IP Strategies for Trade Secrets

Preserving your trade secrets globally

Dr Sam Williams, Siemens plc

All views are author's own

SIEMENS

Trade secrets – preserving the commercial advantage

What is a “trade secret”*

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

*Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016

At its simplest, a trade secret strategy has two elements

Audit

- Identify trade secrets
  - within a specific commercial context
- Identify protection mechanisms and policies
  - within an existing organizational structure
- Identify access and security
  - physically and virtually within the business
- Identify risks
  - for all aspects of the business

Maintain

- Prevent unauthorized access
  - using the identified access and security provisions
- Prevent unauthorized disclosure
  - using the identified protection mechanisms

The world is not perfect…

- Each element is a dynamic entity, constantly changing
- Each element requires the assignment of clear responsibilities
- Each element feeds into an enforcement strategy
- Each element requires that “reasonable steps” have been taken

SIEMENS

How can we improve? First stage: each element is dynamic

Audit

- Identify trade secrets
  - within a specific commercial context
- Identify protection mechanisms and policies
  - within an existing organizational structure
- Identify access and security
  - physically and virtually within the business
- Identify risks
  - for all aspects of the business

Improve

- Recommend policies and a framework for daily use
  - business-wide advice, workflows and rules
- Recommend steps to mitigate risks
  - Should be proportionate and achievable

~~Maintain~~ MANAGE

- Prevent unauthorized access
  - using the identified access and security provisions
- Prevent unauthorized disclosure
  - using the identified protection mechanisms
- Update policies
- Make education a priority
- Police and monitor

Managing is better than maintaining

- By adding in an “Improve” step we can start to create a workable, framework that keeps the trade secret alive
- Risk mitigation is key to ensuring that we can prevent unauthorized access and disclosure
- Monitoring is vital to ensure that mistakes and issues are spotted early

SIEMENS

How can we improve? Second stage: assignment of clear responsibilities

Audit
- Legal/IP carries out the identification steps – using whatever tools are available

Improve
- Legal/IP recommend policies and risk mitigation

Manage
- Legal/IP carry out education

Audit
- Information is needed from commercial, IT, HR, compliance

Improve
- Support is needed from commercial, IT, HR, compliance

Manage
- Assign policy ownership, systems ownership, monitoring roles, implementation

INCLUSIVE

No responsibility – no trade secret
- By involving stakeholders at each stage, we can move to clear assignments of roles
- Ownership is required to ensure that monitoring, maintenance and management work
- If we don't educate, we can have the most watertight policies but no implementation

SIEMENS

How can we improve? Third stage: enforcement strategy

Audit	Improve	Manage	Search
• Legal/IP carries out the identification steps	• Legal/IP recommend policies and risk mitigation	• Legal/IP carry out education	• Breaches in and out, detection, enforcement. response strategy
• Information is needed from commercial, IT, HR, compliance	• Support is needed from commercial, IT, HR, compliance	• Assign policy ownership, systems ownership, monitoring roles, implement	• Involve sales and marketing, R&D, finance, comms, compliance, HR, IT…..

To enforce or not enforce?

- To maintain the commercial value and advantage of a trade secret we need to ensure that it is policed
- We can’t do this alone, and need to engage a cross-functional team
- And if we enforce, we need to assess the risk of disclosure against potential losses from infringement

SIEMENS

What are our AIMS?

Audit
- Identify trade secrets, protection mechanism, policies, access, security and risks

Improve
- Recommend policies, frameworks and risk mitigation

Manage
- Update policies, educate, police and monitor

Search
- Search for breaches in and out, manage detection, enforcement, response strategy

This sits in a framework of international laws

- **Trade Secrets Directive (Europe)**
- **Defend Trade Secrets Act, Uniform Trade Secrets Act, Protecting American Intellectual Property Act (US)**
- **Anti-Unfair Competition Act (China)**
- **Unfair Competition Prevention Act (Japan)**

SIEMENS

Summary

- A trade secret strategy can be driven by the elements of a trade secret:
  - Secret (not generally known)
  - Commercial value due to secrecy
  - Reasonable steps to keep secret

Audit, Improve, Manage, Search

- Build an inclusive team and assign responsibility

SIEMENS

Disclaimer

Contact

Published by Siemens plc

Dr Sam Williams
Head of Intellectual Property
Siemens plc
Pinehurst 2, Pinehurst Road,
Farnborough, GU14 7FB
United Kingdom

Phone +44 7921 243 956

E-mail sam.williams@siemens.com

SIEMENS