These include actions such as incorporating confidential information protection into physical and IT security system planning, implementing system access restrictions, and conducting ongoing assessment and improvement of security.

❑ **OBJECTIVE OF SECURITY SYSTEMS.**

Ensure that protection of the company's most important confidential and proprietary information is one of the objectives used in the design and operation of its physical and IT security systems.

❑ **"NEED TO KNOW" ACCESS.** Segregate and restrict physical and IT system access to confidential and proprietary information only to those persons, groups or departments with a "need to know."

❑ **GUARDS, ID CARDS, OTHER PHYSICAL SECURITY.** Use security guards, ID cards, appropriate surveillance, sign-outs and other physical security mechanisms to restrict and log access to authorized personnel.

❑ **RESTRICTED VISIBILITY AND REMOVAL.** Ensure that confidential materials are not left unattended, posted on blackboards or whiteboards, recycled in unshredded form, or otherwise easily seen or removed by visitors or other unauthorized persons.

❑ **SECURE IT PERIMETERS AND LOGINS.** Use firewalls and secure password logins.

❑ **TECHNICAL MEASURES.** Use technical measures such as encryption, email restrictions, anti-virus and anti-malware software, and electronic "red flags" to limit access, copying and distribution of confidential and proprietary information.

❑ **SECURITY STANDARDS.** Consider implementation of particular IT security standards (e.g. ISO 27001, COBIT, NIST Framework), and ensure that protection of trade secrets is specifically designed into the system.

❑ **RESPONSE AND MONITORING.** Respond rapidly to breaches using a pre-determined rapid-response plan, and routinely monitor and review IT systems for security and compliance with the company's use and confidentiality requirements.

C. RISK MANAGEMENT

The scope and quality of a company's risk assessment and risk management-related efforts can be an important element in identifying, prioritizing and implementing protections for its trade secrets.⁷⁴ Enterprise risk management (ERM) as it does in other areas of corporate risk, typically begins with identifying the items at risk – here, the proprietary information that a company deems its valuable trade secrets. This step can usefully involve developing an inventory or registry of trade secrets.

Courts have looked at whether companies have included particular material in an internal trade secrets registry as

evidence of whether that material was confidential and whether “reasonable efforts” were taken to maintain that confidentiality. In a classic case from 1991, electronics firm Texas Instruments (TI) brought a case against two former researchers that had worked on TI’s pioneering efforts in speech recognition, but had left the company to join a competitor of TI in this field. Each had copied all of the computer directories to which they had access at TI, which included the speech-recognition programs that TI claimed as trade secrets. In convicting the ex-employees of criminal trade secret theft, the court mentioned the inclusion of this information in TI’s trade secret registry among a long list of other “reasonable efforts” that TI had taken, as evidence that TI’s speech-recognition software was protectable: “Significantly, the basic programs from which the items in question were derived were, in fact, listed in the Trade Secret Register kept by the complainant.”⁷⁵

Maintaining a trade secret registry is also one of several elements specifically required by Russian commercial secrecy law for a company to be given trade secrets protection.⁷⁶ Some companies’ failure to identify which information they consider to be trade secrets has been evidence that their material should not be protected. In a U.S. federal case, MBL (USA) Corporation tried to claim in court that the tooling, manufacturing methods, know-how and customer lists it used in producing and selling urethane flat belts, timing belts and other products should be protected as trade secrets from alleged misappropriation and disclosure by a former employee. In denying protection, the court found that “defendant and other employees were not told what, if anything, the plaintiff considered confidential.”⁷⁷

▶ LEADING PRACTICES FOR RISK MANAGEMENT.

CREATe.org recommends that companies consider the following leading practices in implementing their “reasonable steps” to protect trade secrets in risk management:

☐ **TRADE SECRET REGISTRY.** Identify the key trade secrets of the company. A registry or other inventory that can be updated over time is ideal.

☐ **ASSESS POTENTIAL RISKS TO TRADE SECRETS.** Assess which trade secrets might be taken, used or disclosed without authorization, why, and by whom. This may include internal personnel, supply chain companies or staff, or other external parties such as competitors, hackers or nation states.

☐ **ASSESSMENT OF LIKELIHOOD AND SEVERITY OF POTENTIAL RISKS.** Assess the likelihood or

probability that the company’s trade secrets will be taken, used or disclosed by any, and what the likely economic or other impact would be if this occurred.

☐ **RISK MITIGATION PLAN.** Rank risks and develop and implement a risk-mitigation plan to address in ways the most important risks the company faces to its trade secrets. Review and update this plan regularly.

D. THIRD PARTY MANAGEMENT

Suppliers, business partners, customers and other key third parties may from time to time have access to a company’s trade secrets for various reasons – to manufacture using proprietary designs, tooling, or know-how; to evaluate business opportunities; or to use the company’s information, products or services in other ways on condition that the third party maintains the confidentiality of the company’s trade secrets.

Suppliers and other third parties are not an unusual source of misappropriation of trade secrets,⁷⁸ and litigation over trade secret theft and misuse by such third parties has often focused on how a company has managed its exchange and management of confidential material with such third parties.

Third party *nondisclosure agreements* with supply chain members including suppliers and customers were crucial for Technicon, the developer of a proprietary hospital medical record computer system, to secure an injunction against former employees and others claimed to be using its information to develop a competing system. In its order, the U.S. state court noted that Technicon successfully protected its source code and other confidential information in its supply chain, by executing nondisclosure agreements with its outsourced manufacturer and relevant customers including the National Institutes of Health.⁷⁹

Such third-party nondisclosure agreements have been one of the most useful pieces of evidence of “reasonable efforts” in trade secrets litigation in the U.S. The statistical study of U.S. litigation mentioned above found that courts are almost 43 times more likely to find that a trade secret owner has engaged in reasonable efforts if it has such agreements with business partners than if it does not.⁸⁰

Although the existence or absence of a written nondisclosure agreement may not, show that “reasonable steps” have or have not been taken,⁸¹ failure to secure such an agreement can prove fatal to a trade secrets claim depending on the other facts of the case. The developer of proprietary paint-sludge removal technology lost control over the secrecy of such technology after sharing equipment and plans with both a major customer (General

Motors) and another equipment manufacturer for potential joint sales, with no agreements restricting its disclosure or use, and with no legends or warnings on the confidentiality of the information. The court refused to impose sanctions on the other equipment manufacturer, which had submitted a complementary piece of equipment to the same end user and allegedly copied several of plaintiff's features.⁸²

► **LEADING PRACTICES FOR THIRD PARTY MANAGEMENT.** CREATE.org recommends that companies implement “reasonable steps” to protect trade secrets in supply chain management through such practices as due diligence, regular communication with supply-chain partners, written agreements and ongoing reviews:

□ **DUE DILIGENCE.** Conduct pre-appointment due diligence on relevant suppliers, business partners, customers and other key third parties. Include potential problems in protecting and managing trade secrets as a part of the due diligence.

□ **THIRD-PARTY COMMUNICATIONS.** Communicate with third parties, up-front and regularly, the company's expectations on their compliance with its policies to protect trade secrets.

□ **WRITTEN NONDISCLOSURE AND OTHER AGREEMENT TERMS.** Ensure that all agreements with supply chain and other third parties are in writing, and cover in adequate detail issues related to the confidentiality, use and protection of trade secrets, and the policies and procedures these parties are expected to follow.

□ **REGULAR REVIEWS.** Include issues of protection of trade secrets in annual or other regular reviews with supply chain and other third-party partners.

E. INFORMATION PROTECTION TEAM

Problems can arise if no one within a company has overall responsibility for protecting the company's trade secrets, or if all of the departments that may deal with trade secrets (legal, finance, compliance, research and development, manufacturing, and supply chain management) do not coordinate their efforts. A cross-functional team responsible for the company's oversight and coordination of trade secret protection can be ideal for this purpose.

Trade secrets litigation cases rarely contain details sufficient to identify when problems in taking “reasonable steps” to keep

information secret have resulted from insufficient management oversight or coordination. However, courts have noted with approval instances where a particular manager has been given the responsibility of apprising subordinates of their duties of secrecy.⁸³

However, the ad hoc way that some companies have been found to protect their trade secrets often points to the likelihood that, essentially, “no one is in charge” of protecting these important assets. A case involving a former employee charged with violating a bookkeeping company's trade secrets in its client lists was dismissed when it turned out that members of the public had had access to names on those client lists. These had been left on the company's reception desk, on employee desks, on computers to which another company in the building had access, on computers where the passwords were left on the desk or shouted across the room, in areas where the public and janitorial staff could see them, and at a social gathering.⁸⁴ The company had failed to take reasonable efforts to protect this information, and no one had responsibility.

► **LEADING PRACTICES FOR INFORMATION PROTECTION TEAM.** CREATE.org recommends that companies consider the following leading practices in implementing their “reasonable steps” to protect trade secrets by coordinating activities through a cross-functional information protection team:

□ **RISK ANALYSIS.** Identify which of the company's departments or groups have dealings with the company's and/or third parties' trade secrets.

□ **RESPONSIBLE EXECUTIVE.** Appoint an appropriate executive from this group as the leader of a team with responsibility for oversight of protecting of IP and particularly trade secrets within the company. (This team may be standalone or have responsibility for other areas of compliance within the company.)

□ **CROSS-FUNCTIONAL COORDINATION.** Appoint people from the other relevant departments and groups as members of the cross-functional team.

□ **AUTHORITY AND BUDGET.** Ensure that this team has senior management support and sufficient resources.

□ **COMPREHENSIVE OVERSIGHT.** Ensure that this team is involved in implementing best practices in all areas relevant to trade secret protection.

F. TRAINING AND CAPACITY BUILDING

Where staff, supply chain partners and other third parties do not know what information they should be protecting and how they should do so, the chances rise that proprietary material may be misused or disclosed without authorization – and indeed, that the company may be deemed not to have exercised “reasonable steps” to protect the information. It is thus important for companies to give relevant staff, suppliers and others with access to the company’s trade secrets initial and ongoing training on what the company’s trade secrets are and how they should protect them. This training may be less formal at smaller companies, but the essential objective here is for employees to understand what material is proprietary and how they should handle it.

In a case involving the theft of documents relating to its work on the U.S. space shuttle program, The Boeing Company had its trade secret protection measures deemed legally adequate despite the fact that the documents were not as such kept under lock and key. The court noted the company’s “training sessions instructing employees not to share documents with outside parties” among the list of other precautions that the court found collectively to constitute “reasonable measures.”⁸⁵

Employees have been found to have been given effective instructions and cautions on the use of trade secrets in various ways at companies as diverse as the Jack Daniel Distillery (with respect to its trade secret whiskey recipe),⁸⁶ and Micro Lithography (with respect to its know-how in the area of optical pellicle technology).⁸⁷ By contrast, the failure of the MBL (USA) Corporation to inform employees “what, if anything, [the company] considered confidential” was one of the key failures that led the court to dismiss MBL’s case against its former employee.⁸⁸

► **LEADING PRACTICES FOR TRAINING AND CAPACITY BUILDING.** CREATE.org recommends that companies implement “reasonable steps” to protect trade secrets by conducting training and capacity building for staff and supply chain partners, with more specialized training for those dealing regularly with trade secrets.

□ **INITIAL STAFF TRAINING.** Ensure that all staff receive information when they start work and when they change roles within the company, as to what the company considers its trade secrets and how they should protect them.

□ **ONGOING TRAINING.** Include protection of trade secrets in annual or other regular staff training on an ongoing basis.

□ **SUPPLY CHAIN TRAINING.** Include protection of trade secrets in annual or other regular training among relevant supply chain members.

□ **SPECIALIZED TRAINING.** Conduct more specialized training on protection of trade secrets as needed among the information protection team and particular groups (e.g. IT) as appropriate.

G. MONITORING AND MEASUREMENT

Trade secrets can be best protected within a company when this is not simply done ad hoc or as a one-time project, but rather when the management systems and processes within the company are used to monitor and measure trade secret protection regularly and over time.

In the case involving Texas Instruments described above, the court noted with approval that the company not only had nondisclosure agreements and plant security policies for keeping printouts and hard copies of confidential data out of sight, but during their nightly security rounds the company’s security personnel also checked whether such data had been left out on desks, and if so, made a security report that the policy had not been followed.⁸⁹

Likewise the previously mentioned case of Aetna, where the court found that nondisclosure agreements were signed once when an employee started and were reviewed and re-signed annually,⁹⁰ is another good example not only of building employee awareness but also of monitoring this important aspect of trade secret protection over time.

► **LEADING PRACTICES FOR MONITORING AND MEASUREMENT.** CREATE.org recommends that companies implement “reasonable steps” to protect trade secrets through ongoing monitoring and measurement of internal and third party protections.

□ **REGULAR REVIEWS OF INTERNAL PROTECTIONS.** Conduct annual or other regular reviews of the company’s program for protecting trade secrets.

□ **REGULAR REVIEWS OF THIRD-PARTY PROTECTIONS.** Conduct annual or other regular reviews of relevant supply chain members’ and/or other relevant third parties’ programs for protecting trade secrets.

BENCHMARKING. Use or develop a benchmarking mechanism for rating the compliance or effectiveness of these programs.

H. CORRECTIVE ACTIONS AND IMPROVEMENTS

The last major category of trade secret protections involves how corrective actions are taken to redress problems that arise. Ideally, corrective action will not simply deal with particular incidents in isolation, but also address root-cause problems such that the company's trade secret protections can improve over time.

Courts have examined the corrective actions that companies have taken against trade secrets breaches as one of the elements taken into consideration in deciding whether the company has taken "reasonable steps" to protect its trade secrets.

For example, the Pre-Paid Legal Services company found that its practice of taking corrective actions against trade secret breaches was helpful in winning its case against former employees and independent contractors that had used the company's employee roster containing contact information, productivity, performance, and other confidential information in order to recruit other Pre-Paid staff to a new company. In finding that Pre-Paid had adequately protected its trade secrets, the court noted, among other things, that the company had made a regular practice of taking action against breaches, sending cease and desist letters and entering into agreed injunctions against former employees that had misappropriated trade secrets.⁹¹

By contrast, biotech company MicroScan lost its trade secret theft claims against rival Alamar and its founder Lancaster (a former MicroScan employee) because MicroScan failed to take any corrective action in a timely way. As the court explained:

In January 1991, MicroScan's management evaluated legal action against Alamar for misappropriation. MicroScan decided not to investigate further, in part because it thought that any secrets stolen were of little value. Over four years later, MicroScan has changed its mind, but this reassessment comes too late...

It is undisputed that MicroScan strongly suspected Lancaster of misappropriating its trade secrets, but did nothing. As discussed above, its suspicions concerning Alamar's use of resazurin arose to the level of knowledge based on strong circumstantial evidence. MicroScan's failure to bring suit, or even approach and warn Lancaster establishes that MicroScan did not take reasonable steps to protect its trade secrets. Summary judgment is appropriate against MicroScan in light of its inactivity

in the face of strong evidence of Alamar's use of what MicroScan now claims were its trade secrets.⁹²

LEADING PRACTICES FOR CORRECTIVE ACTIONS AND IMPROVEMENTS. CREATE.org recommends that companies implement "reasonable steps" to protect trade secrets by pursuing corrective actions and improvements through a rapid response plan, root-cause analyses of issues, tracking, and periodic reviews.

- RAPID RESPONSE.** Respond promptly to problems of unauthorized taking, disclosure and use of trade secrets, whether internal or among the supply chain.
- RESPONSE PLAN.** Develop and address breaches according to an incident response plan.
- ROOT-CAUSE ANALYSIS.** Ensure that not just immediate problems, but also the root causes of those problems, are addressed.
- TRACKING.** Track corrective actions, for review by the company's information protection team and, where needed, senior management.
- REGULAR REVIEW AND PROTECTION PROGRAM UPDATE.** Use the results of corrective actions to feed into ongoing trade secret risk assessment/risk management reviews and to improve the company's trade secret protection program annually or other regular basis.



CONCLUSION

As trade secrets continue to become more important for companies and economies all over the world, the need for companies to take effective steps to protect trade secrets internally and among their supply chain and other third parties is becoming a more pressing need in order for companies to preserve their assets, business, value and competitiveness.

National and regional laws – perhaps unsurprisingly in a globally connected economy – continue to converge as to the elements required for proprietary information to qualify for legal protection as trade secrets. It is thus vital for companies to understand what “reasonable steps” need to

be implemented to protect trade secrets in accordance with these laws, and to look to leading practices that companies around the world are using to protect such information. The very legal protections that a company hopes to secure for its proprietary information very much depend on taking such “reasonable steps.”

CREATe.org RESOURCES FOR TRADE SECRET PROTECTION

CREATE

▶ Leading Practices *For Trade Secret Protection*

CREATe Leading Practices for Trade Secret Protection is a service helping companies prevent the theft and misappropriation of business critical information. The three-step service offers a practical way to assess and then improve your own internal business processes – or that of your supply chain and business partners – for trade secret protection. www.CREATE.org/Resources. For more information, email info@CREATE.org



CREATE-PWC TRADE SECRET REPORT: ECONOMIC IMPACT OF TRADE SECRET THEFT

This report by CREATe.org in partnership with PricewaterhouseCoopers LLP (PwC), takes a rigorous look at the issue of trade secret theft – the magnitude of the problem, the threat actors and trends – and provides a five-step framework offering practical guidance as to what companies can do to protect intellectual property (IP) assets. <https://create.org/?p=1361>



TRADE SECRET THEFT: MANAGING THE GROWING THREAT IN SUPPLY CHAINS

This whitepaper highlights the issue of trade secret theft in supply chains; shares case studies; and provides practical guidance to help companies implement leading practices with supply chain partners to reduce trade secret theft.

<https://create.org/resource/trade-secret-theft-managing-the-growing-threat-in-supply-chains/>



TRADE SECRET PROTECTION MODEL POLICIES

The policies that your company has in place to protect trade secrets are the foundation to an effect trade secret protection program. CREATe.org has developed sample model polices which can be adapted to your specific requirements and situation. <https://create.org/?p=1355>

ENDNOTES

- ¹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Single Market for Intellectual Property Rights: Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe, at 4 (2011), http://ec.europa.eu/internal_market/copyright/docs/ipr_strategy/COM_2011_287_en.pdf, *citing* http://www.wipo.int/sme/en/documents/valuing_patents_fulltext.html.
- ² The National Bureau of Asian Research, The Report of the Commission on the Theft of American Intellectual Property (May 2013) http://www.ipcommission.org/report/ip_commission_report_052213.pdf.
- ³ CREATE.org, Economic Impact of Trade Secret Theft, at 3, 7-9 (Feb. 2014), <https://create.org/resource/economic-impact-of-trade-secret-theft/>.
- ⁴ See *id.* at 10-12.
- ⁵ D. Almeling et al., A Statistical Analysis of Trade Secret Litigation in Federal Courts, 45 *Gonz. L. Rev.* 291, 295 (2010), <http://www.omm.com/files/upload/AlmelingGonzagaLawReviewArticle.pdf>.
- ⁶ *Id.* at 294.
- ⁷ Nearly all of the top 20 Fortune 500 companies' recent annual 10-K securities filings with the U.S. Securities and Exchange Commission listed cybersecurity or intellectual property issues—both—among their material business risks. CREATE.org, Protecting IP Through Enterprise Risk Management, at 8 (2014), <https://create.org/resource/protecting-intellectual-property-enterprise-risk-management/>.
- ⁸ <http://www.sec.gov/Archives/edgar/data/37996/000003799614000010/f1231201310k.htm#sF9FBED1941F08BA7A1CC649613E193A5>.
- ⁹ TRIPs Art. 39(1), https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm#7.
- ¹⁰ *Id.*, Art. 39(2).
- ¹¹ National Conference of Commissioners on Uniform State Laws, Uniform Trade Secrets Act (UTSA) with 1985 Amendments (1985), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf. See generally <http://www.uniformlaws.org/Act.aspx?title=Trade+Secrets+Act>; Coleman, Randall C., Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism (2014), <https://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft>.
- ¹² USTA Sec. 1(4)(ii).
- ¹³ The outliers — New York and Massachusetts — recognize a common-law (i.e. court-developed) civil claim for misappropriation. See Hargrove, S., Marshall K. The Prospect of a Federal Trade Secret Claim (Smith and Anderson, 2015), <http://www.jdsupra.com/legalnews/the-prospect-of-a-federal-trade-secret-c-33913/>.
- ¹⁴ 18 U.S. Code §§ 1831-1839, <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/html/USCODE-2011-title18-partI-chap90.htm>.
- ¹⁵ *Id.*, § 1839(3)(A).
- ¹⁶ 19 U.S.C. § 1337(a)(1)(A), <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title19/html/USCODE-2011-title19-chap4-subtitleII-partII-sec1337.htm>.
- ¹⁷ See generally P.A. Riley & J. Stroud, A Survey of Trade Secret Investigations at the International Trade Commission: A Model for Future Litigants, *Columbia Science and Technology Law Review* (Fall 2013), <http://www.finnegan.com/resources/articles/articlesdetail.aspx?news=074629d6-20b9-418d-9138-eef40d5a9b2d>.
- ¹⁸ See *id.*, citing Coamoxiclav Products, Potassium Caluvanate Product, and Other Products Derived from Clavulanic Acid, ITC Inv. No. 337-TA-479.
- ¹⁹ In July 2012, for example, the Protecting American Trade Secrets and Innovation Act of 2012 or S. 3389 — which sought to federalize civil trade secret misappropriation — was introduced in Congress. The Senate Judiciary Committee ultimately did not act on the bill, but for reasons unrelated to the merits of implementing a federal civil cause of action.
- ²⁰ Trade Secrets Protection Act of 2014 (H.R. 5233), <https://www.congress.gov/bill/113th-congress/house-bill/5233/text>; Defend Trade Secrets Act of 2014 (S. 2267), <https://beta.congress.gov/bill/113th-congress/senate-bill/2267/text>.
- ²¹ See *supra* note 15.
- ²² Baker McKenzie, Study on Trade Secrets and Confidential Business Information in the Internal Market, Appendix 1: Intellectual Property and Commercial Law — Country Report, at 72 (Apr. 2013), http://ec.europa.eu/internal_market/ipenforcement/docs/trade-secrets/130711_final-study_en.pdf.
- ²³ *Id.* at 76.
- ²⁴ *Id.* at 97.
- ²⁵ *Id.* at 7.
- ²⁶ Law No. 7975 on Undisclosed Information (2008), art. 2(b) (“has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret”), <http://www.wipo.int/edocs/lexdocs/laws/en/cr/cr007en.pdf>.
- ²⁷ Law on the Promotion and Protection of Intellectual Property Rights (Legislative Decree No. 604 of 15 July 1993), art. 177 (“which a person keeps in confidence”; “with regard to which reasonable measures or action have been taken to preserve its confidentiality and restrict access to it”), <http://www.wipo.int/edocs/lexdocs/laws/en/sv/sv001en.pdf>.
- ²⁸ Protection against Unfair Competition Act, 2000 (Act 589), sec. 5(3) (“it has been subject to reasonable steps under the circumstances by the rightful owner to keep it secret”), <http://www.wipo.int/edocs/lexdocs/laws/en/gh/gh005en.pdf>.
- ²⁹ Law No. 30 of December 20, 2000 regarding Trade Secret, arts. 1(1), 3(4) (“the confidentiality of which is maintained by its owner”; “The confidentiality of information shall be deemed to be maintained if the owner or the parties that control the information have taken necessary and appropriate efforts”), <http://www.wipo>.

ENDNOTES

[int/edocs/lexdocs/laws/en/id/id041en.pdf](http://www.wipo.int/edocs/lexdocs/laws/en/id/id041en.pdf).

³⁰ Law No. 15 of 2000 on Unfair Competition and Trade Secrets, art. 4(A)(3) (“has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret”), <http://www.wipo.int/edocs/lexdocs/laws/en/jo/jo013en.pdf>.

³¹ Protection Against Unfair Practices (Industrial Property Rights) Act 2002, art. 9(3)(c) (“it has been subject to reasonable steps under the circumstances by the rightful holder to keep it secret”), <http://www.wipo.int/edocs/lexdocs/laws/en/mu/mu003en.pdf>.

³² Law No. 35 of May 10, 1996 on Industrial Property, art. 83 (“to which he had adopted the means and systems sufficient to preserve its confidential nature and its restricted access”), <http://www.wipo.int/edocs/lexdocs/laws/en/pa/pa002en.pdf>.

³³ Regulations for the Protection of Confidential Commercial Information, art. 1(3) (“if the rightful owner takes reasonable measures to maintain its confidentiality under its current circumstances”, <http://www.wipo.int/edocs/lexdocs/laws/en/sa/sa008en.pdf>).

³⁴ Law No. 5 of the year 2005 on Protection of Secrets of Trade, art. 6 (“The legal holder of confidential information shall have to take measures necessary for maintaining such information in order to prevent others from using the same. In addition, he shall have to regulate use of information within the institution utilizing it and limit utilization only to those who are legally committed to maintain information confidential[ity] and prevent others from using it. The legal holder[s] obligation shall not be waived in the event that other[s] infringe on this information unless he proves that he exerted adequate and reasonable efforts to maintain the information.”), <http://www.wipo.int/edocs/lexdocs/laws/en/qa/qa004en.pdf>.

³⁵ Trade Secret Act B.E. 2545 (2002), sec. 3 (“the controller of the trade secrets has taken appropriate measures to maintain the secrecy”), <http://www.thailawforum.com/database1/trade-secret-act.html>.

³⁶ Protection Against Unfair Competition Act 2002, sec. 9(3)(c) (“the rightful holder has taken reasonable steps to keep it secret”), <http://www.wipo.int/edocs/lexdocs/laws/en/to/to006en.pdf>.

³⁷ Protection Against Unfair Competition Act, 1996, art. 9(3)(c) (“it has been subject to reasonable steps under the circumstances by the rightful holder to keep it secret”), <http://www.wipo.int/edocs/lexdocs/laws/en/tt/tt034en.pdf>.

³⁸ Trade Secrets Act No. 52 of 2000, sec. 3(2)(c) (“reasonable steps to prevent the unauthorised acquisition, use or disclosure of the trade secret”), <http://www.wipo.int/edocs/lexdocs/laws/en/vu/vu041en.pdf>.

³⁹ Anti-Unfair Competition Law, art. 10 (“the trade secret owner has adopted measures to maintain its confidentiality”), http://www.loc.gov/law/help/tradesecrets/china.php#_ftn7.

⁴⁰ See D. Chow, Navigating the Minefield of Trade Secrets Protection in China, 47 Vanderbilt Journal of Transnational Law

1007, 1009 & n.8 (2014), <http://www.vanderbilt.edu/jotl/manage/wp-content/uploads/Chow-Final.pdf>, citing R. Ong, Trade Secret Enforcement in China: Options and Obstacles, China Bus. Rev. (Jan. 1, 2013), <http://www.chinabusinessreview.com/trade-secret-enforcement-in-china-options-and-obstacles/>.

⁴¹ At present, trade secrets are protected by a patchwork of national laws across the EU that vary substantially as to what they protect, how they protect it, and what civil or criminal procedures and remedies apply. See Baker McKenzie, supra note 22; Hogan Lovells International LLP, Report on Trade Secrets for the European Commission (Jan. 2012), http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/120113_study_en.pdf.

⁴² COM/2013/0813 final - 2013/0402 (COD) (Nov. 28, 2014), <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0813>.

⁴³ Id., art. 2(1) (emphasis added).

⁴⁴ Commission Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, No. 9870/14 (2014), <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209870%202014%20INIT>.

⁴⁵ Projet de loi pour la croissance, l'activité et l'égalité des chances économiques (Draft bill for growth, activity and equality of economic opportunities), No. 2498 (2015) (“Projet de loi Macron”), <http://www.assemblee-nationale.fr/14/ta-commission/r2498-a0.asp>. Art. 64 ter of this bill proposes a new Title V to Book 1 of the Commercial Code to protect business secrets.

⁴⁶ Id. Chapter 1, article L. 151-1(3) of the new proposed Title V contains the requirement of “reasonable measures”: “Qui fait l'objet de mesures de protection raisonnables, compte tenu de sa valeur économique et des circonstances, pour en conserver le caractère non public.”

⁴⁷ Russia - Federal Law of the Russian Federation on Commercial Secrecy, No. 98-FZ 2004, art. 3(2), <http://www.wipo.int/edocs/lexdocs/laws/en/ru/ru048en.pdf>. Such measures are recognized as reasonably sufficient provided access is excluded to unauthorized persons, and employees and counteragents can use the information without violating the regime. Id., art. 10. See also http://www.loc.gov/law/help/tradesecrets/russia.php#_ftn5.

⁴⁸ Unfair Competition Prevention Act (Act 47 of 1993), art. 2(6), <http://www.wipo.int/edocs/lexdocs/laws/en/jp/jp174en.pdf>. See generally T. Flynn, Do Japan's Trade Secret Laws Finally Work? A Comparative Analysis of Japanese and U.S. Trade Secret Law (Feb. 2012), http://works.bepress.com/travis_flynn/1.

⁴⁹ See id., T. Flynn at 12-15 (summarizing cases).

⁵⁰ See generally J. Davis, Intellectual Property Law, para. 3.6, at 97 (4th ed. 2012), citing *Coco v AN Clark (Engineering) Ltd*, [1968] FSR 415 (Megarry, J.).

⁵¹ Gurry on Breach of Confidence, para. 7.03, at 243 (2d. ed. 2012).

ENDNOTES

⁵² *Id.*, citing *New Zealand Needle Manufacturers Ltd v Taylor*, [1975] 2 NZLR 33, 36 (McMullin J.).

⁵³ *Sony Hacking Fallout Puts All Companies on Alert*, *New York Times* (Dec. 18, 2014), http://www.nytimes.com/aponline/2014/12/18/us/ap-us-sony-hack-companies-on-alert.html?_r=0.

⁵⁴ See generally CREATE.org, *Protecting Intellectual Property through Enterprise Risk Management*, at 27-29 (2014), <https://create.org/resource/protecting-intellectual-property-enterprise-risk-management/>.

⁵⁵ *Aetna, Inc. v. Fluegel*, 2008 Conn. Super. LEXIS 326, *14 (Feb. 7, 2008).

⁵⁶ *D. Almeling et al.*, *supra* note 5, at 322 n. 128.

⁵⁷ See generally *J. Davis*, *supra* note 50, at 95-97.

⁵⁸ *In re Cooper Tire & Rubber Co.*, 306 S.W.3d 875 (Tex. App. 2010).

⁵⁹ *Paramount Tax & Accounting, LLC v. H & R Block Eastern Enters.*, 683 S.E.2d 141, 148 (Ga. App. 2009).

⁶⁰ *Wyeth v. Natural Biologics, Inc.*, 2003 U.S. Dist. LEXIS 17713 (D. Minn. 2003), *aff'd*, 395 F.3d 897 (8th Cir. 2005).

⁶¹ *Delcath Systems, Inc. v. Foltz*, 2007 Conn. Super. LEXIS 101 **4, 16 (Conn. Super. Ct. Jan. 12, 2007).

⁶² The Maryland Court of Appeals mentioned the company's marking "confidential" on its pricing and strategic-plan data as one significant factor in its finding that the company had exercised "reasonable efforts", in *LeTeune v. Coin Acceptors, Inc.*, 849 A.2d 451 (Md. 2004).

⁶³ *Agilent Techs. v. Kirkland*, 2010 Del. Ch. LEXIS 34, ** 10-12 (Feb. 18, 2010); *Schalk v. State*, 823 S.W.2d 633, 637-640 (Tex. Crim. App. 1991).

⁶⁴ See, e.g., *Otis Elevator Co. v. Intelligent Sys., Inc.*, 17 U.S.P.Q.2d 1773, 1775 (Conn. Super. 1990) (plaintiff did not provide third party manufacturer critical data (including computer source) about its proprietary tooling).

⁶⁵ *Elm City Cheese Co. v. Federico*, 251 Conn. 59, 78 — 86, 752 A.2d 1037, 1049 — 1053 (1999).

⁶⁶ *PatientPoint Network Solutions, LLC v. Contextmedia, Inc.* (S.D. Oh. 2014).

⁶⁷ CREATE, *Trade Secret Model Policies (English)*, <https://create.org/resource/trade-secret-model-policies-english/>.

⁶⁸ *VALCO Cincinnati, Inc. v. N & D Machining Service, Inc.* (S. Ct. Ohio. May 21, 1986), http://scholar.google.co.uk/scholar_case?case=12094991049072361118&q=Valco+Cincinnati,+inc.+v.+N%26D+Machining+Serv&hl=en&as_sdt=2006&as_vis=1. See also *United States v. Howley*, 707 F.3d 575, 579, 105 U.S.P.Q.2d (BNA) 1886, 2013 U.S. App. LEXIS 2397 (6th Cir. 2013) (Goodyear used numerous "reasonable" physical-security steps to protect the equipment it used to assemble steel-reinforced tires for large earthmoving vehicles. The tire assembly machine

was fenced in, the company required visitors to get advanced permission to visit, the company required visitors to pass through a security checkpoint, the company required visitors to sign confidentiality agreements, and visitors were prohibited from having cameras in the facility).

⁶⁹ *E.I. du Pont de Nemours & Co. v. Christopher*, 431 F.2d 1012, 1016 (5th Cir. 1970).

⁷⁰ See generally CREATE, *Building on IT Security for Effective IP Protection* (2014), <https://create.org/resource/building-on-it-security-for-effective-ip-protection/>.

⁷¹ *United States v. Aleynikov*, 2011 U.S. Dist. LEXIS 33345, **3-4 (S.D.N.Y. Mar. 14, 2011), *rev'd on other grounds*, *United States v. Aleynikov*, No. 11-1126 (2d Cir. 2012).

⁷² See *T. Flynn*, *supra* note 48, at 13-14, citing 2004 (wa) 18865, Tokyo District Court, 46th Civil Division (2005) (no indication computer list was secret, no password protection, no prohibition on printing and copying – secrecy element not met).

⁷³ *A. Kardash & R. Weaver*, *The Protection of Trade Secrets in Canada*, at 16-17 (2008), http://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2008/ac2008/126_authcheckdam.pdf.

⁷⁴ CREATE, *Protecting Intellectual Property through Enterprise Risk Management* (2014), <https://create.org/resource/protecting-intellectual-property-enterprise-risk-management/>.

⁷⁵ *Schalk v. State*, *supra* note 63. The court noted that TI had also implemented nondisclosure requirements in its employment agreements, exit interviews for employees leaving the company, strict plant security, restricted physical access to the speech recognition lab, username/password access to the computer directories containing the technology that was restricted to employees having a need to know, the non-authorization of disclosure of the technology, and the general nondisclosure of those programs by TI and its employees.

⁷⁶ See *supra* note 47.

⁷⁷ *MBL (USA) Corp. v. Diekman*, 112 Ill. App. 3d 229, 445 N.E.2d 418, 424-425, 67 Ill. Dec. 938, 221 U.S.P.Q. 725 (1st Dist. 1983), citing *McGraw-Edison Co. v. Central Transformer Corp.* (8th Cir.1962), 308 F.2d 70, 74.

⁷⁸ See generally CREATE, *Trade Secret Theft: Managing the Growing Threat in Supply Chains* (2012), <https://create.org/resource/trade-secret-theft-managing-the-growing-threat-in-supply-chains/>.

⁷⁹ *Technicon Data Sys. Corp v. Curtis 1000, Inc.*, 224 U.S.P.Q. 286, 290 (Del.Ch. 1984).

⁸⁰ *D. Almeling et al.*, *supra* note 5, at 322-23 n.129.

⁸¹ See, e.g., *Wellogix, Inc. v. Accenture, LLP*, 788 F. Supp. 2d 523, 540 (S.D. Tex. 2011) (failure to first obtain written confidentiality agreements from third parties did not warrant summary judgment that material was not a trade secret; this merely raised an issue of fact that needed to be considered with other factors at trial).

⁸² *Palin Mfg. Co. v. Water Technology, Inc.*, 103 Ill. App. 3d 926,

ENDNOTES

431 N.E.2d 1310, 59 Ill. Dec. 553, 221 U.S.P.Q. 640, 641-643 (1st Dist. 1982).

⁸³ See, e.g., *Materials Dev. Corp. v. Atlantic Advanced Metals, Inc.*, 172 U.S.P.Q. 595, 612 (Mass. Super. Ct. 1971) (laboratory assistants had no specific contractual duty not to use or disclose material, but one of the defendants had been in charge of plaintiff's laboratory and had the duty of apprising the assistants of their duties of secrecy; they were found under the circumstances to have known of their duty of secrecy).

⁸⁴ *Columbus Bookkeeping & Bus. Servs. v. Ohio State Bookkeeping, LLC*, 2011 Ohio App. LEXIS 5655, **10-14 (10th Dist. 2011).

⁸⁵ *United States v. Chung*, 659 F.3d 815, 827 (9th Cir. 2011). See also *Farm Bureau Ins. Co. v. Am. Nat'l Ins. Co.*, 505 F. Supp. 2d 1178, 1185 (D. Utah 2007) (fact that company gave employees and agents extensive training on what constituted confidential information was one piece of evidence on question of whether the company's books were trade secrets).

⁸⁶ *Mason v. Jack Daniel Distillery*, 518 So. 2d 130, 132-133 (Ala. Civ. App. 1987).

⁸⁷ *Micro Lithography Inc. v. Inko Indus. Inc.*, 20 U.S.P.Q.2d 1347, 1349-1351 (Cal. Ct. App. 6th Dist. 1991).

⁸⁸ *MBL (USA) Corp. v. Diekman*, supra note 77.

⁸⁹ *Schalk v. State*, supra note 63.

⁹⁰ See supra note 55.

⁹¹ *Pre-Paid Legal Servs., Inc. v. Harrell*, 2008 U.S. Dist. LEXIS 1773, **30-31, at 9, 18 (E.D. Okla. Jan. 8, 2008).

⁹² *Alamar Biosciences, Inc. v. Difco Labs., Inc.*, 40 U.S.P.Q.2d 1437, 1995 U.S. Dist. LEXIS 21342 (E.D. Cal. 1995), <http://www.wipo.int/export/sites/www/pctcaselawdb/en/docs/pct-2006-0004.pdf>.

ABOUT THE CENTER FOR RESPONSIBLE ENTERPRISE AND TRADE (CREATE.ORG)

The Center for Responsible Enterprise And Trade (CREATE.org) is a non-governmental organization (NGO) helping companies around the globe prevent piracy, counterfeiting, trade secret theft, and corruption.

Our mission is to make leading practices in IP protection and anti-corruption achievable for all companies. CREATE works across diverse industries in countries around the world to provide cost-effective and practical assessments, independent evaluations, training and other resources for safeguarding IP and preventing corruption.

To achieve this mission, we have developed three services and eLearning based on best practices drawn from multinational companies, academics, international and business organizations:

- ▶ CREATE Leading Practices for IP Protection
- ▶ CREATE Leading Practices for Trade Secret Protection
- ▶ CREATE Leading Practices for Anti-Corruption

Building on decades of work across the business community on quality assurance, health and safety and other issues, CREATE takes a management systems approach to helping companies implement the internal business processes they need to effectively protect intellectual property and prevent corruption – both internally within their organizations and with third parties.

Companies around the world are using CREATE Leading Practices to benchmark and improve systems for IP protection and anti-corruption. The services are available in Chinese, English, Portuguese and Spanish.

For More Information

Please visit www.CREATE.org, via email at info@create.org or follow us on Twitter @CREATE_org.