Baker McKenzie.

PRACTICAL STEPS
AND BEST PRACTICE:

HOW BUSINESSES CAN ENSURE THEY ARE PROTECTING THEIR TRADE SECRETS

Trade secrets are not registered rights but are granted special protection based on the nature of the information and the way they are treated by their owners. Therefore owners of trade secrets need to ensure they are pro-actively managing their trade secrets to avoid putting these valuable assets at risk. While global trade secret laws will not be completely harmonized any time soon, businesses can prepare through careful housekeeping and planning.

In relation to this, Baker McKenzie has partnered with *Euromoney Institutional Investor Thought Leadership*, on a thought leadership piece focused on trade secrets and its importance for global businesses. Click here to view the results of the study entitled: **The Board Ultimatum: Protect and Preserve (Assessing the Strategic Importance and Protection of Trade Secrets**.

The key four steps are:

- ✓ **identify** trade secrets
- ✓ create and maintain an **inventory**
- ✓ implement **protective** contractual, physical and technical organizational **measures**
- ✓ have a **misappropriation action plan**

STEP 1
Identify your trade secrets

WHY?

- ✓ you need to **identify** the trade secrets and be aware of their value in order to competently protect them
- ✓ trade secrets can include a vast array of information including: ideas, processes, product creation, recipes, methodology, plans, data and software

WHAT?

- ☐ what do you consider the **company's trade secrets** to be?
- ☐ do these "secrets" **qualify** as trade secrets under the relevant law?
  - to which extent is the information **known** (inside and outside the company)?
  - is it possible to identify the boundary between **secret information and employee's experience/skills**
  - what are the **costs** that a competitor should sustain to autonomously obtain the information?
  - what have been the **efforts** to achieve the information (in terms of time, human and financial resources)?
- ☐ is trade secret protection the **right approach** (in contrast to patents, copyright or designs, etc.)?
- ☐ identify **third-party trade secrets** which you have access to and are under a duty to protect and maintain

STEP 2
Create a trade secrets inventory

WHY?

- ✓ essential for establishing and **proving ownership** of rights and interests in your trade secrets
- ✓ helps to ensure that your company's trade secrets (and any third party's trade secrets which you have access to) are **properly protected**
- ✓ useful to **evidence in disputes or proceedings**
- ✓ may facilitate the discovery of **underutilized trade secrets**

WHAT?

- ☐ **list** the (types of) trade secrets owned by the company and any third party's trade secrets which you have access to
- ☐ identify the **jurisdictions** where stored and used so that it is clear which legal regimes apply to which trade secrets
- ☐ **avoid** describing the information in **too much detail** as this may create additional security risks
- ☐ trade secret **owned or licensed**
- ☐ identify who has **access** to which trade secrets
- ☐ describe measures in place which are used to protect each trade secret (see **organizational measures** below)
- ☐ identify potential **expiry** date (if ever), (for example if it is expected to form the basis of a patent application)
- ☐ consider **categories** of trade secrets, ranging from low, medium to highest level of importance (assign a **monetary value** or importance of the trade secret)
- ☐ include regular **review** date for accuracy

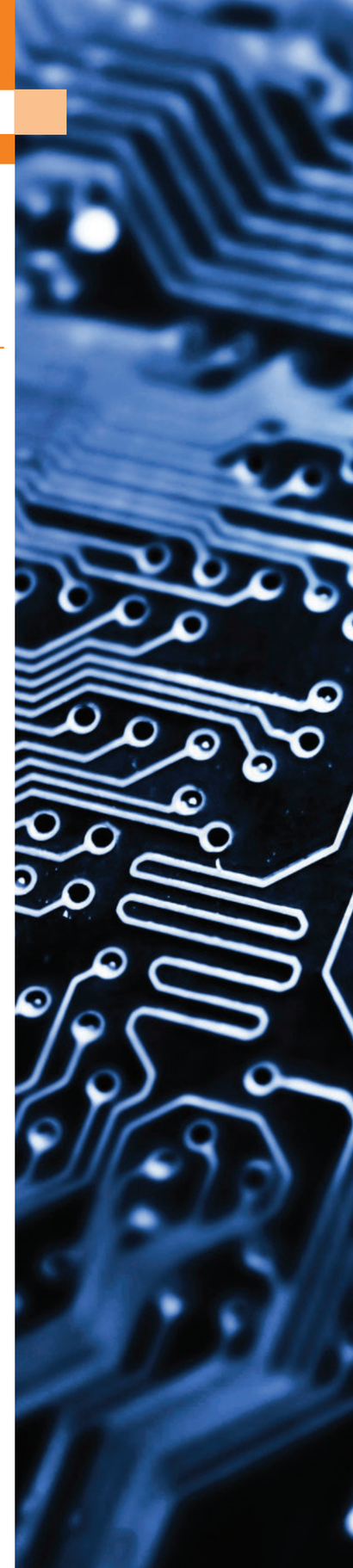
STEP 3
Implement contractual, physical, technical and organizational measures

WHY?

- ✓ prevents **unauthorized access, use, disclosure, loss and modification** of your trade secrets
- ✓ provides clear **protocols and guidance for employees**
- ✓ avoids breaching **duties** imposed in relation to third-party trade secrets
- ✓ ensures **compliance** with any disclosure, discovery or document production obligations in any litigation or arbitration (businesses which have actively taken steps to protect the secrecy of their information must also be able to demonstrate they did so to benefit from protection in the event of a dispute)

WHAT?

- ☐ implement **risk management protocols** and procedures to minimize the unnecessary reproduction/sharing of trade secrets within your organization
- ☐ such protocols and policies will need to be **balanced** against the need to foster **cooperation and transparency** within the organization and partner networks
- ☐ **organizational safeguards** include well-designed and enforced policies and protocols, and **regular training** around confidentiality obligations
- ☐ ensure there is frequent **monitoring** to ensure protocols and policies are being complied with
- ☐ **restrict access** to the information on a need-to-know basis
- ☐ implement **physical barriers**, lock-and-key mechanisms and paper shredders
- ☐ implement **technical safeguards** including passwords, firewalls, automated intrusion detection systems and authentication measures
- ☐ the safeguards you choose to implement should be **tailored** to the specific activities of your organization



- ☐ implement necessary **employment provisions** to support the protection of the trade secrets including provisions in employment contracts, providing training, monitoring, entry and exit interviews, and undertakings upon termination
- ☐ implement necessary **contractual provisions**, such as non-disclosure or confidentiality agreements, in relation to sharing trade secrets with third parties and follow-up on the execution of the contract in order to maintain control over compliance of the other party's duties of confidentiality (ideally these agreements should include a penalty and indemnity clauses and provision of specific rights to facilitate enforcement judiciary measures in case of breach of the contract)
- ☐ **review contracts regularly** in order to ensure that these are always tailored to the employee's position and provide appropriate protection
- ☐ **use of non-compete agreements**; confidentiality agreements may prove inadequate to protect against improper use or disclosure of a key R&D employee; non-compete agreement provides broader protection by imposing a line on the subsequent activities of the employee to minimize the opportunity to use or disclose trade secret(s)
- ☐ use **confidentiality notices**; consider marking written materials as "confidential" (eg, by way of watermark or a heading), this is particularly important when dealing with technical drawings and documents containing sensitive information
- ☐ consider **different levels of protection**; ensure confidentiality obligations attaches to oral communication or in situations or where one forgot to apply a confidentiality notice or the notice was inadvertently modified or removed
- ☐ review any disclosure, discovery or document production obligations in any **litigation or arbitration**
- ☐ ensure there are appropriate and effective **dispute resolution clauses** in contracts relating to trade secrets

STEP 4
Devise a misappropriation action plan

WHY?

- ✓ to prepare for inevitable security breaches ie, situations involving a real and present threat of misappropriation by unlawful acquisition, use or disclosure of a trade secret
- ✓ in threat situations you must act quickly to prevent irreparable harm and imminent dissemination
- ✓ a delay may impact your ability to qualify for preliminary injunctions and other temporary remedies

WHAT?

A misappropriation plan should:

- ☐ set out how to rank or **categorize** the breach so appropriate steps relative to the type of breach can be followed
- ☐ identify who should be **notified** in the event of a breach (including internal and external advisors)
- ☐ set out actions to terminate or limit **access** to your trade secrets (or certain category of trade secrets)
- ☐ identify who and how to **investigate** and document the details of a breach
- ☐ set out actions for seeking **remedies** in response to the breach, including steps to obtain an emergency injunction in any jurisdiction where there is a risk of a breach
- ☐ identify **who is** responsible for taking which steps (ideally a **multi disciplinary approach** involving information technology personnel, directors, lawyers, records managers and public relations staff, as necessary)

- ☐ include special considerations relating to requirements under **data privacy** laws, since these regimes are different from trade secrets and other IP regimes
- ☐ be **readily accessible** to individuals with responsibilities under the misappropriation action plan
- ☐ be included in **training** programs to ensure the effective execution of the misappropriation action plan and have dry run exercises
- ☐ be **updated regularly** according to all relevant legal and business considerations

The type of (re-)action to a (suspected) misappropriation may depend on:

- ☐ **nature** of the breach (intentional or accidental)
- ☐ type of **data affected** (personal data, trade secrets owned by third parties, etc.)
- ☐ identity of actual or potential **infringers** (business partners under contract, employees, criminals, state actors, etc.)
- ☐ the existence of a contractual relationship with **the actual or potential infringers**
- ☐ **jurisdictions affected**
- ☐ **phase** of misappropriation (ie, whether the trade secret is only exposed to potential acquisition, or already acquired, used, disseminated, etc.)
- ☐ the ease or difficulty with which information could be properly acquired or **duplicated by others** (eg, reverse engineering)
- ☐ the **evidence** you have of the (suspected) misappropriation

Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

Contacts

Marcela Trigo
Rio de Janeiro
+55 (21) 2206 4925
marcela.trigo
@trenchrossi.com

Grace Shao
Taipei
+886 2 2715 7306
grace.shao
@bakermckenzie.com

Kevin O' Brien
Washington, DC
+1 202 452 7032
kevin.o'brien
@bakermckenzie.com

Lorenzo de Martinis
Milan
+39 02 76231 334
lorenzo.demartinis
@bakermckenzie.com

David Lashway
Washington, DC
+1 202 835 6179
david.lashway
@bakermckenzie.com

John Murphy
Chicago
+1 312 861 8085
john.murphy
@bakermckenzie.com

Rembert Niebel
Frankfurt
+49 69 2 99 08 209
rembert.niebel
@bakermckenzie.com

Michael Hart
London
+44 20 7919 1938
Michael.Hart
@bakermckenzie.com

Guenther Heckelmann
Frankfurt
+49 69 2 99 08 142
guenther.heckelmann
@bakermckenzie.com

www.bakermckenzie.com