RDS
ADVOCATES & SOLICITORS

In Business Collaboration:
AMT / ANDERSON MORI & TOMOTSUNE

Trade Secrets Under Siege: Lessons From AI, Semiconductor And Tech Wars

14 September 2026

For more information, please contact:

Datuk D P Naban
naban@rdslawpartners.com

Austen Emmanuel Pereira
austen@rdslawpartners.com

Bahari Yeow Tien Hong
bahari@rdslawpartners.com

Farah Shuhadah Razali
farah@rdslawpartners.com

Tan Sri Datuk Harmindar Singh Dhaliwal
harmindar@rdslawpartners.com

Kenny Lam Kian Yip
kenny@rdslawpartners.com

Lim Zhi Jian
jian@rdslawpartners.com

Michael Soo
michaelsoo@rdslawpartners.com

Rosli Dahlan
rosli@rdslawpartners.com

Steven Perian KC
speriankc@rdslawpartners.com

Vinayak Sri Ram
vinayak@rdslawpartners.com

The most valuable asset in the technology economy may be something that cannot be patented, bought or easily replaced: knowledge. That is also what makes it so difficult to protect.

As competition for artificial intelligence (AI) and semiconductor talent intensifies, employees are moving between rivals with unprecedented speed and compensation. At the same time, companies are feeding increasingly sensitive information into AI systems in the pursuit of productivity. The result is a new and uncomfortable question for businesses: where does legitimate employee know-how end and a company's trade secret begin?

The answer remains important in Malaysia, where there is no standalone Trade Secrets Act. Instead, confidential information is principally protected through equitable principles, contractual obligations and related legislation. The traditional test remains grounded in whether information has the necessary quality of confidence, was communicated in circumstances importing an obligation of confidence, and was used to the detriment of its owner.

However, the technology landscape is moving faster than the legal terminology.

Talent Can Move But Trade Secrets Should Not.

The recent wave of aggressive hiring in the AI industry illustrates the distinction.

A company is generally entitled to hire an engineer from a competitor. An employee's skills, experience, judgement and accumulated know-how do not belong to their former employer. A good engineer does not leave their professional abilities at the office door.

The position changes, however, when the employee takes confidential information with them.

This distinction is increasingly important as companies compete for scarce AI and technology talent. Hiring someone who worked on a rival's product is not, by itself, evidence of trade-secret misappropriation. Asking that person to bring confidential source code, product designs, customer information, pricing data or technical documentation is an entirely different proposition.

The practical message for businesses recruiting from competitors is therefore straightforward: hire the person, not the competitor's secrets.

Recruiters and hiring managers should avoid questions designed to extract confidential information about a candidate's former employer. They should not ask candidates to bring documents, demonstrate proprietary systems or identify confidential customers, suppliers or product roadmaps. They should also be cautious about encouraging a new hire to recruit an entire team from the former employer.

The risk is not confined to confidentiality. Aggressive solicitation of employees may also engage contractual and employment-law issues.

The Contract Remains The First Line Of Defence

For employers, the employment contract remains one of the most important tools for protecting sensitive information.

Confidentiality provisions should clearly identify what constitutes confidential information and should be supported by practical controls: access restrictions, information classification, return and deletion obligations, and appropriate protections for company devices and systems.

The lesson is particularly relevant when an employee leaves.

Deleting an email does not necessarily mean that the evidence has disappeared. Modern forensic tools can recover or reconstruct activity from company devices, accounts and systems. Employers investigating suspected misappropriation should therefore consider preservation and forensic measures early, rather than assuming that deleted information is beyond reach.

For employees, the converse lesson is equally important: do not assume that information is yours simply because you can access it or because you created it during your employment.

From Trade Secrets To Economic Sovereignty

The stakes become considerably higher when sensitive technology has implications beyond an individual company.

Recent semiconductor disputes demonstrate how governments are increasingly treating advanced technologies as strategic assets. Taiwan's prosecution of a former semiconductor engineer over alleged disclosure of advanced chip technology illustrates the point: once governments classify particular technologies as matters of national security, the issue is no longer merely whether a company has suffered commercial loss.

Malaysia does not have an identical national-security regime for trade secrets. But companies operating in sensitive sectors should be alert to the wider regulatory environment including the Strategic Trade Act 2010, Official Secrets Act 1972 and Computer Crimes Act 1997.

For businesses handling strategically important technology, the question is therefore no longer simply, "Can we sue if this information is stolen?"

It is also: Who controls the technology, where is the data, who can access it, and which laws can reach it?

Data Sovereignty Is The New Perimeter

This is particularly significant in cloud and AI environments. A common assumption is that data is sovereign because it is physically stored in Malaysia. That is not necessarily the case.

The legal and operational reality can depend on who controls the infrastructure, who has access to the information and which jurisdictions may assert legal authority over the service provider. A Malaysian data centre operated by a foreign-headquartered provider may therefore raise questions that cannot be answered simply by looking at the physical location of the server.

For companies handling highly sensitive information, data sovereignty should consequently be assessed as part of technology procurement and governance, rather than treated as an IT issue alone.

AI Has Created A New Leak- The Prompt

Perhaps the most immediate challenge is generative AI.

The Samsung experience is instructive. Engineers using ChatGPT for legitimate work reportedly entered source code and internal meeting information into an external AI service. The employees were not necessarily trying to steal anything. They were trying to work faster. This is precisely what makes the risk difficult.

An employee does not need malicious intent to compromise confidential information. A well-intentioned employee can create a serious confidentiality problem simply by putting the wrong information into the wrong AI tool.

The legal question will often turn on whether the employee was authorised to do what they did and whether the organisation had clear rules governing AI use. If employees are expressly permitted to use an AI system, it becomes harder to characterise an undesirable outcome as employee misconduct. If policies clearly prohibit confidential information from being uploaded, however, a breach may justify disciplinary action depending on the circumstances and consequences.

The broader lesson is that an AI policy cannot sit in a handbook gathering dust. Employees need to know what they can use, what they cannot upload, which tools have been approved and what information is classified as restricted.

AI Governance Is Now Trade-Secret Governance

The traditional model of trade-secret protection focused on a relatively familiar set of threats: departing employees, competitors, physical documents and unauthorised access.

AI has multiplied the routes through which information can escape.

Confidential information can enter a system through prompts, training data, retrieval systems or uploaded documents. Depending on the architecture and contractual arrangements, questions may arise about retention, access, use for model training and whether information can subsequently be retrieved or exposed.

This makes trade-secret protection an enterprise-governance issue.

Legal, human resource, cybersecurity, procurement and business teams should not operate in separate silos. Companies deploying AI should assess the technology before implementation and ask vendors fundamental questions: what happens to information submitted to the system? Is it retained? Is it used to train models? Who can access it? Where is it processed? What contractual protections apply?

The answers should determine which information may safely be used with the system.

The Practical Takeaway

The trade-secret concept is not becoming obsolete. If anything, it is becoming more important. But protecting secrets in 2026 requires more than a non-disclosure agreement (NDA).

Businesses should know what information is genuinely confidential, classify it appropriately, restrict access according to role and project, maintain sensible contractual protections, and review those controls periodically. They should establish clear rules for employee departures and recruitment from competitors.

And before deploying AI, they should understand exactly what happens to information once it enters the system.

The central principle remains remarkably simple: people can take their skills with them, but companies should not allow their secrets to travel with them.

In the AI economy, however, the employee is no longer the only route out. The prompt may be the new briefcase, the cloud may be the new filing cabinet, and the AI model may be the new and far less predictable recipient.

For boards and management, protecting trade secrets is therefore no longer just an IP exercise. It is a question of technology governance, employment practice, cybersecurity and, increasingly, corporate resilience.

KUALA LUMPUR
Level 16, Menara 1 Dutamas No. 1, Jalan Dutamas 1, Solaris Dutamas, 50480 Kuala Lumpur
T: +603 6209 5400
F: +603 6209 5411
enquiry@rdslawpartners.com

PENANG
Suite S-21E & F21st Floor, Menara Northam, No. 55, Jalan Sultan Ahmad Shah, 10050 Penang
T: +604 370 1122
F: +604 370 5678
generalpg@rdslawpartners.com

JOHOR BAHRU
8-35, Menara Delima Satu, Jalan Forest City 1, Pulau Satu, 81550 Gelang Patah, Johor Bahru
T: +607 585 6414
F: +607 509 7614
generaljb@rdslawpartners.com