EIP

Trade Secrets: Navigating geopolitical risks and IP theft in the semiconductor industry

Cases of IP theft in the semiconductor industry are on the rise. IP theft is often driven by a desire to accelerate technological development and gain a competitive edge without incurring the high costs of R&D. In August 2025, Taiwanese authorities arrested three current and former employees of Taiwan Semiconductor Manufacturing Co. (TSMC) for allegedly stealing technology trade secrets about the company's manufacturing processes to share with a rival company in Japan. Such cases highlight the threats to organisations' IP, highlighting the importance of identifying what IP you own and how best to protect it.

Semiconductor IP: Intellectual Property Rights

Semiconductors and the products which utilise them may be protected by a range of registered and unregistered IP rights, including:

- copyright (written designs, instructions, layouts, software and applications, copyright in data etc);
- patents (the high-level functional designs as well as innovation in the structure or

operation of devices);

p2

- designs (chip layouts and circuit design);
- database rights (the collection of data associated with chip design and manufacturing);
- topography rights (the layout designs of integrated circuits).

IP rights, such as patents, generally require that the right holder discloses their ideas to the public. The right holder is awarded limited legal protection in return for putting their innovation into the public domain. This might not always be desired. Sometimes, keeping information confidential can offer a better form of protection. For example, the secrets of manufacturing processes may not be discoverable from the finished product. Keeping such know-how behind closed doors may offer the owner better protection than disclosing it in return for a patent.

This is where trade secrets come in.

What is a trade secret?

A trade secret is a special category of confidential information. They are statutorily defined to mean information that:

(i) is **secret**, meaning it is not 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 to the business**; and

(iii) has been **subject to reasonable steps** taken by the person lawfully in control of the information to **keep it secret**.

In the UK, trade secrets are primarily protected under common law through the doctrine of breach of confidence (protecting against the unauthorised use of information which is confidential in nature and disclosed in circumstances importing an obligation of confidence). This is supplemented by the Trade Secrets (Enforcement, etc.) Regulations 2018, which implemented the EU Directive 2016/943 (Trade Secrets Directive).

Under the Trade Secrets Directive and Regulations, trade secrets are infringed through unlawful acquisition, use or disclosure.

In the context of semiconductors, trade secrets may be used to protect material compositions, proprietary manufacturing processes and testing methodologies.

The loss of a trade secret can have one of the most significant impacts on a company's competitive edge. Therefore, ensuring that a company has a well-organised trade secret framework and governance which is fit for all key territories, is essential in today's geopolitical landscape.

Protecting trade secrets

What qualifies as a trade secret can be wide ranging. As such, protecting them requires a holistic approach, including strong legal safeguards like contracts (e.g., non-disclosure agreements, restrictions on use and employee and trade restrictive covenants). This should be coupled with robust internal policies, such as employee training, physical and electronic access controls and security measures. Steps should be taken to safeguard proprietary information like manufacturing processes, source code, chip designs, and chemical formulations from both internal and external threats.

In the event of misappropriation of a trade secret, the owner would need to demonstrate to what the trade secret relates. This is in part because a court needs to be able to define the secret in order to make orders relating to it (which is often harder than it sounds) and the steps taken to protect it. This involves:

- **Step 1: Identify** – Businesses must carefully assess their important know-how to determine exactly whether it constitutes economic value to the business. This may require a dedicated team of people with knowledge of the information and strategic understanding of the company's objectives.

- **Step 2: Internal Measures** – Consider what measures would be appropriate to protect such information. For example:

- Limiting access to certain employees;

-

Controlling physical access e.g. housing R&D in a different building to other operations;

- Classifying documents to demonstrate that the organisation clearly distinguishes between different categories of information;
- HR policies and procedures around the protection and use of such information and how to report a disclosure/breach;
- Training around the protection of information; and
- Upgrading and/or adoption of systems and processes to ensure protection of the information.
- **Step 3: Legal Documentation** – Robust contractual provisions can protect trade secrets. For example, an NDA could in certain circumstances prohibit reverse engineering of shared samples. Furthermore, such provisions can make it easier to pursue remedies for breach, including injunctions to prevent further use or disclosure, and compensation for loss suffered as a result.
- **Step 4: Monitoring and enforcement** – Despite available legal protections, semiconductor companies face significant challenges in protecting trade secrets both from internal and external threats. Therefore, it is important that companies carry out ongoing monitoring of the information and take necessary action as soon as reasonably practicable in the event of misappropriation or compromise to the security of its information.

Trade Secrets v Patents

Deciding whether to keep inventions secret or to patent them, largely depends on the ability to detect the invention in a finished product. If an idea is patentable, and it is possible to detect it in the product, getting a patent might be commercially sensible. This

might apply to features relating to the structure of a semiconductor device. A patent would allow the patent holder to exclude others from exploiting the technology, giving them a competitive advantage. Such an advantage might increase revenue, or for early-stage companies, it may help entice investors. However, in doing so the idea will be made public, as most patents are published during the application process. Conversely, it may make better commercial sense to keep an idea secret. For example, inventions relating to semiconductor manufacturing processes are not typically detectable in the end product. By filing a patent, you are telling the world about your important processes, but any resulting patent may not be enforceable, given the difficulty in detecting the use of the process.

In addition, patenting can be expensive, especially if you seek protection in a large number of jurisdictions. You may also need to police and enforce any granted patents, which can prove more difficult in 'hidden' technologies (e.g. in chips and behind APIs). Also, unlike patents, which publish after 18 months and only usually last up to 20 years, trade secrets can remain 'secret' indefinitely (assuming no leaks or independent third-party development). Above all else, commercial considerations are key, and early legal advice is essential to ensure appropriate and proper protection.

Key takeaways for businesses

Trade secrets provide essential protection for proprietary confidential information. The complex designs and innovations that power semiconductor manufacturing are invaluable. However, as geopolitical competition heats up for economic and technological dominance, semiconductor companies increasingly become targets of IP theft. Board members need to be alert to this risk and be putting in place robust measures to protect their intellectual assets. By having a well-organised trade secret framework and robust internal governance, semiconductor companies will be better prepared to handle and respond to challenges posed by the geopolitical landscape.