Business secrets, high potential assets under development

Executive Summary

The importance of business secrets has increased pursuant to the evolution of new paradigms (such as the growing value of data and the development of IT and AI in innovation) and to the creation of a legal protection in many countries and more recently in the European Union and in France. In addition, one must underline that the present digital era creates high risks of illegitimate confidential information disclosures by human error or cyber attacks, as compared to the economy of past decades. Consequently, Business secrets should be at the heart of any company's strategy to protect and value its key confidential information and data procuring a competitive advantage. The value and the need to protect these business secrets as a particular asset are generally implicitly recognized in enterprises but not yet fully established.

This article aims at explaining how confidential information can be a business secret benefiting from a legal protection and, as a consequence, how its value and even its recognition as an intangible asset can be established to the benefit of the company and its users. The authors have chosen to refer to business secrets in line with the French expression "secret d'affaires", as it seems to offer a wider approach than the expression "trade secrets" used in some national laws. All these assets relying on highly secured business secrets can also be at the basis of immediate business value, not only of future value, for instance in R&D that leads to innovative business models and value creation in strategic alliances, competitiveness, reputation, expertise exposure, etc. High Growth Enterprises are naturally particularly concerned, but medium and small businesses or even start-ups should not underestimate their interest either. In conclusion, the governance of business secrets is worth the investment despite its apparent burden for companies.

Introduction

In today's knowledge-driven economy, recognition, understanding and management of intangible assets has become one of the most important value drivers for any type of enterprise, regardless of size. The specific attention given to patents and other registered IP led to poor value recognition and management of other less obvious "assets" despite their value, such as know-how, methods, algorithms, and more generally, of sensitive confidential information, business or trade secrets. The development of the digital industry and of artificial intelligence tools, the critical need for innovation, the development of collaborative platforms for projects and R& D programs and of open data, the evolution of the economic war in particular with cyber attacks, the increase of mergers and acquisitions around the world, have significantly modified companies' vision vis-à-vis trade and business secrets. Awareness of the "commercial" value of such trade secrets and development of a legal status, after many years of lobbying in France and in the European Union for example, are now clearly driving enterprises towards the recognition of its importance for the sustainable development of companies if not, sometimes, for their survival. Globalization, and acceleration of business cycles and digitization, made a primary value-creation driver from the need to protect these competitive advantages. In addition, the growth of cyber-attacks obliges companies to be able to identify the stakes related to the data impacted. This is pushing towards their recognition as intangible assets.

This change of approach gives birth to a need to organize specific policies for their value assessment and protection.

Identifying, protecting and assigning a value to business secrets is a challenge requiring a new culture, a transversal approach and specific methodologies, processes and tools. Therefore, we propose to draw first a focus on the meaning and scope of business secrets today (I), to have a basis to identify why business secrets have or can have a value (II) and finally to present the benefits from a business secrets data governance policy in addition to an intellectual property policy (III).

1. What does "Business Secrets" mean today?

1.1 The development of business secrets

Historically, business practices broadly included management of patents on the one hand, and of confidential information on the other hand. But for the past ten years the status of secrets has changed considerably, under the pressure of various factors:

- The growing importance of innovation;
- Trends towards open access, aiming at developing open science, innovation, law, etc. as levers towards collaborative innovation;
- Significant scientific progresses in digital methods and algorithms;
- Yield in fraud, espionage and cyber-attacks, due to fierce competition and economic war;
- Globalization of companies;
- Limitation of patent protection strategies due to instantaneous digital access to any type of information worldwide.

Protecting business secrets has now become intrinsic and is even critical to the evolution of society, leading to the need for a cultural shift. The European Commission, in the preamble of the 2016 Directive, underlined the strength of the ongoing economic war justifying therefore the attention to pay to business secrets: "*Innovative businesses are increasingly exposed to dishonest practices aimed at misappropriating trade secrets, such as theft, unauthorized copying, economic espionage or the breach of confidentiality requirements, whether from within or from outside of the Union. Recent developments, such as globalization, increased outsourcing, longer supply chains, and the growing use of information and communication technology contribute to increasing the risk of those practices*."

The United States have organized the protection of their companies' trade secrets under the Economics Espionage Act of 1996[1], leading to very strict processes and constraints (e.g. ITAR regulations) to manage critical technical information. Trade secrets are defined broadly to "*include any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others. Combinations and compilations of known elements in the public domain are protectable as trade secrets. Novelty is not required. The actual or threatened misappropriation of trade secrets can be enjoined*."[2].

In China, the Anti-Unfair Competition Law (2019 revised, AUCL) is the principal law regarding trade secrets, which defines and regulates what is a trade secret, its misappropriation, and the

[1] 18 U.S. Code CHAPTER 90—PROTECTION OF TRADE SECRETS https://www.law.cornell.edu/uscode/text/18/part-I/chapter-90.
[2] R. Mark Halligan, Protecting US Trade Secrets Assets in the 21th Century, 2013. https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2013-14/september-october-2013/protecting_us_trade_secret_assets_the_21st_century/.

corresponding legal liabilities, etc.[3] "*The AUCL defines a trade secret as technical, operational or other commercial information unknown to the public that is of commercial value and for which the owner has taken corresponding confidentiality measures. Technical information generally refers to technical solutions obtained by way of scientific and technological knowledge, information and experience, while business information generally refers to various types of business information that can bring competitive advantage to right-holders other than technical information*"[4].

The European Union adopted recently, the 2016/943 Directive (EU) of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against unlawful acquisition, use and disclosure. The EU noticed that there was no harmonized system for the protection of trade secrets union-wide, but mainly contractual liability laws, in particular in relation to employees. The European directive aims, therefore, at standardizing national laws in EU countries against unlawful acquisition, disclosure and use of trade secrets, and at harmonizing the definition of trade secrets in accordance with existing internationally binding standards. It also defines the relevant forms of misappropriation and clarifies that reverse engineering and parallel innovation must be guaranteed, given that trade secrets are not a form of exclusive intellectual property right.

France has, according to the European directive, adopted on July 31st, 2018[5] a law for the protection of trade secrets. As a consequence, article L 151-1 of the French Commerce Code enounces that, in brief, any information can benefit from legal protection as trade secrets if it is i) confidential, i.e. not generally known to the public nor easily accessible to specialists of this type of information, ii) embodying commercial value whether effective or potential due to its confidential status and iii) protected by reasonable measures to preserve holder's confidentiality.

The variety of valuable information and data of a company can even lead to the use of the word "business secrets" rather than of the one of "trade secrets" to ensure the widest possible coverage for a better understanding. The focus must indeed be made on the criteria to satisfy to have the legal status. ***In the present article, we will use thereafter the expression "business secrets" as it appears to be more adapted than "trade secrets"***.

To benefit from legal protection, the scope of business secrets must be clearly stated. "Information" is to be understood broadly as it covers data or else in any format and on any media (paper, material, digital, etc.). The following classification (Figure 1) is an example of major business secrets[6].

[3] R. Mark Halligan, Protecting US Trade Secrets Assets in the 21th Century , 2013.

[4] Yi Xue, Trade Secrets 2020, April 23, 2020. https://www.justice.gov/usao-edpa/pr/second-former-glaxosmithkline-scientist-pleads-guilty-stealing-trade-secrets-benefit

[5] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037262111/.

[6] More examples : "Secret des affaires, comment bénéficier de la protection de la loi du 31 juillet 2018, CCI Guide pratique", p. 6. (https://www.cci-paris-idf.fr/sites/default/files/etudes/pdf/documents/guide-secret_des_affaires.pdf).

Figure 1: proposed classification of business secrets. All company departments are concerned.

In case business secrets derive from innovation (inventions, algorithms, know-how, methods, etc.), Figure 2 below shows how they lead to various types of assets. This approach is interesting to have in mind as a new trend appears where many companies, generally process-oriented, decide not to file patents for strategic reasons: to bypass the time limit of the protection or simply because detection of infringement is difficult or impossible, meaning counterfeiting can never be legally proven. They prefer to classify some inventions as business secrets.

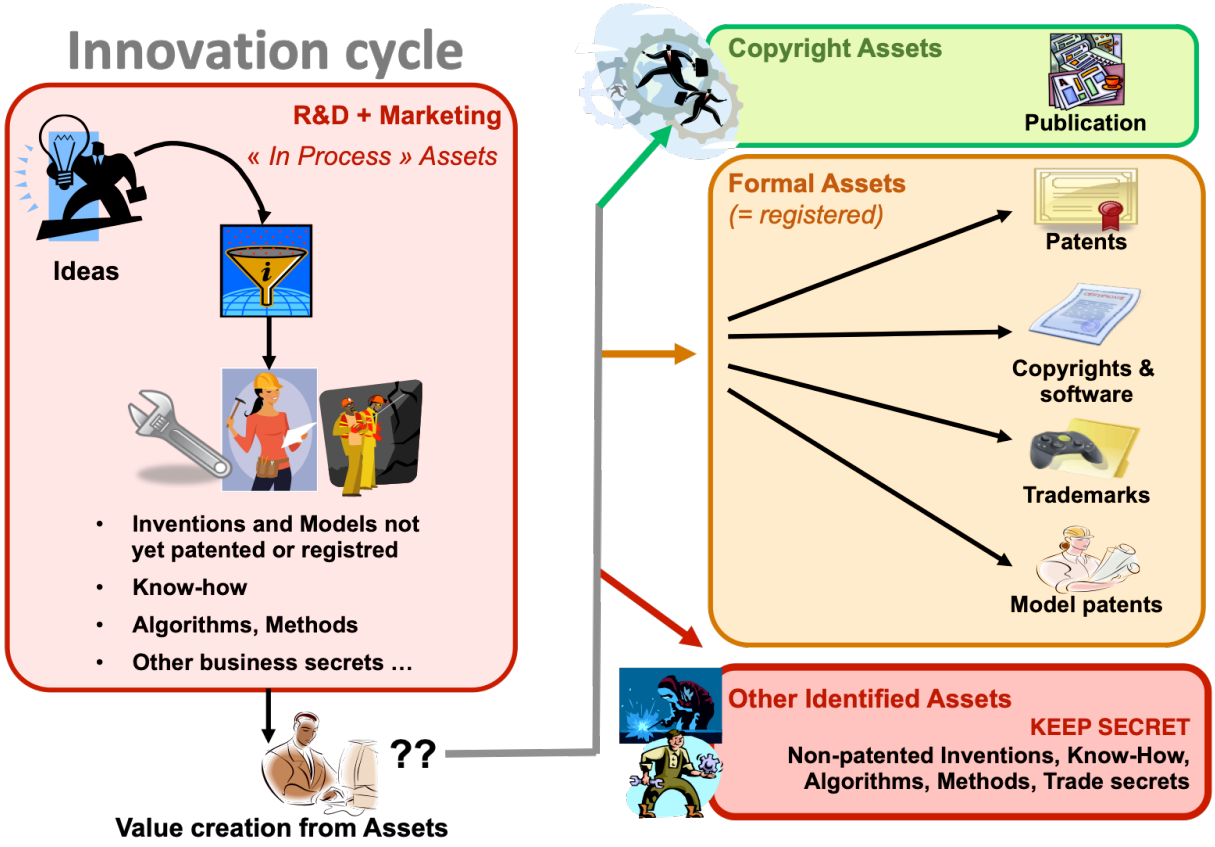

Figure 2: business secrets related to innovation

The development of legal protection for business secrets generates a significant change for companies **as all company's departments are now concerned** as shown in the non-exhaustive example in table 1 below**.** The historical method of management of patents on the one hand and of non-disclosure agreements on the other hand must be modified to ensure that most or all business secrets benefit from the available legal protections.

Executive Committee	Commercial Department	Manufacturing and Quality Department	R&D Department	Purchasing Department	IT Department	Legal, IP and Conformity Department	Financial Department	Human Resources Department
Decisions	Method of calculation f prices	Products Technical specifications Acceptable quality tolerance levels	R&D programs	Expression of needs	IT security measures	Board of directors meeting minutes	Change policy	Employees 'list
Organisational chart	Commercial proposals	Manufacturing processes Quality methods	R&D partners, make vs buy arbitrages	Pricing policy	Codes and algorithms	Contracts	Banks 'list	Declaration of accidents
Planning	Margins	Production volumes Quality levels targeted	R&D roadmaps, milestones and results	Suppliers 'list	IT processes	Disputes	Loans conditions	Minutes of meeting with employees' representatives
Company's objectives	Customers list	Target costs structure, ppm delivered, total quality performance, client satisfaction, KPI's	Unpatented Inventions, new markets targeted, new patents volume	Panel reduction, supplier qualification criteria		Attorneys 'list	EBIT targets	Employees turnover Salaries growth rate

Table 1. Non exhaustive mapping of company's departments production of business secrets

1.2 Why do business secrets become important?

The recent evolution of the importance of business secrets is explained by 2 major factors: the evolutions of innovation and of law.

The nature of innovation has changed in particular with the development of software and artificial intelligence systems, followed with or preceded by methods, processes and new uses, the evolution of materials making for example, bills of materials and formulae critical. In addition, operating processes and organization, marketing and sales, business models, management of social aspects became also critical. Innovation, results of which are coveted by competitors, is more than ever a key lever for companies. Some inventions in these new digitally affected fields are not patentable or would be insufficiently protected by a patent as counterfeiting can be difficult to detect. Some may be protected by copyright (for example, a method of diagnosing flood risks in the building industry to decide where to locate real estate becomes a real business that generates profits) but it is not a sufficient protection, since it protects them from a "servile" copy, whereas companies want to prevent such innovation from unauthorized use and exploitation. Thus, secrecy is a more relevant solution. In a nutshell, innovation plays today a special role by being at the crossroads of numerous transformations for which intangibles are key factors, hence business secrets as well. Therefore,

approaching business secrets by focusing on innovation is, on the one hand, a real **sign for awareness of their potential** as intangible assets, and, on the other hand, an actual **tool that implements** this potential, allowing companies to stand out, to last, to share and to transmit.

The use of the criteria "commercial value" in laws on trade secrets obliges companies to specify a value for the confidential information, when possible, if they want to benefit from the corresponding legal protection. Interestingly, the criterion "commercial value" does not limit legal protection to information that can be sold to a third party on a new or established market. The intent is to protect information that procures a competitive advantage as underlined by the European Commission[7]. This incentive to demonstrate the "value" of business secrets creates a virtuous cycle leading to the development of methodologies and, as a consequence, to their potential recognition as intangible assets as we will show in the next section.

2. An asset on its way to recognition

Companies have historically focused value creation and value assessment of their intangible assets mainly on patents and customer relationship to evaluate sustainability of their business income. But the trend is changing, as the importance of business secrets increases. To recognize business secrets as an asset, a new culture and methods to estimate their value must be developed.

2.1 A new culture to develop

Assessing the value of software, codes, methods and algorithms, formulas, list of components, etc. recently expanded. But defining the commercial value of know-how and other types of confidential information is still a new field to explore. This means that cultural or organizational barriers must be overcome to facilitate such evaluations. Enhancing the value of a company's business secrets requires taking an **active and continuous interest** in them, which in turn compels stakeholders to reinvent themselves and set up adapted governance.

The challenges for companies are to deal with **mass of information and data** having a potentially **fluctuating status** (as shown in Figure 3 below) and **a fluctuating value** (as presented below).

[7] https://ec.europa.eu/growth/industry/policy/intellectual-property/trade-secrets_en.

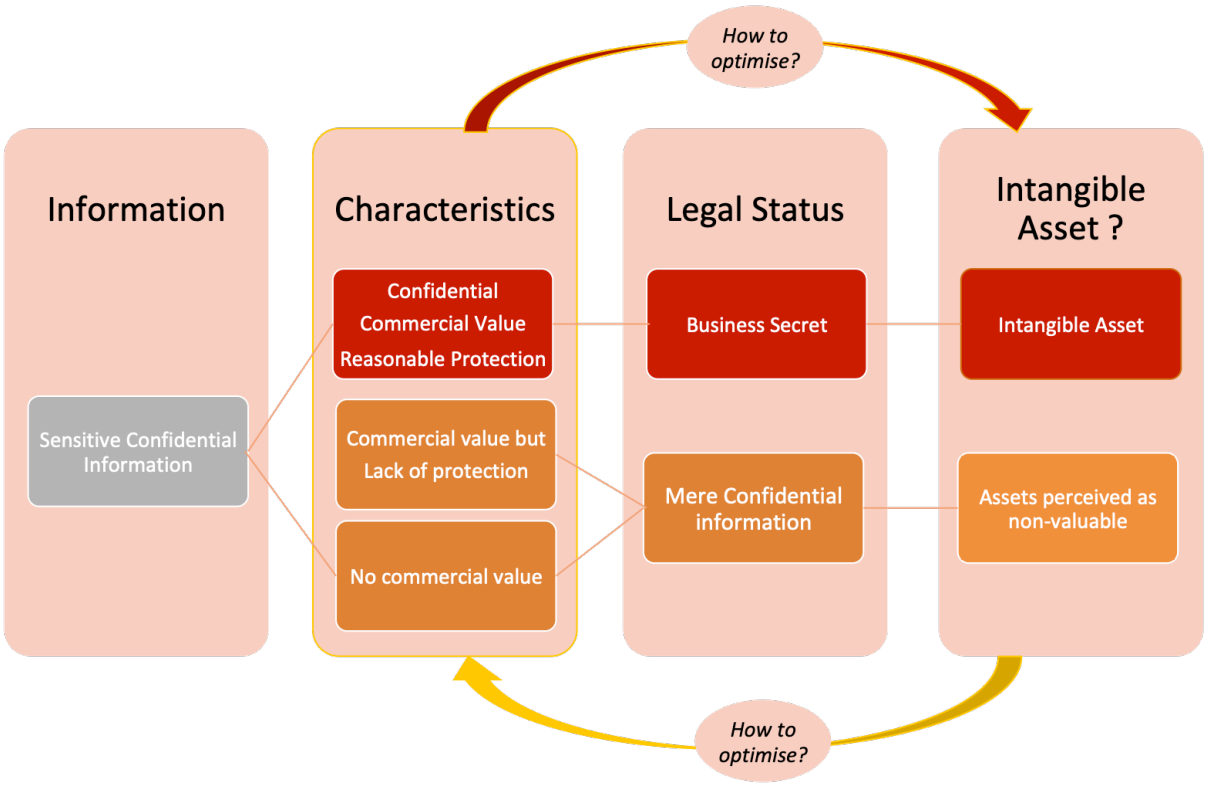

Figure 3: Fluctuating status of information and data

Up till now, some companies treated their confidential information value via risk management (potential damages) rather than using an opportunity approach (value). Consequently, the intrinsic value of confidential information was not systematically determined. Its qualification as intangible asset was even less considered. In general, the value of any intangible asset is derived from the future benefits it will generate. But this may vary depending upon the type of confidential information:

i) Information reserved to a company's internal benefit is generally hard to value because its contribution to the actual revenues is difficult to quantify. This difficulty is compounded by the absence of "similar" or "comparable" transactions;

ii) Information that is part of the products and services sold can have an intrinsic value depending upon the competitive advantage it procures; except for that which is reserved by essence or by contract to a single customer in the defense field for example;

iii) Information that is under development continuously evolves as stand-alone know-how or as related to one or several invention sources patented or not, making its formalization highly difficult; therefore, assessing a commercial value becomes quite hard or even impossible. Conversely, a strategic characteristic of an asset is that commercial value shall emerge from future customers or partners, who might purchase the asset (i.e. the business secret itself) or obtain a license for its exploitation.

In other words, a paradigm shift emerges that relates to how companies understand business secrets and intangible assets:

- ✓ All valuable Business secrets should be managed: business secrets management is not often part of companies' data management, except through a knowledge management (KM) repository for some specific secrets;
- ✓ For scientific business secrets, the level of maturity of an invention on the TRL Scale

("Technology Readiness Level") has a clear impact on evaluating income flows;

- ✓ The debate opposing intangible assets and informational assets has shown its limits. Indeed, this distinction led to concentrating efforts on valuing intangible assets only. Some confidential information is generally part of "hard to value intangibles", and thus is not reported as part of a specific assets. The protection of business secrets will change this situation;
- ✓ The lack of established legal protection for business secrets, up to recently, is an explanation for the low level of efforts put by companies to appreciate their value;
- ✓ There may be financial and legal debates disclaiming the status of "asset" for some business secrets. But data being the new precious metal of the 21st century, the recognition of its value may give rise to changes in its legal status[8].

2.2 How to estimate the value of business secrets?

To evaluate a business secret, various transversal factors must be taken into account from different fields, such as quality of innovation, technology readiness level (TRL), competitors' R&D strategies, company's attractiveness for M&A, etc.

The evaluation should include all business secrets having a commercial value and all exploitation by co-owners, licensees and other beneficiaries. A difficulty is that certain myths persist, such as the one that says know-how, for example, is neither quantified nor quantifiable, or also that it cannot be assigned a financial value. It is often part of what is called the "informational assets " of the company, which is a big catchall that is viewed to escape company classification and quantification processes. In addition, the potential attractiveness of business secrets for third parties may have to be determined in their original field of use ("market innovation") and in other fields of use ("derivative innovation").

The R&D organization is also impacting business secrets value. Collaborative developments (like "Wiki" processes), suppliers relations, or joint developers web portals, efficiently mobilize stakeholders' resources and knowledge, and mechanically create value by allowing each partner to access the knowledge, know-how, formal IP assets, etc. developed by or acquired from others. The business secrets on these portals may have different values for the owner (or joint owners) and for the users. Part of the benefits resulting in the development may be immediately quantifiable, others may remain "qualitative" for some time, but value creation in such contexts is undoubted. A business secret in the form of an invention (patentable or not), yet to prove its capacity and potential, has less value than an invention already industrialized, since it has longer and less predictable payback. Such invention can climb up the TRL scale, with sometimes unforeseen and unforeseeable steps. Know-how for example, should be seen as an ever-increasing stock fed by information exchanges that would generate income flows, if realized and associated to other complementary assets, be they tangible or intangible.

Whatever the type of business secrets emerging from R&D projects, capturing their value demands to:

i) Specify in the R&D and consortia agreements the foreseen exploitations with an update mechanism, in order to introduce those which become reasonably foreseen,

ii) Organize the follow-on of the exploitation really made. Some rights are granted to third parties with no consideration at the beginning, because the value is difficult or

[8] La protection du patrimoine informationnel de l'entreprise, Antoine Gendreau in Manuel d'Intelligence Économique, Puf 2019, p.317 – 318.

impossible to estimate. Value and profits may arise afterwards, but only if a follow-on is organized.

In other situations, such as licensing or M&A, measuring the financial value of such a business secret may be a must if it is a competitive advantage to the company. This demands execution of a thorough qualitative assessment of the extra-financial value, showing that both a financial value and an extra financial value (e.g. estimated by a set of KPIs) are essential, and in effect, complementary.

2.3 Can certain business secrets be recognized as bona fide assets?

Two types of principles can become a difficulty in obtaining recognition for the stock value of business secrets as intangible assets:

1) « Only the flows are measurable », which does not reveal the full underlying value:
   - Inventory values = result of a flow calculation in relation to a conventional benchmark;
   - In the same way that mass or energy balances are fundamental in physics, chemistry or process engineering, the stock is seen as a reservoir from which a flow can be extracted.
2) It is most likely much easier to find a method for separating flows rather than for separating stocks:
   - The different intangible assets interact with each other (i.e., through flows);
   - This disrupts the notion of "extractable value of a stock" in case of strong interactions.

The advantage of flows is that they behave more often as unit quantities over time, as opposed to stocks, which are usually the result of the integration or balance over time of multiple flows. There are many ways of classifying these flows; for example the 7 flow classes inspired by the V3 method [9] (*Flow 1: shareholders – company, Flow 2: human potential of key people, Flow 3: internal collective potential, Flow 4: external human relational potential, Flow 5: relational flow suppliers partner competitors, Flow 6: customer relations, Flow 7: societal and environmental*).

As a result of these, real wealth is perceivable once a measurable level exists, i.e. it results from observing the information and financial flows between companies' assets and their ecosystem. The flows then appear as links between internal sources of value creation (*organization, infrastructure, equipment, IP and knowledge, reputation*) and external sources of value creation (*shareholders, talents, customers, etc.*) In the end, this shows a dynamic of attractiveness and potential capacity to efficiently exploit company's assets. The following diagram (Figure 4) illustrates this differentiation between ecosystem, flow capital [15] and stock or capital[10.]

[9] La Méthode V3 (« Vision, Valeurs, Volonté »)**, Joyeux, Portnoff, Lamblin.**
https://www.futuribles.com/fr/groupes/methode-v3/

[10] For definition and nomenclature of Capitals, see for example WICI (https://www.wici-global.com/) or International <IR> Framework (https://integratedreporting.org/resource/international-ir-framework/)
And also " Référentiel français de mesure de la valeur extra-financière et financière du capital immatériel des entreprises".
http://observatoire-immateriel.com/wp-content/uploads/2015/11/Thesaurus-Volet-1.pdf

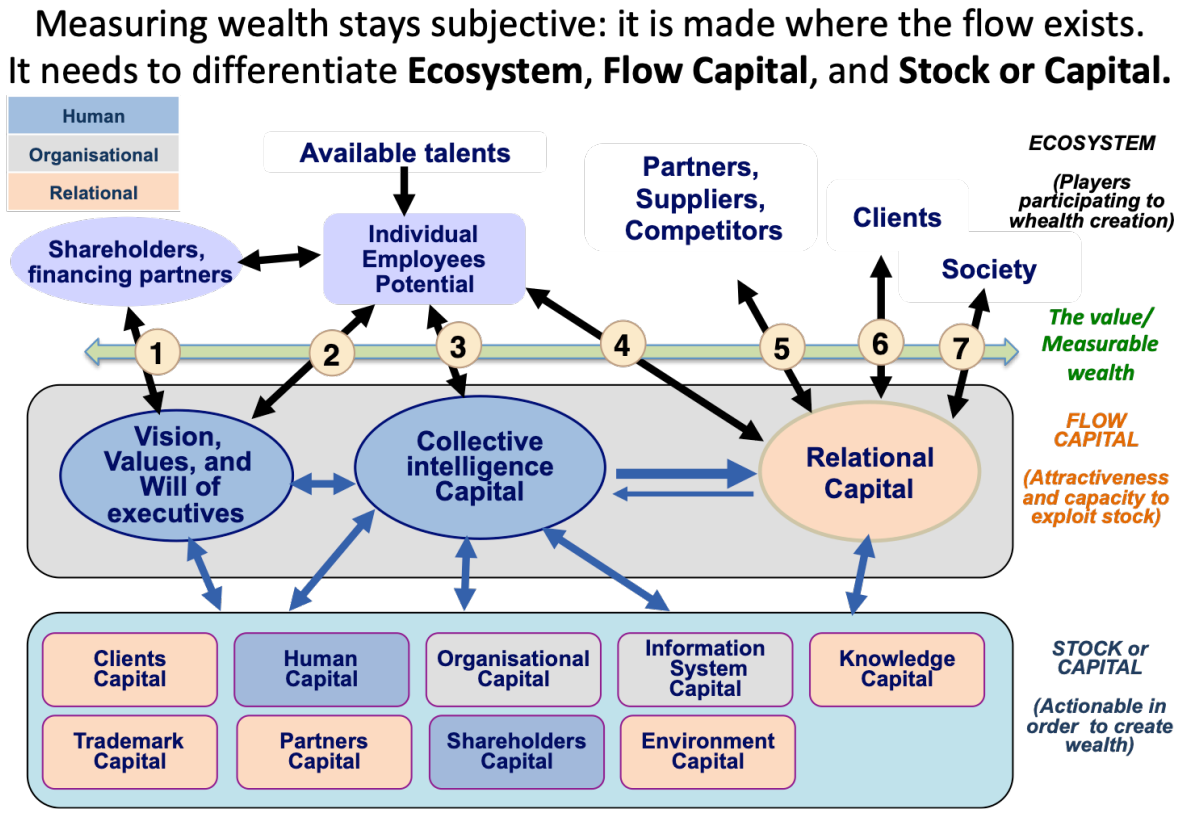

Figure 4 Differentiation between ecosystem, flow capital and stock or capital

Therefore, business secrets should be considered as intangible assets or capitals, whether recognized in balance sheets or not. One way of looking at them is as reservoirs or stocks of knowledge, interconnected with other assets by information flows.

Nevertheless, trying to assess how these may or may not enter the balance sheet is a significant challenge, due to some remaining hard tasks:

- Recognition, in agreement with accounting standards,
- Valuation of the assets, in cash value (e.g. determined from the revenues or cost savings they will generate over time),
- Valuation of the information flows, in cash value /year.

To assess the status of an intangible asset, should we consider a stock value or a flow value? Asset flows can be defined as the interactions between asset holders that can be measured and compiled in order to assess wealth creation (= potential value creation). It is unusual, except for example in social Systems Theory (e.g. Luhmann's approach) to speak of flows between assets (for example, a key know-how, once it is capitalized, passes from human capital to organizational capital), because the notion of intangible assets was first born from the search for a value that was unrevealed by the organizations. Indeed, most current asset value methods assume that asset value decreases in time due to an amortization mechanism; however, considering a number of assets, among which business secrets, it can be shown that their flow value could increase over the years, just by measuring flow intensity that results from using these assets in the business.

As a result, flows, whose intensity reflects the attractiveness of assets and the capacity to exploit them, become as important as assets (capital that can be mobilized for wealth creation), just as labor

becomes as important as capital. Some authors[11] put forward the notion of non-market wealth creation to account for the revolution in society with the advent of digital technology: social networks and generalization of "like" buttons on the Web create unrivaled new metrics that can be used to measure wealth creation of specific products or services through flows of "like" clicks. Yet, this assertion of "non-market wealth" of data is itself still evolving, since data has increasingly acquired an undeniable market value, due to the raise of artificial intelligence (AI) and its "big data" inputs on virtually all of economic sectors.

In the case of know-how for example, estimates are difficult to fit smoothly into accounting reporting standards, because of the intrinsic uncertainties impacting the economic flows that characterize them. Valuation methods for intangibles are based either on historical costs, or on discounted future revenue streams, or else on benchmarks of observed "comparable" transactions; these three approaches remain heuristic, producing opinions and confidence intervals rather than fixed values, leading economists and IP valuation experts to regularly debate their effective robustness. Valuation of intangible assets is thus a delicate exercise, widely discussed, highly dependent on assumptions such as the utility curve of potential buyers facing the seller, the date of assessment, and [12] the expertise of the evaluators. This leads to intrinsic uncertainties, either up or down, on the value determined at a specific moment and in given circumstances. This is obviously true for value assessment of a patent, which is already an asset of high recognition.

Nevertheless, it remains promising and possible to demonstrate, for a number of business secrets, that they have a commercial value, simply by specifying the potential interest of competitors to obtain such information, or by demonstrating the loss the company would suffer in case of disclosure either for the initial goals and the target markets or for other markets known or emerging, should development efforts lead to innovations unrelated to the initial goals (e.g. "side ground"). Whenever these assessments are performed, it appears that the management ratio "value to cost", even in orders of magnitudes, proves it is urgent for companies to organize governance for business secrets. But is the effort worthwhile?

3. A governance to organize

3.1 Why a governance for business secrets and for which benefits?

Practically, such governance is recommended when a company wants to[13]:

[11] http://www.fondapol.org/etude/vincent-lorphelin-la-republique-des-entrepreneurs/ (La République des Entrepreneurs, Vincent Lorphelin, janvier 2017)
https://www.advisorengine.com/blog/design-led-organizations-in-wealth-management
(How design-led organizations are transforming the wealth management space, Rafal Czapski on October 10th, 2019)
https://www.pwc.com/us/en/financial-services/publications/assets/pwc-fsi-whitepaper-digital-wealth-management.pdf
(Digital wealth management: Driving engagement through data-driven insights, PwC, January 2018)
https://knowledge.wharton.upenn.edu/article/the-user-experience-why-data-not-just-design-hits-the-sweet-spot/
(The User Experience: Why Data – Not Just Design – Hits the Sweet Spot, Wharton University of Pennsylvania, Feb. 2016)
https://www.oecd-ilibrary.org/docserver/9789264037472-en.pdf?expires=1600879924&id=id&accname=guest&checksum=1C23FF5A7CE338E44051D8B7662C5BA7
(Participative Web and User-Created Content - WEB 2.0, WIKIS AND SOCIAL NETWORKING)
https://core.ac.uk/reader/42142490
(THE USE OF SOCIAL MEDIA AND ITS IMPACTSON CONSUMER BEHAVIOUR:THE CONTEXT OF HOLIDAY TRAVELJOHN N. FOTISA, PhD thesis, MAY 2015, BOURNEMOUTH UNIVERSITY)
https://www.researchgate.net/publication/263566377_The_Like_Economy_Social_Buttons_and_the_Data-Intensive_Web
(The Like Economy: Social Buttons and the Data-Intensive Web, November 2013, New Media & Society 15(8):1348-1365)

[12] European Commission, Final Report from the Expert Group on Intellectual Property Valuation, 29th November 2013.

[13] Other examples: Donal O'Connell, IPEG Consultancy, 2015

- Benefit from legal protection to defend its business secrets from unauthorized use or attacks;
- Allocate resources between several types of tangible and intangible assets and complete the census of intangible assets;
- Impose clear obligations on employees and third parties for protection of business secrets;
- Prevent losses in case of employee's departure;
- Optimize traceability to prevent unauthorized disclosure and use;
- Reduce costs by setting various appropriate levels of protection;
- Optimize storage for costs, energy and risks of error saving;
- Organize insurance protection thanks to a data management policy.

The benefits of organized governance may be as follows:

1. **Creating new value**: certain "assets" are recognized for accounting purposes and enrich the balance sheet;
2. **Boosting innovation**: knowing what you already own can be a source of inspiration;
3. **Optimizing resources and time** by adapting the protection of business secrets to their sensitivity. Time and money can be saved as efforts will be concentrated on business secrets instead of on all confidential information;
4. **Facilitating the authorization of publication** and disclosure to third parties;
5. **Facilitating the destruction of data** out of the secrecy map;
6. **Increasing the level of protection of secrets**: the advent of the digital economy creates high risks of illegitimate disclosure of confidential information through human error, risks and cyber attacks that are totally new if we compare them with those of the last decades. A single leakage of secrets could destroy an enormous value for a company. In addition to human errors, web-based business intelligence now uses powerful artificial intelligence (AI) tools, which easily identify and exploit any publicly released information, be it legitimately disclosed or not. Due to these powerful tools, company executives should now realize that once a secret is erroneously disclosed, the whole world would immediately know about it and exploit it as if it had been voluntarily publicized. Employees and third parties may also be more easily warned of secrets' legal status and obliged to comply with specific protective measures;
7. **Increasing the level of royalties** the company should collect: the follow-on of the effective use of right to exploit can favor such collection;
8. **Enabling a faster and more effective response** (legal and/or operational) to looting, counterfeiting and/or unauthorized use: the company will be able to demonstrate quickly that its concerned business secret satisfies the legal criteria in case of litigation. Crucial questions may still remain such as how can one evaluate the damage for a company and for its contractors, whose confidential information was made public by human error or malicious deeds?

3.2 How to implement business secrets governance?

To achieve the benefits mentioned, the following actions can be implemented:

a) Specify a group policy: despite the variety of laws applicable to a company or group, the company governance can be built on the basis of the highest applicable legal standard, and then adapted to

https://www.ipeg.com/trade-secrets/#:~:text=A%20trade%20secret%20is%20therefore%20defined%20as%20any%20information%20that%20is%3A&text=It%20must%20have%20commercial%20value,information%20to%20keep%20it%20secret.

local laws and regulations where necessary with a chart comparing legal definitions and processes.

b) Deploy the policy over 3 fields: any company's efficient secrecy policy should be audited and enforced among all critical partners and stakeholders in the supply chain. The KPI's chosen to validate compliance and identify dysfunctions should be shared by at least all "critical" stakeholders as shown in Figure 6 (Fields of Business secret governance).

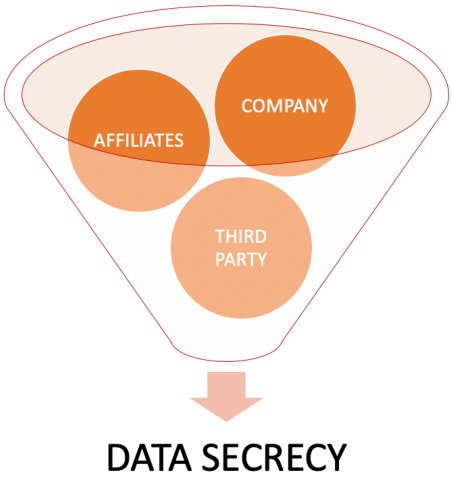

Figure 6 (Fields of business secret governance)

c) Organize cross-cultural collaboration between several functional departments and business units (cf. Table 1 above). It involves the legal and intellectual property department, all departments producing or receiving information, IT, security, HR and insurance; in a nutshell, the whole company. Only the combination of inputs from these departments and business units makes it possible to build up a consistent policy meeting all legal criteria. Besides, it also suggests new management behaviors, an evolution of the ethics charter, new data management rules, new IT hardware and software policy.

d) Detect secrets: verify their status as business secrets as per the applicable law or as mere confidential information.

e) Map the business secrets, starting with know-how and key algorithms and formulas. The mapping should be made in forms that can be used to support operational decisions for protection or disclosure. An efficient Knowledge Management system, which provides an obvious "repository", eases the management of such data and therefore their protection. Some digital tools or methods available on the market help to set up this governance. Several are easily adaptable to fit the decision support of any specific company process. Specific methods, such as the CLAIRE® method by LEX Colibri, can be used to map the innovations, their components, history and logical links, particularly in collaborative research and development programs where the traceability of ownership and exploitation is a critical issue with high value stakes. The following steps should be followed:

- ✓ ***Define a typology*** (e.g. classify know-how into a logical and understandable hierarchy);
- ✓ ***Classify past, present and future confidential data*:** the work can be split in 2 phases to be conducted in parallel or in sequence for company's confidential information and data[14] depending upon their data:

  . The *past i.e. confidential information generated* by the company or received from a third party prior to the enforcement of the applicable law. As this protection may vary from

[14] Cartographie des secrets d'affaires : quelle démarche mettre en œuvre ? Véronique Chapuis-Thuault, Le Secret des Affaires, Sophie Schiller, dir. Actes Pratiques et ingénierie sociétaire n°169, janv-fev 2020, p 15 et s.

one country to another, a precise analysis should be made per relevant country in addition to the general one specifying the standard of reference. Attention must be put on the most important confidential information disclosed and the conditions for their disclosure.

. *The present and future confidential information* which may or may not be a business secrets as per the applicable law as shown in Figure 5.

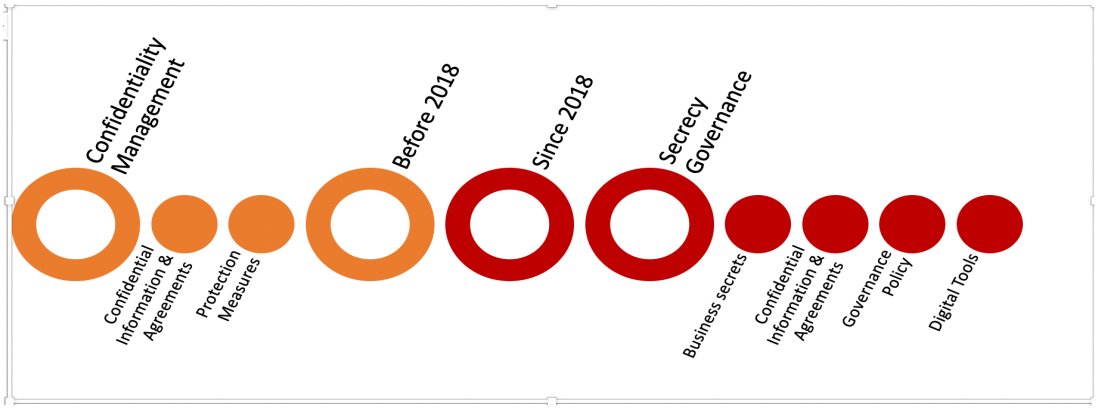

Figure 5 Legal historical chart for France

- ***Specify levels of criticality***: as the stock of data can be quite substantial, it is useful to pay attention first to confidential information holding substantial value. It is advised to request from each company's department to list their **top ten business secrets and the top ten of their stakeholders**. Then an analysis can be made as per the relative **criticality levels**. Depending on companies' strategy, adopting a gradual approach, one can select business secrets characteristics and countries of operation using 3 types of criticality levels with varying degrees of impact, value, and life cycles:

1. Vital and essential data	The disclosure of which can have irreparable impact and result in companies' destruction or in significant loss leading to bankruptcy
2. Competitive advantages	The loss of which can have costly, but not irreversible, consequences
3. Non-vital secrets	Secrets which still need protection because their *disclosure or exploitation by third parties could still be detrimental* to the company

Thereafter, a check must be made of the consistency of protective measures with the level of criticality of business secrets.

f) Organize traceability: census or mapping, (creation of a typology) for management and traceability purposes, using the criticality levels in particular by formalizing key know how and ensuring that all work and inventions produced are stored on company's data management system rather than on employees' computers. Ensure that the same is made with deliverables from contractors.

g) Estimate the value creation potential and the actual Value creation potentials that can be achieved, and then act on them at the right time with full knowledge of the facts, and with legitimate reasons (strategically and/or financially justified).

h) Verify their effective protection:

- Design and implement direct protection measures (physical, technical, operational);
- Identify their exposure to the risk of illegal capture by third parties;
- Design and implement behavioral protection measures (awareness-raising, training of personnel according to their mission or ability to detain sensitive information);

- ✓ Perform assessment of critical stakeholders' including suppliers' and clients' own performance in business secrecy policies (existence, robustness, history of failures, ...).

i) Specify duration of storage, then archive together with the corresponding supports.

Conclusion

The novelty in the approach proposed here is ***to use Law as an opportunity instead of as a constraint***. ***The protection of company's sensitive confidential information evolves then, from a risk management process to a quality management process,*** involving all company's departments and stakeholders in a transversal and intercultural approach, aiming at saving time and money. Mastering efficient methods and tools to manage business secrets adds to the efficiency of the data management program with a kind of quality management process, having a high potential for progress and upscaling, applicable in particular to innovation. The outcome of such a successful process may be the emergence of solid strategic advantages, way beyond the formal benefit of pure regulatory compliance. A specific attention must of course be paid to the evolution of debates, case law and creation of standards for the definition of "commercial value" and of "reasonable measures of protection". Any new legislation creates new challenges and operational constraints but conversely, these ones provide opportunities, which efficient secrecy governance may capture: a difficult challenge with interesting benefits to catch.

Dr. Pierre Ollivier, PhD
Managing Partner, Winnotek,
Managing Director, Kannon-MSD,
Paris, France,
E-mail : pierre.ollivier@winnotek.com

Dr. André Gorius, PhD
Partner, Winnotek,
Lyon, France,
E-mail : andre.gorius@winnotek.com

Philippe Simon, MBA
Partner, Winnotek,
Paris, France,
E-mail : philippe.simon@winnotek.com

Veronique Chapuis,
Legal BI Consultant,
Ceo LEX Colibri,
Manager of the Legal BI Executive Master Ecole de Guerre Economique,
Author (Master 2 of Law Paris I-King's College London)
Paris, France,
E-mail : veronique.chapuis@lexcolibri.com