STUDY ON THE PROTECTION AND MANAGEMENT OF TRADE SECRETS IN SINGAPORE

IPOS
INTELLECTUAL PROPERTY
OFFICE OF SINGAPORE

A. INTRODUCTION

Trade secrets generally refer to information that is secret and has commercial value. Reasonable steps must be taken by the owner (such as an enterprise or innovator) to keep such information confidential.[1] Examples of trade secrets include methods or techniques of manufacture, commercial data such as lists of suppliers and clients, recipes, formulas and source codes.

Globally, trade secrets are viewed as increasingly important to economic and enterprise growth. A 2015 study by the Organisation for Economic Co-operation and Development ("OECD") found that increased trade secret protection translated to better innovation inputs and international economic flows.[2]

Among enterprises, there is increasing recognition of the importance of trade secrets for business growth. A 2017 survey by Baker McKenzie[3] found that 8 in 10 respondents regarded trade secrets as an important, if not essential, part of their business. A 2021 study by the Economist Intelligence Unit[4] also found that the top perceived consequences of trade secret misappropriation[5] were loss of business (cited by 52% of the respondents), loss of competitive advantage (51%), and reputational damage (42%).

In addition, there has been an increased focus on protection of trade secrets in some jurisdictions with legislation[6] specifically targeted at trade secret infringement.[7]

B. AIM

As part of the national efforts under the Singapore IP Strategy 2030 to maintain Singapore's world-class intangible assets ("IA")/intellectual property ("IP") regime and support innovative enterprises in using their IA/IP for growth, a comprehensive study of trade secrets in Singapore was undertaken by IPOS.

The study aimed to gain a deeper understanding of Singapore's trade secret regime vis-à-vis other comparable economies. The study also sought to find out the level of knowledge and ability of enterprises operating in Singapore to protect and manage their trade secrets, and how they might be supported in this regard.

---

[1]The World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS") stipulates that the accepted definition of trade secrets is information that must meet three criteria – it must be secret, it must be reasonably protected, and it must derive value from its secrecy.
[2]OECD. 2015. Enquiries into Intellectual Property's Economic Impact. Chapter 4: An Empirical Assessment of the Economic Implications of Protection for Trade Secrets.
[3]Baker McKenzie. 2017. The Board Ultimatum: Protect and Preserve. The Rising Importance of Safeguarding Trade Secrets.
[4]Economist Intelligence Unit. 2021. Open secrets? Guarding value in the intangible economy.
[5]For the purposes of this report, the term "trade secret infringement" refers to various acts including misappropriation, unlawful use and unlawful disclosure. As this study covers these various acts, the term "trade secret infringement" is generally used throughout this report. The term "trade secret misappropriation" is used only when citing a survey or a study which uses this specific term, for accuracy.
[6]Examples of such legislative efforts include: (i) the enactment of the Defend Trade Secrets Act by the United States of America in 2016 (ii) amendments to the Anti-Unfair Competition Law in 2019 by China to shift the burden of proof to the defendants to prove the independent and legitimate origin of the trade secrets which they are alleged to have infringed and (iii) the introduction of the Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure in the European Union ("EU Trade Secrets Directive").
[7]For the purposes of this report, the term "trade secret infringement" refers to various acts including misappropriation, unlawful use and unlawful disclosure. As this study covers these various acts, the term "trade secret infringement" is generally used throughout this report. The term "trade secret misappropriation" is used only when citing a survey or a study which uses this specific term, for accuracy.

C. STUDY APPROACH

A mixed method approach was adopted comprising desktop research, a survey of enterprises operating in Singapore of various sizes from a wide range of industries, and in-depth engagements (based on the Chatham House Rule) with such enterprises, legal academics, in-house counsels, legal practitioners, foreign IP Offices and relevant government agencies.

The study focused on two key areas:

- Understanding and Supporting Enterprise Needs
- Review of the Legal Framework

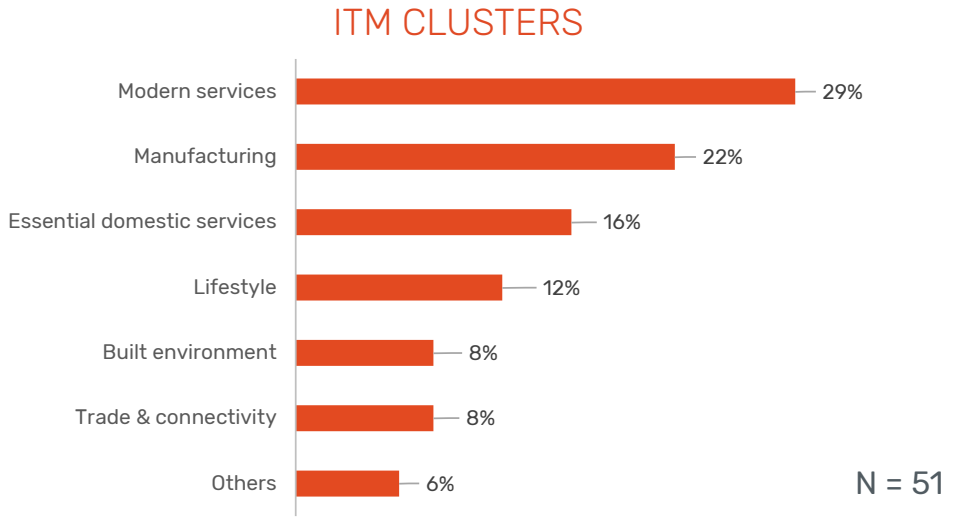
Understanding and Supporting Enterprise Needs

Beyond desktop research, an enterprise survey was conducted. A total of 51 enterprises responded. The profile breakdown of these enterprises is as follows:

- Majority of the respondents (82%) belonged to Small and Medium-sized Enterprises ("SME").[8]

- Two-thirds of the respondents (66%) were private businesses, with 16% from business/ trade associations and just 4% are related to the government sector. The remaining respondents were from research institutes and higher education.

- There was a good spread of respondents across the various Industry Transformation Map ("ITM") clusters, with Modern Services (29%) and Manufacturing (21%) being the most represented; and Built Environment and Trade & Connectivity (both 8%) being the least represented.



- Individual engagements were also conducted with local and foreign enterprises across different profile types, including with SMEs, Multinational Corporations and Large Local Enterprises from the Manufacturing, Essential Domestic Services, Trade & Connectivity and Modern Services ITM clusters.

[8] Based on Enterprise Singapore's definition of an SME i.e., 200 or less employees or S$100mil or less in sales revenue.

Review of the Legal Framework

A comparative cross-jurisdictional review was conducted,

- Across the common law and civil law spectrum;
- Across various regions; and
- Across various socio-economic contexts;

including the following jurisdictions:

ASEAN Member States

Australia

Canada

China

Denmark

Germany

Israel

Japan

Republic of Korea

United Kingdom of Great Britain and Northern Ireland

United States of America

The review also considered the EU Trade Secrets Directive.

The comparative review employed an indices approach with the following indices:

- Subject Matter Protected i.e. the type of information that will be protected.
- Definition of Infringement/Breach i.e. the types of acts that will be considered infringement/breach.
- Consequences of Infringement/Breach i.e. civil remedies and criminal sanctions.

- In-depth engagements were also conducted with IP Offices from various jurisdictions and legal academics with IP law expertise.
- Roundtable sessions were also conducted with legal practitioners with expertise in IP litigation and in-house counsels from a variety of enterprises (including from the Manufacturing, Essential Domestic Services, Professional Services and Lifestyle ITM clusters).

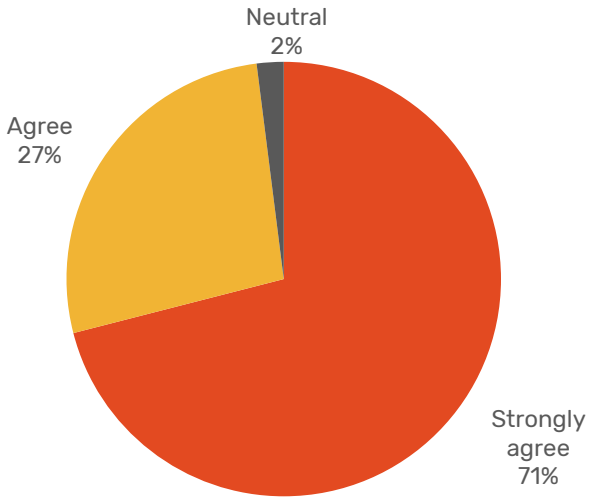
D. STUDY FINDINGS

I. Understanding and Supporting Enterprise Needs

(i) Enterprises recognise the importance of trade secrets.

Almost all (98%) of the enterprises surveyed recognised the importance of trade secrets to their business growth.

TRADE SECRETS ARE IMPORTANT TO THE GROWTH OF MY ORGANISATION. DO YOU AGREE?

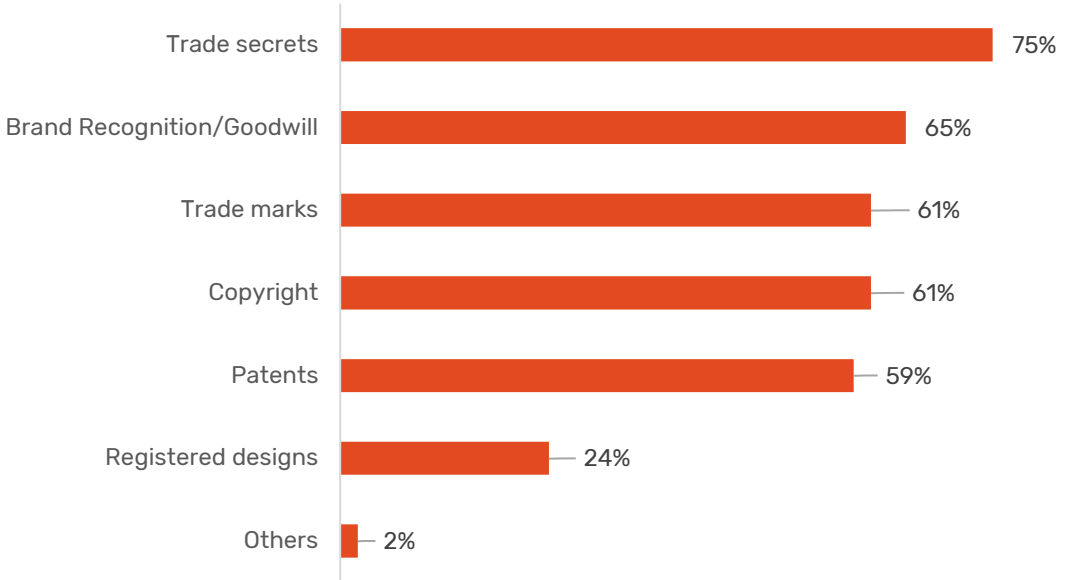


N = 51

Trade secrets were also most frequently considered to be important (selected by 75% of the respondents), followed by brand recognition/goodwill (65%), and trade marks and copyright (both 61%).

WHICH OF YOUR ORGANISATION'S IP DOES YOUR ORGANISATION CONSIDER TO BE THE MOST IMPORTANT TO ITS BUSINESS?

(may select more than one option)

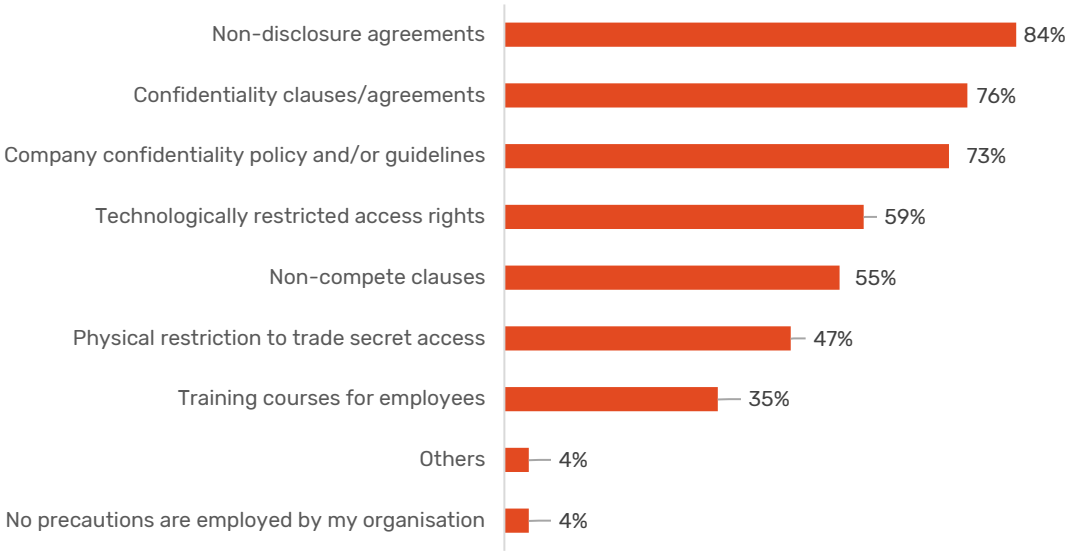


N = 51

Similar observations were made in the aforementioned study by Baker McKenzie, which found that 7 in 10 respondents saw trade secret protection as becoming more critical than other types of IP protection.

The majority (96%) of the enterprises surveyed also indicated that they had at least one type of trade secret protection measure in place, with the most common measure being the use of non-disclosure agreements (used by 84% of the respondents).

WHAT TYPES OF PRECAUTIONS ARE EMPLOYED BY YOUR ORGANISATION TO PROTECT TRADE SECRETS?



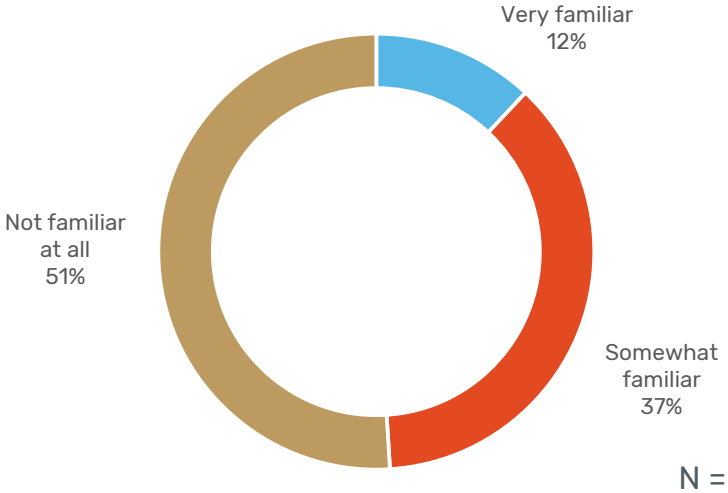
N = 51

A study by the Economist Intelligence Unit[9] also found that confidentiality agreements and policies (indicated by 68% of the respondents) were the most common measures used to protect their trade secrets.

(ii) Many enterprises are unsure of how best to protect and manage their trade secrets.

More than half (51%) of the survey respondents indicated that they were not familiar at all with Singapore's trade secret regime.

HOW FAMILIAR ARE YOU WITH SINGAPORE'S TRADE SECRET REGIME?



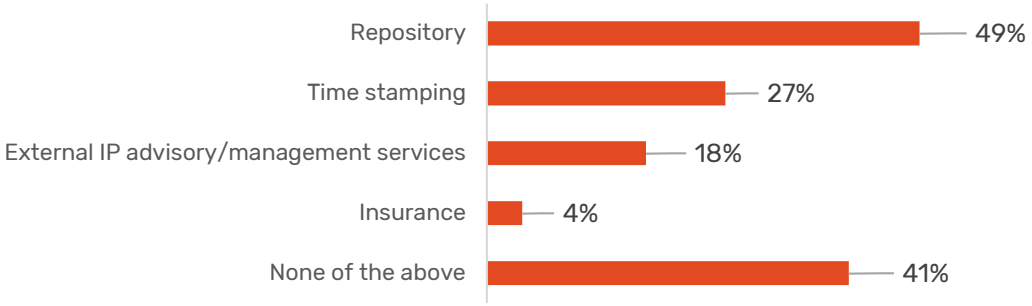
N = 51

[9] Economist Intelligence Unit. 2021. Open secrets? Guarding value in the intangible economy.

2 in 5 of the enterprises surveyed did not use any trade secret-related services. Of those who used such services, the most common type of service was a repository (used by 49% of the respondents).

WHICH OF THE FOLLOWING SERVICES HAVE YOU USED TO SAFEGUARD YOUR TRADE SECRETS?

(may select more than one option)



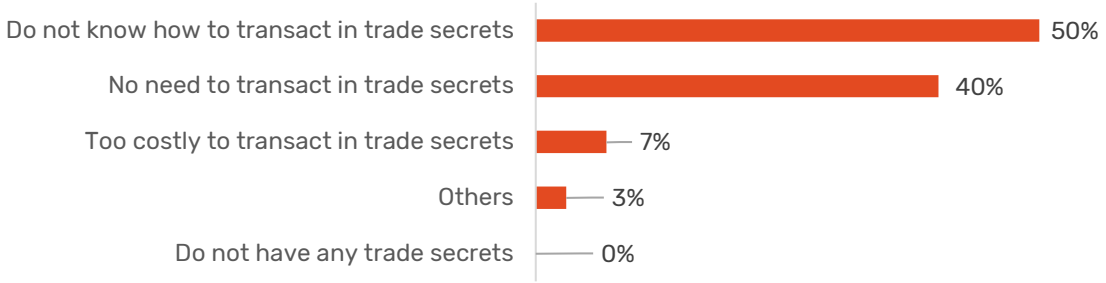
N = 51

Through the in-depth individual engagements, the following common challenges faced by enterprises were identified: (i) Lack of dedicated IT systems to manage trade secrets; (ii) Lack of training and a strong culture of trade secret management; and (iii) Difficulties by SMEs in safeguarding their trade secrets via contracts due to their small size and lack of bargaining power.

More than half (55%) of the enterprises surveyed did not transact in trade secrets, with most of them citing a lack of knowledge as a reason.

WHY DID YOU NOT TRANSACT IN TRADE SECRETS?

(may select more than one option)

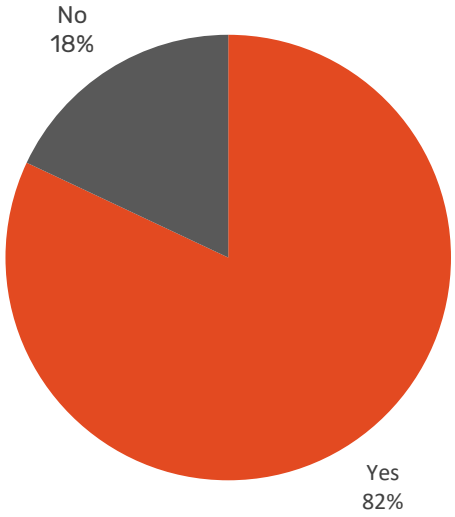


N = 30

(iii) Enterprises need help to strengthen their trade secret protection and management practices.

More than 80% of the enterprises surveyed indicated that their organisation needed more measures or policies in place to protect and manage their trade secrets.

DO YOU THINK YOUR ORGANISATION NEEDS TO HAVE OTHER MEASURES OR POLICIES IN PLACE TO PROTECT ITS TRADE SECRETS?



N = 51

SMEs lagged behind larger enterprises in terms of awareness and capabilities. Larger enterprises were more likely to provide training for their staff and know what legal recourse to take in the event of a trade secret misappropriation.

N = 51

Larger enterprises had a better understanding of trade secrets and how it impacts their business. MNCs also benefitted from support and guidance on trade secrets and other IP matters from their international headquarters.

(iv) Most enterprises highlighted trade secret misappropriation as a concern, with 1 in 5 encountering at least one instance of trade secret misappropriation in the past 10 years.

Although 9 in 10 of the enterprises surveyed indicated that the misappropriation of trade secrets was a concern to their organisation, just 1 in 5 had encountered at least one instance of trade secret misappropriation in the past 10 years.

The incidence rate of trade secret misappropriation closely mirrors that of a separate study by the European Commission,[10] in which 1 in 5 of the respondents had suffered at least one attempt of trade secret misappropriation in the last 10 years. In the United States of America, various commentaries from institutes and law firms have indicated that trade secret litigation continues on a steady upward trajectory since the enactment of the Defend Trade Secrets Act in 2016.[11]

Former employees were often identified as the main perpetrators. This was indicated by 55% of the enterprises surveyed who had experienced at least one instance of trade secret misappropriation in the past 10 years.

Enterprises typically avoid an adversarial approach when addressing alleged trade secret misappropriation, citing the lack of evidence and difficulty in ascertaining the value of damages suffered. That said, most noted that the "soft" approach, e.g., negotiation and mediation, was generally effective, especially if the misappropriation was unintentional.

[10] European Commission. 2013. Study on Trade Secrets and Confidential Business Information in the Internal Market.
[11] Examples include: Lex Machina. 2020. Trade Secret Litigation Report; Stout Risius Ross LLC. 2020. Trends in Trade Secret Litigation Report 2020; ip-watchdog.com. 2020. Trade Secret Litigation Reports: Four Years after the Enactment of the Defend Trade Secrets Act; IAM-media.com. 2021. Damages track upward in US trade secret litigation.

(v) Enterprises need to maintain their guard against trade secret infringement in light of innovation trends.

Despite an apparently low reported incidence of trade secret misappropriation, there is nonetheless a heightened need for enterprises to strengthen protection of their trade secrets as they navigate the current and emerging trends driving innovation. With rapid digitisation, increasing use of cloud services for safeguarding and managing confidential information as well as continued remote working, enterprises are at an elevated risk of an increase in cybertheft of trade secrets.

For example, a 2021 report by Verizon found that phishing and ransomware attacks have increased by 11% and 6% respectively over the past year.[12] A separate study by the European Centre for International Political Economy estimated that cybertheft has led to a €60 billion loss in economic growth in the European Union and the potential loss of 289,000 jobs.[13] A recent report by Gartner further highlighted the need for businesses to establish a "Cybersecurity Mesh" to extend data protection beyond internal IT systems to also include external networks.[14]

II. Review of the Legal Framework

(vi) The findings from our comparative cross-jurisdictional review showed that Singapore's legal regime is relatively robust across the three indices employed in the review (see page 3 at Section C of this report). This aligns with the findings from the engagements with the various groups of stakeholders such as legal academics, in-house counsels and legal practitioners. The commonly expressed views were that Singapore's current trade secret legal framework is sufficient with a comprehensive toolbox for the protection of trade secrets[15] and that there is no need to enact a trade secret specific legislation nor introduce new criminal sanctions for trade secret infringement. Moreover, while the regime for protection of confidential information is largely premised on principles from case law, case law has been evolving and adapting to changing business practices and technological advancements to ensure that our regime continues to be robust in the protection of such information.[16]

Index (i): Subject Matter Protected i.e. the type of information that will be protected.

In terms of subject matter protected, a relatively wide range of information is covered. Under the breach of confidence regime, if the information has a quality of confidence and was imparted and/or received under an obligation of confidentiality, the information would be caught by the breach of confidence regime. This is generally understood to mean that the subject matter protected goes beyond trade secrets to a wide range of confidential information.

[12]Verizon. 2021. Data Breach Investigations Report 2021.
[13]ECIPE. 2018. Stealing thunder, Cloud, IoT and 5G paradigm for protecting European commercial interests. Will Cyber espionage be allowed to hold Europe Back in the global race for industrial competitiveness?
[14]Gartner. 2021. Top Strategic Technology Trends for 2021.
[15]This toolbox includes the common law Breach of Confidence regime, Employment Law, Contract Law, Copyright Act, Computer Misuse Act and Penal Code.
[16]See analysis on Index (ii) on developments in case law in ascertaining the types of acts that constitute a breach of confidence.

Index (ii): Definition of Infringement/Breach i.e. the types of acts that will be considered infringement/breach.

In terms of defining what constitutes an infringement or breach, a relatively wide scope of acts is covered including acquisition, use and disclosure. The Computer Misuse Act also deals with the issue of cybertheft as it imposes criminal sanctions against unauthorised access to or modification of computer material.[17]

With regard to the breach of confidence regime, infringement/breach may be made out even in circumstances where defendants do not use or disclose the confidential information but have wrongfully accessed or acquired the same.[18]

Index (iii): Consequences of Infringement/Breach i.e. civil remedies and criminal sanctions.

In terms of this index, there is recourse under the breach of confidence regime, employment law, contract law as well as the relevant statutes which impose criminal sanctions for infringing acts. The view generally expressed at the roundtable with legal practitioners was that the various regimes provide ample avenues for the protection of trade secrets in terms of both criminal and civil liability.

(vii) In addition to the above, other views from the engagement sessions with the various groups of stakeholders from the legal field included:

- Concerns about the loss of flexibility resulting from codification.
- Feedback on the need to balance between providing strong protection for existing trade secret holders, and the inadvertent effect an overly strong regime could have on chilling local innovation, for example by creating barriers to entry.
- Shared sentiment on the need to improve awareness and training of both management and employees, in terms of trade secret protection.
    - This sentiment is corroborated by the enterprise survey results and in-depth enterprise engagements, which highlighted that a fundamental concern for enterprises is their lack of awareness of the existing legal framework and the corresponding measures or policies to put in place to protect and manage their trade secrets (see pages 5 to 7 at Section D(ii) and (iii) of this report).
- The importance of maintaining confidentiality in legal proceedings and the need for clearer rules and processes to give certainty and confidence in instituting legal proceedings in Singapore.

[17] See Part II Offences sections of the Computer Misuse Act.

[18] See the Court of Appeal case of *I-Admin (Singapore) Pte Ltd v Hong Ying Ting and others* [2020] SGCA 32 [43] – [45], [61] – [62], which modified the approach towards breach of confidence claims. The decision has been generally regarded by legal practitioners in Singapore as addressing evidential difficulties faced by owners of confidential information in bringing a claim for breach, and also taking into account modern technology.

E. SUMMARY AND RECOMMENDATIONS

The Singapore IP Strategy 2030 underscores IPOS' commitment to maintaining a world-class IA/IP regime and supporting innovative businesses in leveraging their IA/IP for growth. This involves looking into current and emerging business trends.

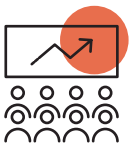
The mixed methodologies adopted for this study and range of stakeholders consulted provided IPOS with good insights into the attitudes and approaches of both business and legal stakeholders to trade secret protection and management. Such insights include the need to strike a balance between stronger policies that protect existing rights holders and encourage further investments in research and innovation, against the need to allow information flows and labour mobility to encourage future innovation.

The findings from this study demonstrate that more may be done to support enterprises in the protection and management of their trade secrets. Addressing these gaps will place the enterprises and Singapore in better stead to compete in this era of rapid technological advances. On the legal framework front, there is scope to explore refinements to processes for the preservation of confidentiality of trade secrets during legal proceedings. That said, the stakeholders engaged in this study have also affirmed that there is no substantive need for legislative reform to strengthen trade secret protection in Singapore.

I. Understanding and Supporting Enterprise Needs

In terms of enterprise support, IPOS will look into these three areas as part of the efforts under the Singapore IP Strategy 2030:

Awareness raising. Curating resources and activities that are designed to generate awareness on the importance of trade secrets, including publishing an enterprise guide on Singapore's trade secret regime to provide practical advice for enterprises in protecting and managing their trade secrets, and case studies of successful protection and management measures.



Building capability. Building enterprises' capabilities in trade secret protection and management to enable enterprises to derive better value and business growth from trade secrets.

Access to services. Increasing accessibility (or availability) of trade secret-related services (e.g., time stamping and repository) to support enterprises in trade secret protection.

II. Review of the Legal Framework

On the legal framework front, IPOS and the Ministry of Law are looking into the feedback on ensuring the confidentiality of trade secrets during legal proceedings, and will follow up on the matter with the relevant stakeholders.

F. ACKNOWLEDGEMENTS

We would like to extend our appreciation to our partners - SGTech, Singapore Business Federation, Singapore Corporate Counsel Association, Singapore Manufacturing Federation, and IPOS International, who have assisted us in disseminating the survey to their stakeholders.

We would also like to thank all participants involved, which due to the Chatham House Rule, we are unable to thank by name.

For all who contributed, this report would not have been possible without your valuable input.

Thank you. We look forward to working closely with you to support enterprises in protecting and managing their trade secrets as they compete globally in this era of rapid technological advancements.

The Intellectual Property Office of Singapore (IPOS) is the national authority that registers and is responsible for the administration of IP rights in Singapore. IPOS helps businesses use IP and intangible assets (IA) to grow and is committed to building Singapore into an international IA/IP hub. IPOS is a statutory board under the Ministry of Law.

Published September 2021

IPOS
INTELLECTUAL PROPERTY OFFICE OF SINGAPORE