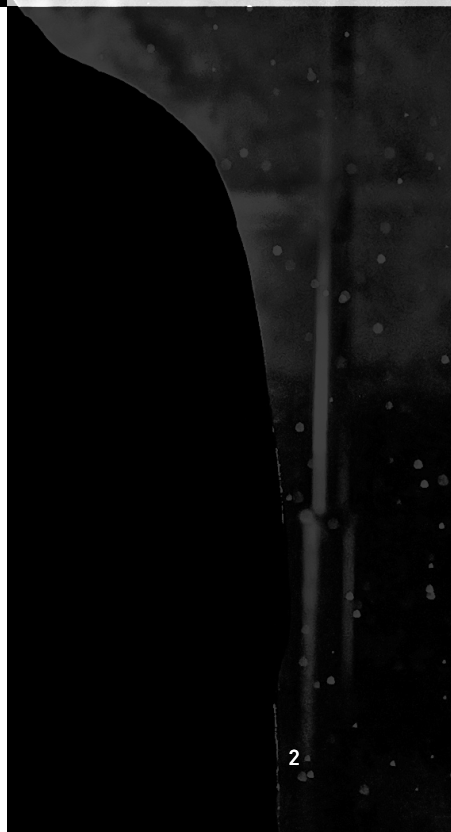
TRADE SECRET STRATEGY PLAYBOOK

Getting to grips with the growing challenges of managing confidential information

IAM SPECIAL REPORT

FOREWORD



The importance of trade secrets as both assets and as a form of legal protection has risen dramatically over the past decade. While patents have long been the key focus for IP teams at innovative companies, this new emphasis on knowledge and know-how is only likely to grow. Trade secrets are also rocketing up the agendas of business executives and IP professionals – yet despite this new awareness, company protection strategies are typically in an early stage of development. What is more, the management of proprietary know-how by disparate corporate departments is often less cohesive than is the case for other forms of intellectual property.

This special report takes a deep dive into trade secret law and strategy around the world, with the aim of creating an invaluable resource for IAM readers seeking not only to hone their protection approach but also to optimise their use of trade secrets as a business asset. To that end we include a range of pieces by acknowledged trade secret experts from law firms and leading business consultancies across the globe.

An understanding of international laws on protection and enforcement is key, so the report provides a robust collection of analysis of the legal and litigation landscape in the world's major jurisdictions. As well as illuminating US trade secret litigation trends since the introduction of the Defend Trade Secrets Act in 2016, we also provide a detailed analysis of enforcement actions at the International Trade Commission before moving on to take a closer look at the regimes in China and in the United Kingdom. To provide a truly international perspective, we also provide a Global Trade Secrets Tracker, which handily summarises the situation in 10 key jurisdictions.

But the 'how', as ever, is fundamental for IAM readers. With a view to cultivating a panoramic understanding of the topic, we asked some of the top experts in the field to provide actionable insights. These delve into valuation, strategies for identifying valuable know-how, tactics for preventing employee misappropriation in the age of the Great Resignation, and how to enforce legal protections across borders. The report also explores how companies should go about creating a joined-up trade secret strategy embodying all of these facets.

IAM is grateful to all the authors for their contributions to the report. IAM

CONTENTS

EXECUTIVE SUMMARY

1

2

3

4

5

In the United States, the Defend Trade Secrets Act has been game changing for rights holders since its introduction in 2016, with the additional layer of protection and enhanced enforcement powers creating a much-improved landscape. Benefits include the law's extra-territorial application and the possibility of *ex parte* seizures. More than $1 billion in damages have been awarded under the act thus far.

The picture is less clear in China. While the 2019 amendment to the Anti-Unfair Competition Law was intended to provide more robust protections for trade secrets, the win rate for plaintiffs remains worryingly low, as do damages awards. However, the newly reversed burden of proof could prove pivotal.

Trade secret protection and enforcement is made much harder by the international nature of trade, manufacturing and research – especially in this new era of remote working. Trade secret strategies must therefore be cross-border in nature and based on a concrete understanding of how data is shared internally, as well as with partners in different territories.

Such planning must go beyond enforcement tactics and policies to prevent disclosure. Identifying and harvesting proprietary know-how is crucial, as is understanding its commercial value and usefulness.

A holistic trade secret strategy is key. Not only should it incorporate the many functions involved in trade secret management – including R&D, IT, HR, legal and intellectual property – but it must integrate those functions into a coherent whole.

THE HOW AND WHY OF MANAGING TRADE SECRETS

While acknowledging the necessity of patents, international trade secrets expert James Pooley explains why a strong trade secret protection programme must be part of a business' IP protection strategy, and what makes a good one

We talk more about patents, but it is our secrets that we should be worried about. Control of confidential information has been key to business success for centuries. Long before patents were – so to speak – invented in Venice in the 15th century, China had a lock on the production of silk, which at the time was more valuable than gold. The Industrial Revolution brought a focus on the factory, guarding formulas and processes for transforming raw materials into commercial goods. But it has been the Information Age, in which data is the raw material, that has made us fully appreciate the critical importance of trade secrets. Indeed, while companies have always gathered data about how to improve their business, these days data collection and analysis are forming the core of their business models – think Amazon and its algorithmic understanding of your buying habits.

According to a 2021 report from the National Science Foundation, businesses view trade secrets as more valuable than patents, by a significant margin. Across enterprises of all sizes and industries, 23% consider trade secrets as important, while utility patents lag far behind at 8%. You might say that is because the sample includes businesses that have no real interest in intellectual property. But when you sharpen the focus on companies that engage in R&D, the preference for secrecy remains, with 76% seeing trade secrets as very or somewhat important, and just over 50% assessing patents that way.

"Critical to the success of any information security programme is recognising that rules and technological controls are only a part of the picture"

This does not mean that patents are fading away – there is nothing quite as powerful as the ability to exclude others from using your invention. But over the last 15 years in the United States, we have experienced an erosion of patent enforcement through court decisions, along with a lift for trade secrets from the America Invents Act. That statute effectively removed the requirement that an inventor reveal the 'best mode' of an invention, allowing implementation details to be retained as a trade secret without risking the invalidation of the patent. The law also expanded prior user rights to all areas of technology, making it safer for a company to choose secrecy for technology that might later be patented by someone else. These developments have helped shine a light on trade secrets – not necessarily as an alternative, but certainly as a more robust companion to patent protection.

Although we now recognise these information assets as extremely valuable, how to manage them is not so obvious. Many people inside and outside a company must have access to these assets, usually through electronic systems for storage and communication that are inherently insecure. Therefore, if you are faced with this challenge, a lot of your effort will be spent simply on not losing control of what you have. But equally, sensible management requires that you realise the potential of your data to enhance enterprise value, by ensuring that managers focus on putting it to work in the business.

Fine, you might say, but how do I do that? I am comfortably familiar with the registered rights, I know what they are, I can count them, and there are accepted ways to value them and to sell the ones I do not need. In contrast, managing information sounds like tying string around a cloud. Where do I start?

First, some good news: the legal requirement for establishing a trade secret aligns very well with achieving the corporate purpose of protecting and exploiting it. The basic law expressed in Article 39 of the TRIPs Agreement requires only "reasonable steps" to maintain secrecy of information that provides some commercial advantage. National laws reflect this fundamental policy to protect information so long as the business has taken reasonable measures to keep it confidential. But what does 'reasonable' mean? One recognised implication is that perfection is not required, otherwise any act of misappropriation would prove that you had failed to do enough. The law accepts that you cannot anticipate every kind of mistake or misbehaviour by those whom you have trusted with access.

In effect, the law expects what the company's board expects: that management will exercise ordinary prudence under the circumstances to protect assets of the business. That means that you identify and analyse the risks and make a thoughtful determination about how to eliminate or reduce them. In other words, the framework for proper handling of trade secrets is nothing more than an application of classical risk management. One useful example of this sort of risk-based approach can be found in the Cybersecurity Framework published by the National Institute of Standards and Technology. Although originally directed at protection of critical infrastructure such as the financial system and energy grids, the institute's framework has been used as a general information security guide by businesses of all sizes in a variety of sectors.

Objectives for a trade secrets programme

As with any sort of strategic corporate exercise, establishing a trade secret protection programme begins with defining objectives.

Prevent loss

This is the classical objective: you have a secret formula and you want to keep the competition from learning it. But the issue is more complicated than just locking it up because you have a business to run. Employees need access, as do business partners, potential acquirors, suppliers and customers. The focus is on maintaining control in those relationships so that the risk of any improper use or disclosure is reduced.

Avoid contamination

No risk is a one-way street – this applies equally to information belonging to others that is received by the organisation, either through a structured exchange under NDA, or unintentionally, as when a high-level employee is hired from a competitor. Your objective here is to keep any competitor's confidential information out of your systems and operations unless it is there with permission and you have procedures in place to protect it.

Demonstrate importance

The structure – and especially the implementation – of an information security system will signal to both insiders and outsiders the significance of this issue for the company. And proof of a robust programme will help establish the "reasonable efforts" in case you need to go to court to enforce your trade secret rights.

Enable value creation

By definition, trade secrets can extend to information of potential value in a business. But that value will only be realised if there is someone in management who is tasked with ensuring commercialisation of the secret, either through internal use to increase the quality or profitability of outputs, or through a collaboration or other external transaction. In the old corporate patent committee, the innovations not chosen for filing were often forgotten. In the current competitive environment that is unacceptable.

Building a team

With clarity of purpose established, you begin the process by identifying a leader of the programme and assembling a cross-disciplinary team of managers of each business unit and of relevant functional areas such as physical security, IT, HR, legal, R&D, marketing and supply chain management. The ultimate objective will be the establishment of a strategy and set of policies that adequately address the company's information security needs, in the context of the unique risk environment it faces. Actual preparation of policy documents, however, comes later. At the outset, the responsibility of this group is to:

- identify the organisation's most valuable secrets (the crown jewels, if you will);
- determine the risks associated with those assets (including the risk of failing to exploit them); and
- the available options to reduce those risks to an acceptable level.

We should pause here to consider a common question: why not just find out what other companies in the same industry are doing and do that? Although there is nothing wrong with trying to benchmark security measures, be aware that it is difficult to gather meaningful data. That is partially due to the fact that many companies prefer not to share their means and methods, but more importantly you will at best be getting information about what they think is appropriate for their secrets in their particular risk environment, which is likely to be different than yours. At worst you will be copying a checklist that was copied from another checklist, full of latent flaws. All this is a reflection of the basic truth that there is no one-size-fits-all approach to information security management; every organisation needs to understand and meet its individual needs.

In my experience the most productive way to do that is to pull together the cross-functional team in the same room. It is certainly possible to begin with individual interviews. But a real-time conversation among the most knowledgeable managers almost always produces better results, as each of them, speaking from their distinctive experience, catalyses insights and suggestions from their peers. This initial process does not require an offsite retreat; usually two to three hours is sufficient to set parameters, share ideas and agree on a way forward, led by the appointed champion. Normally the results will be reported back and expanded in further meetings and interviews, until there is enough consensus to begin drafting documents.

Identifying what to protect and areas of risk

Having determined the participants, let us return to the agenda, which begins with identifying the most critical secrets. Even though the overall process is sometimes referred to as an 'audit' or 'inventory', it is not necessary, indeed it is futile, to try to boil the ocean by creating a list of every bit of confidential information at the company.

Instead, ask the participants to describe the four or five categories of information which are most likely to keep them awake at night when it comes to maintaining their advantage over competitors. The conversation will lead quickly to a discrete list which can be enhanced with observations about relative value (how important is this in comparison to other assets), time value (how quickly the sensitivity of this information might degrade) and the various ways in which secrecy might be lost. As to each category, the group should ask themselves: given our business model and current operations, what can go wrong

in the handling of these assets that might compromise their integrity? How likely are such events to happen, and what would be the impact on the business if they did? An open discussion, often facilitated by counsel to preserve the option of applying a privilege, will usually unearth vulnerabilities and threats that had not previously been considered.

All of this naturally leads to a discussion of risk mitigation techniques although that does not necessarily happen at the first encounter where the primary objective is to agree on what is most important and most at risk and why. But at some point, management has to confront the reality of the identified risks and decide how best to mitigate them. That involves balancing the likelihood of threat reduction against the cost of various techniques, either in terms of money or, more often, in terms of inefficiency or annoyance. All security measures come with a degree of inconvenience, and part of the job of management is to appreciate the pain threshold of the workforce, who may react with non-compliance. In addition, there are cultural or indirect productivity issues that may counsel against tighter security, as when management perceives that their engineers work more effectively through open collaboration, supported by freer information flows.

To better understand how information security is operationalised, it can help to look at a few examples of common areas of concern. One of the most obvious is employees, through whom most information loss occurs. This is not because they intend to steal, but because they have the deepest exposure to the company's secrets, and without sufficient management are likely to misunderstand or be careless. This is particularly challenging for staff who have been taught by social media that sharing information is a good thing. Here the risks are generally organised into three parts, representing the lifecycle of employment.

In the recruiting and onboarding phase, the company faces risks from bringing on experienced talent from the competition. Depending on the specific competitive environment and individual involved, the risk of contamination may be acute, calling for scrubbing by counsel to ensure that both the recruit and their new colleagues understand the necessary protocols.

The second phase of risk reduction for employees is in their training and others forms of management communicating its expectations of their behaviour. Thorough, frequent training may be the single most effective way to avoid misunderstanding and increase awareness about the employee's role in maintaining secrecy.

The third phase, naturally enough, is termination. The exit process represents the employer's final opportunity to communicate the seriousness of the treatment of confidential information, and to discover information about the employee's next position, in order to identify more specific risks that call for additional measures, such as reaching out to a new employer to negotiate assurances.

Another common area of risk for many companies is their external relationships. These might be long term (eg, with a supplier), or relatively brief (eg, a possible licensee or acquisition partner). Particularly with the more exploratory transactions, the sharing of confidential information is fraught with risk. If the deal does not go through, the company has placed some of its valuable information assets in the hands of a third party, typically with no protection beyond their good faith compliance. And if the NDA on which the transaction is based has been treated as a trivial form rather than a consequential contract, it is likely that the NDA itself will carry risks resulting from poorly drafted terms or negligent compliance by both sides. A risk management plan for any business that engages in these information-sharing relationships (which is to say most companies in most industries) will have to take a hard look at how they have been managed and how they can be improved.

A third example of information security risk involves distant supply chains, which are difficult enough to manage in normal times, but have recently been disrupted by trade wars and the pandemic. When these suppliers have been entrusted with confidential information in order to fulfil their duties, it can be challenging to maintain control over that information as they look for other sources of revenue in an uncertain market. This puts a premium not only on how those relationships are defined by locally enforceable contracts, but also by how they are managed in order to reduce the risk of misappropriation.

As these examples demonstrate, identifying and addressing the various dimensions of information security risk can be complex and demanding. But preservation of what is often the company's most valuable asset class deserves close and consistent attention, especially when – as is usually the case – the risk environment is dynamic. If the company has invested in a comprehensive analysis of the sort outlined above, it should be sufficiently informed to create a plan that fits its unique needs.

Building a plan

Typically the plan will be documented as part of an existing corporate strategy, along with a suite of policies designed to communicate and enforce the company's commitment to protection of its own data and respect for others'. These policies will provide guidance in all areas that touch on trade secret risk, such as facilities security; IT system external protections, access controls and device management; employee on-boarding, training and exit procedures; data classification and handling; and third-party relationships. For organisations that handle large amounts of personal consumer data, or that deal with sensitive government programs, the related security issues will be coordinated.

Critical to the success of any information security programme is recognising that rules and technological controls are only a part of the picture. Secrets are handled by people who do not automatically follow rules and who may be inclined to look for ways to defeat restrictions. Therefore, success often depends on the quality of the managers who have been tasked with responsibility for oversight of trade secret issues. Normally programme implementation and feedback will be handled by the heads of relevant business units, but there should be a central manager with overall accountability for making the programme work and continuing to engage with the control group to ensure that it is modified periodically as experience dictates. Just as no trade secrets programme comes off the shelf, so none can remain static and still be fit for purpose.

No system is perfect and there will always be leaks, but you want your bucket to have fewer, smaller holes than your competition. In the modern enterprise, trade secrets need attention on a level that is at least equal to the registered forms of intellectual property in order to preserve information assets and the business opportunities they represent. IAM

James Pooley is a former deputy director general of WIPO; he serves as an expert witness and advisor on trade secret management and dispute resolution (james@pooley.com)

"In the modern enterprise, trade secrets need attention on a level that is at least equal to the registered forms of intellectual property"

ABOUT IAM

IAM is the leading intelligence platform for the global IP market. Our unrivalled coverage and in-depth analysis of key sectors gives our clients critical information to enable them to maximise the value of their IP assets.

Our unique and timely intelligence, analysis and data service informs high-level corporate decision making, while our extensive connections with senior operators in the corporate, legal, policymaking and investment worlds provide a clear line of sight into market developments before they are widely known.

IAM offers global coverage of the IP value creation environment. Our worldwide team of reporters, researchers and analysts provides unmatched understanding of local markets in North America, Europe and Asia to ensure that IAM is the first to provide the analysis that matters.

Contact us

London
Holborn Gate
330 High Holborn
London WC1V 7QT
United Kingdom
T +44 20 7234 0606
info@iam-media.com

Hong Kong
1901, 19/F Dominion Centre
43-59 Queen's Road East
Wan Chai
Hong Kong
T +852 3956 1600
info@iam-media.com

Washington DC
2122 P Street NW
Suite 201
Washington DC 20037
United States
T +1 202 831 4654
info@iam-media.com

IAMSPR_SPCLRPT_Q422

FURTHER READING

Trade secret strategy and management

- Trade secrets strategies are falling short, suggests EU study (13 October 2022)
- Embracing the trade secrets buzz (8 September 2022)
- Trade secret developments that chief IP officers need to know about as they grapple with 'Great Resignation' (24 February 2022)
- The trade secrets revolution may only just have got started (31 July 2021)
- Protecting trade secrets using non-disclosure agreements (12 April 2017)

US trade secret landscape

- Palantir seeks client-attorney discovery in case involving alleged IP litigation fraud (9 May 2022)
- Samsung slams "betrayal of trust" by former IP head (22 February 2022)
- Damages track upward in US trade secret litigation (25 June 2021)
- With US trade secret litigation on the rise, a new suit from Intel follows an increasingly familiar storyline (29 November 2018)
- Data sheds much-needed light on the trade secrets litigation landscape (1 June 2018)
- Defend Trade Secret Act to bring consistency to trade secret litigation (18 May 2016)

US International Trade Commission

- Why ITC actions are an increasingly important tool for life sciences IP owners (16 May 2022)
- As "Great Resignation" continues, ITC deserves a closer look from trade secret owners (19 March 2022)
- AbbVie heads to the ITC in dramatic final battle over Humira biosimilars (10 January 2022)
- Trade secret dispute between LG Chem and SK Innovation shows power of the ITC (6 January 2020)

Trade secrets in China

- What a successful trade secrets case in China looks like (26 April 2022)
- Big global IP owners wary of proposed trade secret rules in China (3 November 2020)
- Enforcing patents and trade secrets in China (22 October 2022)
- China fast-tracks changes to trade secret law ahead of further talks with Trump administration (25 April 2019)
- The viability of trade secret protection in China (6 April 2016)

Trade secrets in the life sciences

- Diagnosing the patent and trade secret strategy behind a biotech company's success (22 September 2022)
- GSK case shows US authorities mean business on biotech trade secrets (6 May 2022)
- Pfizer acts quickly to tackle alleged covid-19 vaccine trade secrets misappropriation (25 November 2021)

Trade secrets and covid vaccines

- WTO to push for greater covid-19 compulsory licensing flexibilities (5 May 2022)
- TRIPS covid vaccine IP waiver proposal fails to address crucial questions (20 April 2021)