Trade Secret Audits

DAVID COHEN, KIDON IP AND DONAL O'CONNELL CHAWTON INNOVATION SERVICES LTD, WITH PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

Search the Resource ID numbers in blue on Westlaw for more.

A Practice Note addressing audits of a company's trade secrets, which provide insight into whether a company is effectively managing its trade secret portfolio to bring value to the company. This Note discusses the audit process so counsel can gather and consider relevant information from multiple and diverse sources to develop a deep understanding of their client's trade secret situation and to confirm that the company can accurately and fairly describe its trade secret portfolio and the value it provides to the company.

Companies generally obtain significant value from conducting an intellectual property (IP) audit. However, an audit's quality is a function of the quality of the audit's measurement and assessment criteria. While it is important to conduct IP audits periodically, it is also more important that an audit be conducted so it can be compared to prior and later audits.

IP audits are even more challenging when a company seeks to audit its trade secrets and take a proactive, systematic approach to assessing its trade secret portfolio in a comprehensive manner. This Note discusses the trade secret audit process and identifies key issues to address during the audit so the company's key business, technical, and legal personnel can apply their respective skills, knowledge, and experience to aid in the audit.

For more information on trade secrets generally, see Trade Secret Laws: State Q&A Tool.

For more information on other forms of IP, see Box, IP Summary Comparison Chart and Practice Note, Intellectual Property: Overview (8-383-4565).

For more information on patent and trademark audits, see Practice Notes, Patent Portfolio Audits (W-000-7106) and Trademark Audit.

RATIONALE FOR CONDUCTING A TRADE SECRET AUDIT

A well-conducted trade secret audit:

- Provides the client with a complete picture of its trade secret portfolio.
- Helps ensure the trade secret owner's compliance with requirements and deadlines for maintaining trade secret rights.
- Helps the client identify and take corrective action concerning potential risks to its trade secrets.
- Enables the client to make informed decisions concerning management of the trade secret portfolio.
- Makes it easier for the client to identify and describe relevant trade secrets in future litigation.

Besides the above benefits, companies also should consider conducting a trade secret audit because:

- IP law has been evolving (see The Changing IP Law Landscape).
- Technology advances change the calculus concerning IP protection (see Changes in Technology).
- Cybercrime is increasing (see Cybercrime).
- Companies are increasingly engaging in open-innovation, which raises certain risks for the company (see Open Innovation).
- Actions by governmental authorities may affect how companies operate (see Government Action).

THE CHANGING IP LAW LANDSCAPE

In addition to being good IP management practice, companies should conduct a trade secret audit because of evolving IP law, including:

- The Defend Trade Secrets Act (DTSA) (see Trade Secret Law).
- The Leahy-Smith America Invents Act (AIA) (see Patent Reform).
- Certain changes in the law outside the US (see Law Outside the US).

Historically, companies may not have appreciated the significance of trade secrets but these changes in IP law are rapidly changing that perception, as shown by the increase in trade secret litigation (see Lex Machina Releases New Trade Secret Litigation Report, July 18, 2018).

Trade Secret Law

Trade secrets are governed by both:

- Federal law in the DTSA.
- State law. Each state (except New York) has adopted the Uniform Trade Secrets Act (UTSA).

The DTSA (18 U.S.C. § 1836, et seq.) was enacted on May 11, 2016 and provides another tool for IP owners to protect their trade secrets. It is broader than the USTA because it does not limit the kind of information that can qualify as a trade secret, although, like the USTA, the DTSA places the burden on the trade secret owner to use reasonable measures or efforts to protect the trade secret.

UTSA	DTSA
§ 1(4): "Trade secret" means information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value ... from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.	18 U.S.C. § 1839(3): ... the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information;...

For more information on the DTSA and its effects, see:

- Article, Expert Q&A on the Defend Trade Secrets Act and Its Impact on Employers (W-002-2128).
- Article, The DTSA Turns One, But What Has It Done? (W-007-9652)
- Defend Trade Secrets Act (DTSA) Issues and Remedies Checklist (W-003-6953).
- Levine, The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act, 53 WFLR 105, 153 (Spring 2018).

Patent Reform

US patent laws and practice continue to evolve and change, most notably for:

- Patent subject matter eligibility. Determining whether some inventions, especially certain computer-implemented and life-sciences inventions, are eligible under Section 101 of the Patent Act (35 U.S.C. § 101) for patent protection is an important consideration. For more information on patent-eligible subject matter, see Practice Note, Patent-Eligible Subject Matter: Overview (1-525-8503) and Section 101 Patent Eligibility Toolkit.
- Post-grant patent trials in the US Patent and Trademark Office (USPTO). The AIA created various new proceedings at the USPTO allowing the USPTO to reconsider the patentability of previously issued patents. For more information on AIA patentability trials, see Practice Note, USPTO Post-Prosecution Patentability Proceedings (9-553-6247) and PTAB Proceedings Toolkit (W-002-2510).

The increased likelihood of a patent being challenged on Section 101 grounds or in a post-grant USPTO proceeding make it more likely that companies are going to rely more heavily on trade secret protection for their innovations.

Law Outside the US

In addition to changes in US law, counsel should be at least aware that:

- China updated its Anti Unfair Competition Law on January 1, 2018, which provided:
  - a broader trade secrets definition more in line with international norms;
  - clarity on how the law impacts third parties in disputes; and
  - increased fines for violation.

  (See 5 Eckstrom's Licensing in For. & Dom. Ops. § 29:73.)
- In Europe the EU Directive on trade secrets was enacted across all member states on June 9, 2018. This directive:
  - standardizes the national laws in the EU member countries concerning trade secret misappropriation;
  - harmonizes the trade secret definition with existing international standards;
  - defines relevant forms of misappropriation; and
  - clarifies that reverse engineering and parallel innovation are allowed.

US counsel should retain foreign counsel to address trade secret issues outside the US. However, it is clear that trade secret protection is a viable tool outside the US and many jurisdictions are strengthening trade secret law (see Stibble, International Trend Toward Strengthening Trade Secret Law, 26 No. 4 IPTLJ 18 (April 2014)).

CHANGES IN TECHNOLOGY

A significant engine of innovation, at least in the high-tech industry, is cloud-based and other internet-based technologies. These technologies may be relatively easy to reverse engineer or copy as compared to other technologies. This is especially the case if a patent discloses their innovative features.

In the past, this supported an argument for protecting those technologies with a patent instead of trade secrets. However, in the current IP environment where it is challenging to enforce patents covering computer-implemented inventions or the infringer may be outside jurisdictions where patents can be enforced, many cloud-based technology innovators are increasingly using trade secrets to protect aspects of their innovations that do not have to be publicly disclosed (see Halligan, *Trade Secrets v. Patents*: The New Calculus, 2 No. 6 Landslide 10 (July/August 2010)).

CYBERCRIME

Cyber criminals:

- Leverage different approaches and techniques to identify a company's information technology (IT) network vulnerabilities.
- Constantly seek to steal various organization's trade secrets.

These cyber attacks, including hacking of business websites and computer systems, can be extremely damaging, particularly if security is breached and confidential business and personal information compromised.

For more information on cyber attacks, see Practice Note, Cyber Attacks: Prevention and Proactive Responses (3-511-5848).

OPEN INNOVATION

Traditionally, most companies:

- Engaged in internal innovation.
- Kept their discoveries highly secret.
- Did not incorporate into their internal developments any information from outside their own research and development laboratories.

This attitude is known pejoratively as the "Not Invented Here Syndrome."

However, recently companies in different industries have begun to experiment with different innovation processes, including:

- Outsourcing innovation to independent contractors as innovators or innovation-facilitators. With this approach, companies use various agreements addressing confidential information and IP ownership. For an example pro-company independent contractor agreement, see Standard Document, Independent Contractor/Consultant Agreement (Pro-Client) (2-500-4638).
- Accepting information, ideas, and technology from outside the company to augment and aid in the company's own research and development. Although this approach may accelerate the company's development life cycle, it can raise many legal obligations and risks because it requires sharing and collaborating on trade secrets. For more information on the legal risks involved in open innovation, see Article, Managing Unsolicited Idea Submission Risk for Open Innovation (5-549-7865).

Both these innovation models:

- Raise challenges for trade secret protection, which an audit may be able to address.
- May result in intangible innovations that may leave the company because of its highly mobile and transitory workforce. For more information on employers and trade secret protection, see Trade Secrets and Confidential Information Best Practices at Hiring Checklist (5-505-7753).

GOVERNMENT ACTION

Many governments around the world are addressing IP rights in their tax policies. For example:

- The recent US tax reform:
  - lowers the corporate tax rate, which encourages US companies to repatriate their IP back to the US;
  - moves the US toward a territorial system of taxation for foreign income; and
  - introduces new concepts for taxing income derived from intangibles.
- For more information on the 2018 tax reform legislation, see Legal Update, Sweeping Tax Overhaul Enacted (W-012-3642).
- The Organization for Economic Co-operation and Development (OECD) instituted new rules for base erosion and profit shifting (BEPS) and transfer pricing, which may significantly:
  - impact the accounting for trade secrets; and
  - increase the pressure for companies to have up-to-date trade secret protection policies and processes.
- For more information on BEPS and transfer pricing in the context of trade secrets, see Practice Note, Trade Secret Valuation: The OECD and BEPS (W-019-2083) and Transfer Pricing (W-019-2083).
- Patent box tax regimes, the particulars of which change periodically, exist in many countries to provide an incentive for companies to develop and commercialize patented technology in the country. For example, in the UK, an optional reduced corporate tax rate is available in certain situations. For more information on the UK Patent Box, see Hill, The Patent Box as the New Innovation Incentive for the Several States: Lessons from Intellectual Property-Tax Competition, 42 AIPLA Q.J. 13, Winter 2014. Some countries provide this tax incentive for other forms of IP, such as for trade secrets and know-how.

A trade war, which can be linked to trade secret theft concerns, is also a risk factor for most companies. For more information, see Article, Five Trends in Geopolitical Risk for Investors to Watch in 2018 and Beyond (W-013-0385) and Office of the United States Trade Representative, Update Concerning China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation, November 20, 2018.

THE KEY PHASES OF TRADE SECRET AUDITS

A trade secret audit typically includes the following phases:

Planning	The party conducting the audit, such as inhouse or outside counsel or other relevant specialists, proposes, discusses, and agrees on a comprehensive project plan with the audited company.
Communication	Distribution of a general communication that defines: ■ Expectations and employee obligations. ■ Applicable project details.
Interviews	Interviews of key individuals.
Data Gathering	Collection of trade secret related documents, including: ■ Trade secret policy, product and process description, and protection mechanisms. ■ Key employment agreements and human resources and IT policies.
Data Analysis	Analysis of data collected from the interviews and documents.
Reporting	Distribution of a report setting out the audit's findings and recommendations.
Wrap Up	Address any outstanding issues.

TRADE SECRET AUDIT'S KEY COMPONENTS

The key components of a trade secret audit, include an audit of the company's:

- Trade secret policies and procedures (see Trade Secret Policies and Procedures).
- Trade secret portfolio (see Trade Secret Portfolio).
- Associated costs and valuations (see Associated Costs and Valuations).

TRADE SECRET POLICIES AND PROCEDURES

This part of the audit is simply to identify the company's:

- Corporate trade secret policy.
- Procedures and systems that address employee education and governance.

Counsel can evaluate these to ensure they are sufficiently robust and suitable for trade secret protection. If not, counsel can then identify appropriate enhancements the company should include. For more information on protecting trade secrets, including model presentation materials and employee agreements, see:

- Practice Note, Protection of Employers' Trade Secrets and Confidential Information (5-501-1473).
- Standard Document, Confidential Information Policy (W-005-2678).
- Standard Document, Employee Confidentiality and Proprietary Rights Agreement (6-501-1547).
- Standard Document, Notice of Immunity Under the Defend Trade Secrets Act (DTSA) Provision (W-003-5261).
- Standard Document, Protecting a Company's Confidential Information and Trade Secrets: Presentation Materials (8-617-5966).

TRADE SECRET PORTFOLIO

This part of the audit identifies and examines each trade secret and any associated metadata to determine if the trade secret:

- Should be maintained as a trade secret.
- Meets the criteria necessary for trade secret protection.

Some companies resist this trade secret identification and analysis because they may be concerned that:

- Allowing people, whether third-party experts or company employees, access to a company's "crown jewels" puts the trade secrets at greater risk than necessary.
- Defining its trade secrets before any trade secret misappropriation litigation:
  - limits what it can claim was misappropriated in later litigation; and
  - forces the company to prematurely address tax, securities, and financial reporting obligations for its intangibles that may later harm the company.

While these concerns may have been justified in the past, recent changes in the legal and accounting rules make this "know-nothing" approach to its trade secrets increasingly risky.

Counsel may also be able to mitigate some of these concerns by using a generic trade secret identifier with its associated metadata, which summarizes basic information about the trade secret, such as:

- Dates of creation.
- Responsible parties.
- Location.
- Parties with access.
- Governing agreements.

Using trade secret metadata can aid in trade secret management and audits.

ASSOCIATED COSTS AND VALUATIONS

The audit should also focus on the trade secrets' costs and valuation, including the methodology used to determine these results. For more information on trade secret valuation, see Practice Note, Trade Secret Valuation (W-019-2083).

TRADE SECRET MANAGEMENT LEVEL

A critical goal of the audit is for management to gain an understanding of the company's trade secret management activities and how it may compare to the company's peers. For example, the following provides useful categories describing a company's trade secret management activities, which may improve or degrade over time.

Level 0:	No trade secret policy, process, or governance.
Level 1:	Ad-hoc and chaotic approach to trade secret management.
Level 2:	Basic trade secret policy, process, and governance in place.
Level 3:	Formal policy, process, and governance defined, followed, and managed.
Level 4:	Level 3 plus the company's policies, process, and governance structure extend outside the company, such as to suppliers and collaboration partners.
Level 5:	Level 4 plus company is also BEPS compliant (see Government Action).

TRADE SECRET AUDIT QUESTIONNAIRE

The trade secret audit should address the following topics and questions:

Topic	Clarification and Key Points of Inquiry
Awareness and Education	■ What is being taught about trade secrets, to which persons and by which persons? ■ How is this educational material kept current? ■ What records of trade secret education exist within the company?
Trade Secret Definition	■ What trade secret definition does the company use? ■ Is it consistent with the legal and tax definitions of trade secrets?
Policy	■ Is there a trade secret policy in existence? ■ How does it compare and contrast to a 'template'?
Process	■ Is there a trade secret process description? ■ If so, does it cover all the key stages (identification, review, protection, maintenance)? ■ Does it link to other processes within the company, such as HR, IT, finance, security, sourcing or procurement, legal, and IP? ■ Is the trade secret process actually in use across the company? ■ Is the process consistent across all parts of the company?
Qualification	■ On what basis does certain information within the company qualify as a trade secret?
Trade Secret Classification	■ Are trade secrets classified in any way, and if so, how is this done?
Trade Secret Policy Ownership	■ Which person is responsible for the trade secret policy and its implementation across the company?
Trade Secret Process Ownership	■ Which person is responsible for the trade secret process and its implementation across the company?
Access and Access Controls	■ How is access to the company's trade secrets controlled?
Protection Mechanisms	■ What administrative, legal, and technical protection mechanisms are deployed to protect the trade secrets? ■ Are these protection mechanisms actually in use across the company?
Sharing Trade Secrets With Third Parties	■ Are trade secrets shared with others and if so, how is this managed? ■ Are third parties provided access in any way to trade secrets? ■ How are trade secrets handled in company agreements?
Third-Party Trade Secrets	■ Are there trade secrets belonging to others entrusted to the company? ■ If so, how are these managed and controlled?
Trade Secret Valuation	■ Has the company determined the value of its trade secrets? ■ If so, why, how, when, and by which person?
Trade Secret Portfolio Management System	■ Is there a trade secret portfolio management system or tool in use? ■ If so, what is the system, and what are its key features and functions?
Trade Secret Metadata	■ What trade secret metadata exists within the company? ■ How does the company use this metadata?
Previous Audits	■ Has the company ever conducted a trade secret audit? ■ If so, what was the nature of those audits? ■ What were the findings?
Audit Trails	■ Can the company determine the prior status and value of its trade secrets? ■ If so, how?
Governance	■ What is the company's trade secret governance structure? ■ Which persons participate? ■ Is there a budget for trade secrets? ■ Are trade secret costs tracked? Is so, how? ■ Are there targets set? Are there key performance indicators used? ■ What management attention is given towards the company's trade secrets?

Topic	Clarification and Key Points of Inquiry
Tax	■ Is any information on trade secret assets shared with the company's finance or tax functions or governmental tax authorities? ■ If so, please provide some details.
Disputes	■ Have there been any trade secret disputes involving the company? ■ If so, how have these been resolved? ■ What lessons have been learned?

TRADE SECRET AUDIT REPORT

The trade secret audit report is the formal report providing the company with the audit findings, which the company may use for financial reporting, investing, altering operations, enforcing accountability, or making other decisions. The report should identify:

- The trade secret management standards used to maximize the value of trade secret assets.
- Any deficiencies in the company's trade secret management.
- The evidence used to evaluate the company's trade secret management and why it does not conform to the specified benchmark.

The report should therefore provide sufficient information so the company can take concrete steps to improve its trade secret management.

AUDIT REPORT STRUCTURE

The audit report should include:

- A cover page.
- A table of contents.
- An introduction.
- An executive summary.
- The definition of a trade secret.
- An explanation of why trade secrets are growing in importance.
- A background to the trade secret audit.
- A description of the methodology used.
- Key findings.
- Recommendations.
- Information about the auditors.
- An appendix, which may include the audit's questions and answers.

GENERAL CONTENT CONSIDERATIONS

Beyond identifying any shortcomings in the company's trade secret management, the report should:

- Identify areas where the company's trade secret management is working appropriately in addition to any shortcomings. This may allow the company to apply some current processes to other areas needing improvement.
- Identify high-risk areas and currently compliant areas at risk of falling out of compliance or that may be improved.

The report should include clear definitions of key terms, both for the audit process and the relevant technical and business issues and use those terms consistently. This enhances the future use of the audit report.

Counsel should also consider whether to use the word "audit" or "assessment" when referring to the audit. Sometimes, people react negatively to the word "audit," assuming that the audit is merely an exercise to determine if the company passes or fails a trade secret management test. Therefore, counsel should understand:

- How company personnel are to receive the audit activities and consider ways to describe the process as value enhancing.
- The report's recipients and their knowledge of the language the report is using.

TRADE SECRET MANAGEMENT BEST PRACTICES

The audit report can compare and contrast the company's trade secret management with best practices, which include:

- Employee education on trade secrets.
- A trade secret policy outlining the company's general approach to trade secrets.
- A robust fit-for-purpose trade secret process, including a governance structure.
- Trade secret access controls.
- Reasonable protection mechanisms, including a mix of administrative, legal, and technical protection mechanisms.
- Trade secret provisions in agreements.
- Use of a trade secret management system.
- Good quality trade secret metadata.
- Associated cost and valuation data.
- Third-party assessment when sharing trade secrets.
- Action plan when trade secrets are misappropriated.
- Network of external trade secret specialists, such as cyber security, insurance, and legal experts.

AUDIT REPORT FOLLOW-UP

The trade secret audit report, with its findings and recommendations, should not be simply filed away with no follow-up. If the company is not at the desired level, it should determine the needed investments in time and money to address the report's recommendations and undertake efforts to improve its trade secret management to obtain the appropriate value from its trade secret portfolio.

IP SUMMARY COMPARISON CHART

	Trade Secret (18 U.S.C. and state law)	Patent (35 U.S.C.)	Copyright (17 U.S.C. and state law)	Trademark (15 U.S.C. and state law)
Requirements for Protection	■ Secrecy, so it is not generally known or available to others. ■ Reasonable efforts to maintain secrecy. ■ Value due to secrecy.	■ Patent-eligible subject matter. ■ Novel. ■ Nonobvious. ■ Useful. ■ Patent adequately discloses the claimed invention.	■ Independent creation. ■ Modicum of creativity. ■ Fixed in a tangible medium of expression. ■ No protection for ideas, facts, or useful articles.	■ Performs source-identifying function. ■ Inherent or acquired distinctiveness. ■ Priority of use. ■ No protection for generic words or functional features.
Basis for Liability	Acquisition by improper means or violation of confidential relationship.	Making, using, offering to sell, selling, or importing claimed invention.	Actual copying and substantial similarity.	Likelihood of confusion or dilution.
Defenses	Independent discovery, reverse engineering.	Invalidity, inequitable conduct, first sale, experimental use.	Fair use, independent creation, first sale.	Abandonment, descriptiveness, fair use, first sale.
Remedies	Injunction, damages, including statutory damages for registered copyrights, and potential criminal liability except for patent infringement.			

For more information on other forms of IP, see Practice Notes:

- Copyright: Overview.
- Patent: Overview.
- Trademark: Overview.

04-19