COMMERCIAL SECRET MANAGEMENT IN TERMS OF SHADOW DIGITAL ECONOMY

Serghei Ohrimenco[1],
Dinara Orlova[2],
Valeriu Cernei[3]

Abstract: The article explores trade secret protection management in the context of the shadow digital economy (SDE). The study aims to identify threats to trade secrets associated with SDE and propose effective protection methods. It emphasizes that the economic value of trade secrets lies in their confidentiality, making them vulnerable to data leaks, cyberattacks, and other risks, particularly in the digital environment.

The authors examine the nature of trade secret in terms of SDE spread. The paper presents methods of trade secret protection, including documentary, economic-organizational, and information-analytical types. Special attention is paid to the combined use of patent protection and encryption techniques.

The study concludes with key findings, highlighting the need for enhanced cybersecurity, international cooperation to combat cyber espionage, and improved organizational measures. This work significantly contributes to the understanding of commercial secret management and offers valuable recommendations for businesses operating in the digital economy.

Keywords: shadow digital economy, entrepreneurial activity, commercial secret
JEL: L1, K0, C8, O17, M15.
DOI: https://doi.org/10.58861/tae.bm.2025.2.04

[1] Doctor of Economic Sciences, Professor, Laboratory of Information Security, Academy of Economic Studies of Moldova, Chisinau, Moldova, e-mail: osa@ase.md, ORCID: 0000-0002-6734-4321

[2] Doctor of Economic Sciences, Professor, Department of Economics, Financial University under the Government of the Russian Federation, Moscow, Russia, e-mail: drorlova@fa.ru, ORCID: 0000-0002-2901-070X

[3] PhD student, Laboratory of Information Security, Academy of Economic Studies of Moldova, Chisinau, Moldova, e-mail: valeriu.cernei@bsd.md, ORCID: 0000-0003-3300-334X

INTRODUCTION

Information is one of the most significant factors of production and management in modern economies. Modern entrepreneurship depends as much on the possession of information about potential customers, trade venues, and technical data as it does on personnel, machinery, and other capital goods. The reliance of industry on rapidly developing technologies amplifies the value of information. However, information is also different from other types of economic resources. It can be divided into an infinite amount of parts and, hence, is very complex. Importantly, it is often impossible to guarantee exclusive possession of this resource.

The importance of informational security for management is especially keen in today's world, where the information highway influences all aspects of social and economic life (Popova, P., Popov, V., Marinova, K., Petrova, M. and K. Shishmanov, 2024); (Petrova, M., Popova, P., Popov, V., Shishmanov, K. and K. Marinova, 2022); (Popova, P., Popov, V., Marinova, K. and M. Petrova, 2023). It becomes more and more important in terms of spreading the SDE. The EU Cybercrime Directive acknowledges the link between cyberattacks and the "loss or alteration of commercially significant confidential information". This means that protecting company data from leaks is a crucial aspect of cybersecurity (Porcedda, 2023). The efficiency of commercial production and other business activities increasingly depends on the ability of a business to use information correctly (Tairov & Petrova, 2022). However, information is only an asset that gives certain companies an edge over the competition if it is an excludable good that is not freely available to all. In an environment of escalating competition and in terms of SDE spread, business profits depend on the secrecy of information about entrepreneurial potential, special production technologies, and other data. For example, if a company's trade secrets were freely available, a competitor could develop a competing product using technological information or even market its own products to the company's clients using confidential client lists.

1. LITERATURE REVIEW

The critical literature review conducted by the authors allows the identification of several groups of important publications, which characterize the following directions:

1. One significant and highly important area of research is the analysis of the legislative framework regulating this field of knowledge. These include works such as (Lang, 2003; Mali, 2019; Maskus, 2012; Pasquale, 2011), and etc.

2. Publications that describe the trade secrets managing practices, its definition as an economic category, and the information constituting trade secrets. In particular (Margoni, 2025; Peskova et al., 2017; Png, 2012; Robertson, 2015; Schneider, 2017; West, 2015).

3. Sources analyzing the shadow digital economy (SDE) as a phenomenon in the development of the modern economy, its impact on actions related to categories such as cyber threats, information leaks (including trade secrets), and other activities constituting criminal activity. This group literature includes (Huateng, 2021; Ohrimenco et al., 2024; Ohrimenco et al., 2023).

2. RESEARCH METHODOLOGY

The methodology of this research is based on a systematic approach to investigate the management and protection of trade secrets in the context of the shadow digital economy (SDE). It includes the formation of a concept and statement of tasks, the collection of analytical information from available sources (scientific and monographic literature, reports of research companies specializing in the field of information security and its economic aspects), processing and analysis of the collected information. The research is structured around both qualitative and quantitative methodologies to explore the legal, organizational, and technological aspects of commercial secret protection in terms of SDE.

In legal and economic frameworks, different types of secrets serve to protect information that is crucial for national security, economic stability, and individual privacy. The most commonly recognized types of secrets include:

- State secrets – classified information related to national security, defense, foreign policy, and intelligence. Unauthorized disclosure may pose a threat to national sovereignty and public safety.
- Commercial (Trade) secrets – confidential business information that provides a company with a competitive advantage, such as production processes, client databases, and marketing strategies.

- Banking secrets – confidential information about a client's financial transactions, bank accounts, and credit history, protected by banking laws to ensure financial privacy.
- Medical secrets – Patient-related data, including diagnoses, treatments, and medical history, safeguarded to uphold doctor-patient confidentiality.
- Personal data protection (Privacy secrets) – information related to an individual's identity, including biometric data, personal correspondence, and communication records, protected under privacy laws.
- Judicial secrets – information related to ongoing investigations, court proceedings, and legal cases, ensuring fairness and integrity in the justice system.
- Professional secrets – confidential information held by professionals such as lawyers, journalists, and priests, ensuring trust and ethical responsibility in various fields.

Among these different types of secrets, commercial secrets hold a unique position due to their direct influence on economic competitiveness and innovation. Unlike state or judicial secrets, which are primarily associated with governance and legal order, or banking and medical secrets, which ensure personal confidentiality, trade secrets drive market success by protecting proprietary knowledge and business strategies. A very important issue relates to personal data protection, which is governed by the profound regulations established by EU legislation (Mali, 2019; Taal, 2021).

Trade secrets are critical for both large corporations and small businesses, as they help maintain market leadership, encourage research and development, and prevent unfair competition.

Given the rapid development of the digital economy (Ohrimenco et al., 2023; Ohrimenco et al., 2024) and increasing risks of industrial espionage and cyberattacks, the importance of commercial secrets continues to grow. Companies must implement comprehensive security measures, including legal safeguards, cybersecurity protocols and employee training, to ensure the confidentiality of their commercially valuable information.

The concept of a commercial (trade) secret was developed to limit access to commercially valuable information.

A "commercial secret" is a piece of confidentially kept information that gives an entrepreneur some economic advantage over competitors. This could range from information about specific production techniques or production formulas to marketing strategies or customer data. In (Lang, 2003), (Cottier, 2005; Robertson, 2015) explained the term as follows:

"Commercial (trade secret)" means information including but not limited to a formula, pattern, compilation, program, method, technique or process, or information contained or embodied in a product, device or mechanism which (1) is, or may be used in an entrepreneurship activity, (2) is not generally known in that trade or business, (3) has economic value from not being generally known and (4) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Trade secrets are an inherent component of a market economy. Allowing managers to protect their economic interests in valuable information facilitates the establishment of the economy model, which in turn stimulates innovative development and entrepreneurship (Sherwood, 2008). Regardless of the form of ownership, trade secrets help ensure the competitiveness of the entrepreneurs that possess them. This is particularly important in transitional economies, which are often dominated by small and medium enterprises that must protect their unique know-how in order to succeed in an open market (Värv et al., 2010).

Nonetheless, while protecting trade secrets can clearly advance a growing economy, doing so also creates a risk that certain shadow economic activities can be hidden under the umbrella of a trade secret. This is particularly the case in emerging economies where shadow economic activities have formed the backbone of the market for years. Un-entrenching these shadow activities even while creating safeguards for entrepreneurs is a daunting problem.

The term 'trade secrecy' points at two major characteristics of the phenomenon: secrecy and a connection with commercial activities (Pasquale, 2011). In other words, the commercial secret doctrine protects the owner's commercial interests by giving the owner the right to preserve the secret of commercially valuable information for unlimited time period. The term 'trade secret' itself has a slightly different meaning and impact based on the point of reference. From a scientific and practical point of view, a commercial secret could be either (i) *information* (i.e., knowledge or data) that is kept secret for commercial reasons or (ii) the concept of *the protection of* the secrecy of this information. From an economics perspective, a commercial secret is generally understood as 'a piece of confidentially kept information that gives an entrepreneur some economic advantage over competitors' (Peskova et al., 2017). In law, a 'trade secret' is a piece of information protected under the law because of measures that have been taken to protect it.

It is important to note that the authors encountered certain challenges in developing the methodology for the present study. First, the absence of official statistical data significantly complicated the information-gathering process. Second, data collection was carried out based on reports issued by leading specialized firms engaged in cybersecurity research. However, it should be emphasized that the statistical data presented were obtained through surveys and, therefore, do not fully capture the complexity of the phenomena under investigation. This represents yet another unresolved issue, which calls for the development of new methodological approaches and measurement techniques, as well as comprehensive sets of economic-mathematical models and advanced statistical data processing tools.

The methodological specificities of the subject area necessitated the construction of the following technological sequence of actions: identifying and verifying reliable information sources; analyzing and systematizing their content; selecting relevant data sets; and subsequently processing and analyzing the collected data.

3. DISCUSSION

It should be mentioned that the concept of commercial secret is more developed in law literature. For instance, the book “Trade Secrets: Law and Practice” by David Quinto and Stuart Singer (Quinto & Singer, 2009) serves as a practical guide to the protection of trade secrets, exploring their legal nature, methods of safeguarding, and strategic approaches in litigation. The authors provide a detailed analysis of what qualifies as a trade secret, examining key elements such as “independent economic value,” “not generally known to others,” and “reasonable efforts to maintain secrecy”.

The trade secrets are often understood in general as a part of intellectual property. In the book "Intellectual Property Culture: Strategies to Foster Successful Patent and Trade Secret Practices in Everyday Business" (Dobrusin & Krasnov, 2012), trade secrets are mentioned in the context of their role in corporate culture. Specifically, emphasis is placed on the importance of creating an intellectual property protection policy, which includes measures for safeguarding trade secrets, such as confidentiality agreements and restrictions on disclosing information. The protection of trade secrets is seen as a crucial element in maintaining competitive advantages, and the book highlights the need to incorporate this aspect into the daily operations of the organization. It also discusses the importance of developing

corporate strategies to protect these assets, training employees, and implementing systems that allow for effective information management. SDE escalates the risks of commercial secret loss tremendously.

3.1 Shadow digital economy as a damaging environment for the commercial secret

As noted in (Keshelava, 2017), the topic of the digital economy is highly expansive and has become increasingly popular in recent years. "The excitement surrounding this field, on the one hand, and the lack of a unified conceptual framework, on the other, have led to the emergence of a vast number of seemingly incompatible opinions and, consequently, to the impossibility of a coherent dialogue."

Chinese expert Ma Huateng (Huateng, 2021) presents an important and valid argument that the digital economy represents a new stage of economic and social development following the agrarian and industrial economies. Public understanding of the fundamental principles of the digital economy has evolved gradually. Among the many definitions of the digital economy, one of the most representative is the one proposed within the framework of the *Development and Cooperation of the Digital Economy* project of the G20 and presented at the G20 Summit in Guangzhou in 2016. This initiative defines the digital economy as encompassing a range of economic activities in which digitized knowledge and information serve as key production factors, with modern information networks acting as their primary carrier, and the effective use of information and communication technologies (ICT) as the main driving force for increasing efficiency and optimizing economic structures.

The *shadow economy* refers to the informal sector of a national economy that is not accounted for in official statistics. It encompasses all forms of unregistered and unrecorded economic activities, including the following (Schneider, 2017):

- Transactions that are not prohibited by law (the so-called "gray market");
- Criminal activities explicitly outlawed by legislation (the "black market");
- Non-market activities, where goods and services are produced and consumed within households;
- Barter transactions involving goods and services that do not enter formal market exchanges.

Unlike the *classical* shadow economy, the SDE differs in its composition and structure, which will be briefly outlined below.

The *shadow digital economy* refers to a sector of economic relations encompassing all forms of production and business activities that, by their nature, content, characteristics and structure, contradict legal requirements and are conducted in defiance of state economic regulation and oversight.

At its core, the SDE consists of shadow entrepreneurial activities, which are characterized by:

- A hidden, latent (covert) nature, meaning that these activities are not registered with government authorities and are not reflected in official reports;
- Coverage of all phases of the economic reproduction process (production, distribution, exchange, and consumption);
- A parasitic nature of operations at all levels.

Three economic justifications have traditionally been advanced to support the protection of trade secrets.

First, the protection of trade secrets creates incentives to engage in the creative, inventive process and then to invest in the development of such innovations (West, 2015; Risch, 2011). For example, one study (Png, 2012) finds that technology and manufacturing firms in US states that have passed laws protecting trade secrets tend to spend more on research and development than firms in states without such protections. This is an important justification for protecting trade secrets in developing and transitional countries, where innovation is a key component of economic growth (Maskus, 2012).

Second, when the government or legal process provides protection of such confidential information, businesses themselves do not need to invest in ‘costly measures to prevent breach of security’ (Margoni, 2025). This allows the wealth of innovation to be spread more easily; for example, a firm will not be as likely to feel a need to hire only family members or to pay ridiculously high salaries to prevent employee movement (see (Risch, 2011)). Third, and somewhat contrary to what one might think, protecting trade secrets allows for their dissemination to more people—resulting in consequent learning and spillovers (Margoni, 2025). For example, if a firm knows that it can bring a lawsuit against former employees who divulge a trade secret, the firm might be more willing to share the secret with the employees. Even if the employees never share the specific information they have learned with others, the employees ‘may benefit from their enhanced

stock of knowledge' and this more general learning may be passed on to future employers or business associates.

These merits have come under criticism, however. Importantly, trade secrecy laws are meant to protect information that the owner *is already taking steps to protect*; that is, the information is not already in the public domain. This is quite a different type of protection from that offered under patent or trademark laws. Those laws protect information or technology that is already public from being copied by others, and then only for a certain period of time. Upon expiration of the period, the patent or trademark must either be renewed, or the intellectual property becomes a public good (Risch, 2011). The real power of trade secrecy laws does not come from any power of the law itself to prevent disclosure; the owner of the commercial secret is responsible for taking steps to do this. The power of trade secrecy laws is creating an incentive for owners of trade secrets to undertake efforts to protect their own property by (i) not publicly disclosing the confidential data and (ii) alerting employees or business partners who have access to the confidential data of the possibility of becoming subject to legal damages if they misappropriate the information. In short, at most, trade secrecy merely allows firms to obtain damages when a secret is misappropriated and then used to the firm's detriment.

Furthermore, trade secrecy protection continues indefinitely; disclosure is *never* allowed. In fact, a court might only access a commercial secret once the secret has been divulged. In the usual course of business, trade secrets remain part of a business's proprietary information. This means that if a firm were so inclined, it might have an incentive to use the veil of trade secrecy as an excuse to hide all sorts of 'secret information' from the public domain. This is a special area of concern in countries such as Russia, where private firms engage in a wide range of 'quasi-public' activities - from constructing and operating telecommunications to overseeing electronic voting. Often, these operations require advanced technologies that would normally be subject to commercial secret protection. However, when public or at least quasi-public activities are involved, hiding information about these technologies from public scrutiny could create ethical risks.

These industries, such as those in the financial and energy world, are using commercial secret exemptions in open government laws to prevent the public from accessing basic information about the use of taxpayers' money. Governments are funding private-sector research, or even providing the facilities in which the research is conducted, and yet the public is denied access to the results of that research because of trade secrecy doctrine.

3.2 Methods of commercial secret protection

The management of corporate commercial secrets should include their protection from threats such as leaks and loss. One of the key vulnerabilities of commercial secrets is their low resistance to disclosure in the SDE. They can be subject to simple analysis, expert "data pumps," accidental leaks, hacker attacks, and more.

Provisionally, the process of commoditization divides information kept as a commercial secret into two types:

- Inalienable commercial secrets, which ensure the safety and competitive integrity of a company's internal activities.
- Seizable commercial secrets, which gain the status of a commodity.

In practice, inalienable commercial secrets are more widespread, while seizable commercial secrets are better protected by patents to facilitate commercialization.

A comprehensive threat assessment should precede the implementation of a data protection system. The sequence of actions includes: identifying threats (evaluating probability levels, systematization), estimating potential losses, selecting appropriate commercial secret protection methods, and assessing economic efficiency and associated costs. The following classification of threats to commercial secrets can be suggested (Table 1):

Table 1.
Classification of commercial secret threats in SDE

Criteria	Types
Threat Source	External (business espionage, competitors' illegal activities, theft of tangible and intangible assets); Internal (employee disclosures, low motivation, ineffective security services)
Severity of Consequences	High (business shutdown, severe financial losses); Medium (high recovery costs, moderate downtime); Low (potentially disruptive impact)
Probability of Occurrence	Unlikely; Real risk
Business Stage Affected	Initialization phase (most critical); Ongoing operations phase
Object of Infringement	Information, finances, tangible assets, goodwill, etc.
Infringement Subjects	Organized crime, unscrupulous competitors, employees, state authorities
Type of Damage	Direct financial loss, lost profit

Elaborated by authors using (Peskova et al., 2017)

As shown in Table 1, threats to commercial secrets are classified by their source (external and internal), severity of consequences, and likelihood of occurrence. These threats range from disruptive to business-critical, with even unlikely risks requiring attention. Enterprises are especially vulnerable during the initialization phase, and targets often include information, finances and goodwill. Offenders may range from criminal organizations to state authorities, leading to direct financial losses and reduced profits. This highlights the need for a comprehensive and proactive security strategy across all stages of business development.

4. RESULTS

Existing methods for protecting commercial secrets can be grouped based on functional criteria (Figure 1) (Peskova, 2017):

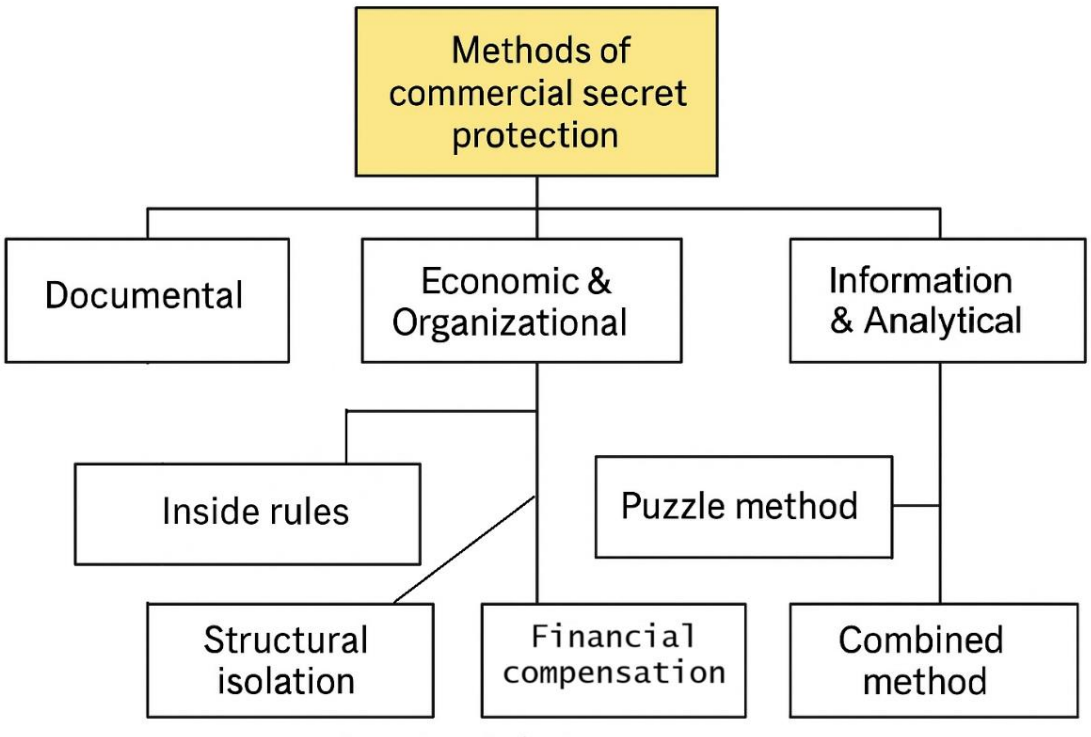


Figure 1. Methods of Commercial Secret Protection
Elaborated by authors using (Peskova, 2017)

4.1 Documental methods

These include regulations governing the circulation of internal documents containing confidential information. A "commercial secret" status is considered established once confidentiality measures are implemented:

- Creating a list of confidential information subject to protection.
- Regulating internal relations concerning the handling of commercial secrets via labour contracts and civil law agreements with business partners.
- Labeling physical media containing confidential data with a "Commercial Secret" designation, specifying the information owner.
- Utilizing technical measures for information protection.

While these methods provide clarity and enforceability, they mainly protect against unintentional leaks. However, judicial measures for enforcing confidentiality often indicate an irreversible loss of secret information.

4.2 Economic and organizational methods

Within the institutional economic framework, an employer can adopt three primary approaches to protect commercial secrets:

1. Establishing corporate policies for handling confidential information.
2. Implementing compensation schemes for employees involved in creating and maintaining commercial secrets.
3. Structuring internal operations to ensure departmental isolation.

a) Inside rules

Companies can enforce strict internal regulations requiring employees to adhere to confidentiality protocols. However, weak enforcement measures may render these rules ineffective. Examples include restricting inter-company communication with competitors and regulating access to sensitive documentation through password systems and physical security.

b) Financial compensation

Providing financial incentives for employees to maintain secrecy can be an effective strategy. This compensation should be proportionate to the potential losses incurred from information leaks. Moral incentives, such as team-building and corporate loyalty programs, can also strengthen adherence to confidentiality requirements.

c) Structural isolation

Restricting access to sensitive areas and information to only authorized personnel minimizes the risk of leaks. This approach enhances protection by narrowing the scope of vulnerability.

4.3 Information and analytical methods

a) Puzzle method

This method involves segmenting commercial secrets into discrete components, with different access conditions for each. Only key personnel have a complete understanding of the full picture, making unauthorized comprehension of the data challenging. However, improper implementation may lead to unintentional information disclosure.

b) Combining patents and Trade secrets

Patent protection can complement trade secret safeguards. Patents offer legal recognition, commercialization opportunities and legitimacy, while trade secrets protect non-patentable but commercially valuable information. The primary disadvantages of patents include limited duration, high costs, and potential exposure of technological innovations to competitors.

Porcedda (Porcedda, 2023) provides the following recommendations for strengthening protection of the commercial secret:

- Enhancing encryption mechanisms and access controls.
- Developing international cooperation in combating cyber espionage.
- Integrating law enforcement approaches to cybercrime and data protection.

Thus, cybersecurity plays a key role in protecting trade secrets.

None of the methods discussed above can provide absolute protection for a company's trade secrets, especially in the face of an evolving shadow digital economy that continuously adapts to new technological advancements. However, recognizing these challenges opens avenues for further research into more sophisticated commercial secret management strategies, integrating emerging cybersecurity solutions, regulatory frameworks, and corporate governance practices. Future studies could explore the role of artificial intelligence in commercial secret protection, the impact of cross-border legal harmonization, and the ethical implications of balancing transparency with corporate confidentiality. We invite scholars, policymakers, and practitioners to contribute to this critical discourse, fostering a more resilient and adaptive approach to commercial secret security in an increasingly complex digital landscape.

5. EMPIRICAL DATA STUDY

The object of the study will be two sets of data: statistics on data leaks and expert assessments of damage costs. The data used in the study are based on empirical evidence and reflect real-world practical situations.

One of the most serious global issues in the field of IT is information leakage. We will analyze the available empirical data, which primarily characterize data leakage. Information leakage refers to the intentional or accidental disclosure of sensitive, confidential, or personal information (such as identification data, credit card details, usernames, passwords, etc.) and its exposure to third parties, which can have serious consequences for the affected organizations and individuals. Unauthorized transmission of information occurs via web channels, through programs and applications, and on physical media (storage devices, printer outputs, etc.).

The general picture of information leaks in the world from 2013 to 2024 is shown in the following figure (Infowatch, 2025).

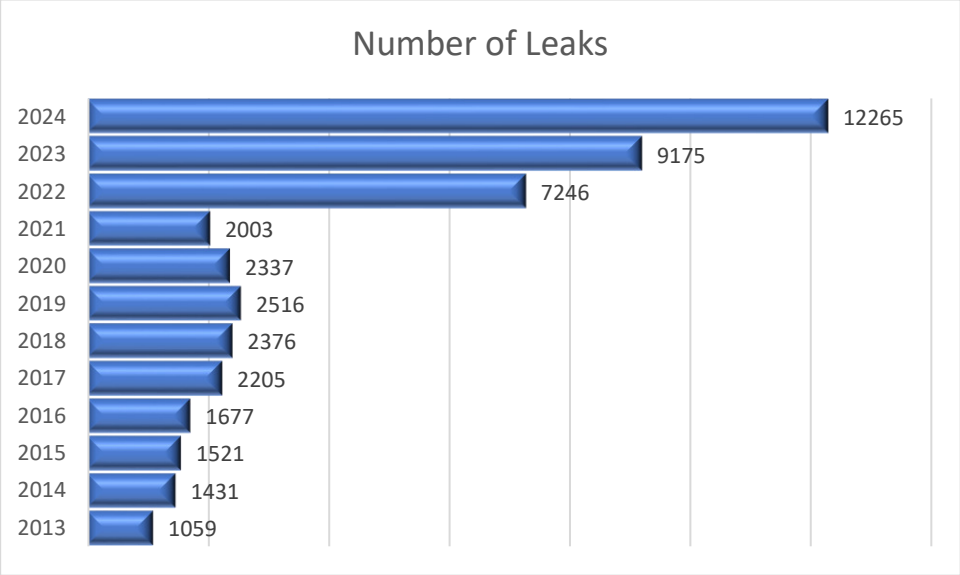


Figure 2. Number of information leaks in the world in 2013-2024
Source: (Infowatch, 2025)

An analysis of the table data leads to the principal conclusion that there has been a quantitative increase in data breaches worldwide over the observed period, with consistently high growth rates. Specifically, the number of breaches recorded in 2024 was 8.6 times higher than in 2013. The peak in the number of breaches occurred in 2023, amounting to 12,265 incidents.

It is important to note that the table reflects quantitative metrics only, encompassing breaches involving personal data records, trade secrets, and other sensitive information.

The primary channel of information leakage remains information and communication technologies, with internet-related breaches accounting for approximately 69% of all incidents. Paper-based document leaks constitute slightly more than 10%. Other significant channels include theft of removable media, loss or theft of equipment, and unauthorized manipulation of email systems.

The following table presents data on the dynamics of information breaches and the number of leaked personal data records in selected countries for the period 2023–2024.

Table 2.
Dynamics of information leaks and number of leaked personal data records

	Data Breaches			Leaked Data Records (bln)		
Country	2023	2024	Change (%)	2023	2024	Change (%)
USA	4823	3310	-31.37	8.18	553	-32.40
Russia	786	778	-1.02	1.2	1.58	31.67
India	542	498	-8.12	4.44	2.34	-47.30
United Kingdom	384	352	-8.33	3.12	0.18	-94.23
Canada	280	266	-5.00	0.2	0.35	75.00
France	313	232	-25.88	0.24	0.45	87.50
Indonesia	245	217	-11.43	4.99	1.29	-74.15
Germany	251	207	-17.53	0.08	0.09	12.50
Italy	220	177	-19.55	0.13	0.22	69.23
Brazil	258	176	-31.78	1.58	0.77	-51.27
Spain	223	166	-25.56	0.05	2.08	4060.00
Australia	204	159	-22.06	0.11	0.15	36.36
China	272	144	-47.06	12.75	3.93	-69.18
Thailand	112	105	-6.25	0.3	0.17	-43.33
Israel	142	95	-33.10	0.09	0.05	-44.44

Source: (Infowatch, 2025)

An analysis of the table's content indicates a decrease in the number of data breaches across all countries without exception. However, the same cannot be said for the number of leaked personal data records, which shows both increases and decreases. For example, Russia experienced a rise of +31.7%, Canada +75%, France +87.5%, Germany +12.5%, Italy +69.22%,

Australia +36.4%, and the most significant increase was recorded in Spain, reaching +4060%.

We will expand the analysis of the data presented in the previous table by incorporating information on the compliance with the key provisions of the GDPR. Specifically, we will analyze the overall number of personal data breaches across European countries, drawing on an analytical report (Dlapiper, 2025).

Our focus will be on the data regarding the total number of personal data breaches (both registered and reported), as well as the overall amount of imposed fines.

Table 3.

Total number of violations GDPR (2018-2020)

	Country	Total number of data breaches from May 25, 2018, to January 1, 2020	Total number of data breaches from May 25, 2018, to December 31, 2019	Total number of data breaches from May 25, 2018, to December 31, 2019	Cost of data breaches in 2019 (million EUR)
1	Netherlands	40647	25247	15400	147.2
2	Germany	37636	25036	12600	31.12
3	United Kingdom	22181	11581	10600	17.79
4	Ireland	10516	6716	3800	132.52
5	Denmark	9806	6700	3100	115.43
6	Poland	7478	5278	2200	13.74
7	Sweden	7333	4383	2500	48.14
8	Finland	6535	3983	2500	71.11
9	France	3459	2153	1306	3.2
10	Norway	2844	2004	820	37.31
11	Italy	1886	1276	610	2.05
12	Slovenia	1845	1105	740	5.25
13	Spain	1698	1028	670	2.08
14	Austria	1644	1164	580	12.1
15	Belgium	1332	912	420	7.88
16	Hungary	749	479	270	4.87
17	Czech Republic	720	430	290	4.03
18	Romania	668	408	260	1.9
19	Luxembourg	545	345	200	56.97
20	Iceland	338	313	25	91.15
21	Malta	239	139	100	31
22	Greece	232	162	70	1.5
23	Lithuania	222	118	105	4.18
24	Estonia	132	82	121	9.74
25	Latvia	127	117	57	6.13
26	Cyprus	94	59	35	4.8
27	Liechtenstein	30	15	15	39.18
28	Bulgaria	-	-	-	-
29	Portugal	-	-	-	-
30	Slovakia	-	-	-	132.60

Source: Calculated from DLA Paper GDPR Data breach survey (DLA, 2025)

European countries are ranked in descending order based on the total number of personal data breaches. The Netherlands tops the list with a total of 40647 breaches while Liechtenstein ranks last with 30. A markedly different pattern emerges when considering fines: Germany leads with €54,574,525 followed by Finland (€51,100,000) Austria (€18,107,700) and Italy (€11,500,000). These data highlight the complexity of implementing the General Data Protection Regulation (GDPR).

In addition to the number of data leaks we can include information about the general GDPR fines as of January 2022: Luxembourg €746,299,400; Ireland €226,046,500; Italy €79,144,728; Germany €69,329,916; France €58,580,300; UK €45,350,000; Spain €29,003,000; Austria €24,853,650; Sweden €18,000,000; Netherlands €10,073,000 (Infowatch, 2025). The provided data indicates high amounts and significant fines.

Another important indicator is the channels through which information leakage occurs. Among them, the following should be highlighted: computer networks, removable storage devices, mobile devices, paper documents, email, as well as theft and loss of equipment. These channels are responsible for the leakage of personal data, payment information, trade secrets, and state secrets.

The very notable recent examples of valuable information leakage include two cases:

- Bleeping Computer: The largest data breach in the history of healthcare occurred in the spring of 2024 in the United States. Data on 190 million American patients was stolen as a result of a hack targeting a subsidiary of the insurance company UnitedHealth. The attack was carried out by hackers from the AlphV (BlackCat) group. The company paid $22 million in ransom in hopes of retrieving the data and preventing its dissemination. However, the attackers, having received the money, did not keep their promise. As of 9 months after the incident, in 2024, UnitedHealth estimated the damage at $2.45 billion.

- The Cyber Express: A data leak involving the Italian government leadership and other prominent individuals occurred in Italy in the same 2024 year. It resulted from a conspiracy between hackers and police officers. The accused gained access to confidential information by bribing law enforcement personnel and installing spyware. The obtained data was used for blackmail, allowing the perpetrators to extort over €3 million in total.

The second group of empirical data represents the information of individual experts regarding losses from a wide range of cyber threats,

accumulated both by independent researchers and leading computer companies (Vergara & Cakir, 2025), (Miranda et al., 2024), (Correia, 2022).

For example, Steve Morgan, the editor-in-chief of Cybercrime Magazine (Morgan, 2024), presented to experts a material describing the top five most significant facts about cybersecurity:

1. According to forecasts, by 2025, the global damage from cybercrime will amount to $105 trillion per year. If this damage were evaluated as a country, cybercrime, which is predicted to cause damage totaling $6 trillion worldwide in 2021, would be the third-largest economy in the world after the USA and China. Global costs of cybercrime are expected to grow by 15 percent annually over the next five years, reaching $105 trillion per year by 2025, compared to $3 trillion in 2015. Innovations and investments in cybercrime significantly outweigh the damage caused by natural disasters and will be more profitable than global trade in all major illegal products combined (including drugs, pornography, arms trafficking, etc.).

2. Global spending on cybersecurity from 2021 to 2025 will exceed $175 trillion. In comparison, the global cybersecurity market was valued at only $35 billion in 2004, and now it is one of the largest and fastest-growing sectors of the information economy. It is expected that the cybersecurity market will grow by 15 percent annually from 2021 to 2025.

3. According to forecasts, by 2031, the global damage from ransomware will exceed $265 billion. Global losses from ransomware damage are expected to reach $20 billion per year in 2021, compared to $325 million in 2015, which is 57 times higher. In ten years, the costs will exceed $265 billion. The average ransom amount, according to estimates [56], is a significant sum — $220,298 ($220,298 compared to $154,108, which is 43% higher than in Q4 2020). The median ransom amount is $78,398 ($78,398 compared to $49,450, or 59% more than in Q4 2020), which signals a quantitative and qualitative increase in new attacks.

4. By 2025, the total volume of global data storage is expected to exceed 200 zettabytes. This includes data stored in private and public IT infrastructures, private and public cloud data centers, and personal computing devices.

CONCLUSION

This article explores the key aspects of trade secret protection in the context of the SDE. The economic value of trade secrets lies in their

confidentiality, making them vulnerable to data leaks, cyberattacks and other risks, especially in the digital environment. In the context of SDE, the risks of leakage become particularly relevant, as many business processes are shifting to informal, state-unregulated sectors, making control and protection more challenging.

The shadow digital economy is characterized by its covert nature and violation of legal frameworks, which increases risks for the security of trade secrets. Modern protection methods - ranging from documentary to information-analytical approaches, including patenting and encryption - offer effective tools for minimizing these threats. However, no method can guarantee absolute protection, especially given the continuous evolution of technologies and methods of cyber espionage.

The conducted study has made it possible to identify a number of significant aspects characterizing the current state of the institution of trade secrecy in the context of the digital shadow economy. However, the presented material does not claim to provide an exhaustive account of all the issues and challenges in this area. On the contrary, the results of the analysis highlight the complexity and multifaceted nature of the phenomenon under consideration. In this regard, the development of a new research methodology, as well as the improvement of approaches to the collection, systematization and analytical processing of relevant empirical data, appears to be necessary.

We consider it necessary to highlight another issue that remains unresolved to this day. Specifically, this concerns the development and implementation of ethical practices in the field of modern cybersecurity. In certain disciplines - such as medicine, engineering, and law - comprehensive codes of ethics and conduct have been established and are widely observed. Unfortunately, a comparable ethical framework is lacking in the cybersecurity domain. This absence should be viewed as a potential threat to individual, societal and state security, as well as a significant factor hindering trade and constraining investment. Addressing this issue remains an urgent and unmet imperative.

Thus, protecting trade secrets in the SDE requires a comprehensive approach that includes not only technical security measures but also legislative initiatives and international cooperation to combat cyber espionage. A key challenge for the future is the development of more advanced trade secret management strategies that integrate new solutions in cybersecurity and regulatory frameworks. Further research into the role of artificial intelligence and the harmonization of international legal norms in the context of trade secret protection will open new opportunities for enhancing business resilience in the digital age.

References

Correia, G. (2022, July 1). Making the most of cybercrime and fraud crime report data: A case study of UK Action Fraud. *International Journal of Population Data Science*. DOI:10.23889/ijpds.v7i1.1721

Cottier, T. (2005). The agreement on trade-related aspects of intellectual property rights. In T. Cottier, P. Delimatsis, & N. Diebold (Eds.), *The World Trade Organization: Legal, economic and political analysis,* pp. 1041–1120\. Springer US.

DLA Piper. (2025, May 7). DLA *Piper GDPR Data Breach Survey 2020.* Retrieved 03 2025. Available online:https://www.dlapiper.com/en/insights/publications/2020/01/gdpr-data-breach-survey-2020

Dobrusin, E. M., & Krasnow, R. A. (2012). *Intellectual property culture: Strategies to foster successful patent and trade secret practices in everyday business*. Oxford University Press

Huateng, M. Z. (2021). *The Chinese digital economy*. Palgrave Macmillan.

Infowatch. (2025, May 7). *AI-based Data Loss Prevention System*. Retrieved 03 2023. Available online: https://infowatch.com/products/data-loss-prevention-traffic-monitor

Keshelava, A. V., Budanov V. G., Dmitrov, I. D., Keshelava, V. B., Rumyantsev, V.Yu., Sorokin, K. S., Khaet, I. L., & Shcherbakov, A. V. (2017). Introduction to the digital economy. VNIIGeosistem Publ. Retrieved 04 2025 Available online: https://spkurdyumov.ru/uploads/2017/07/vvedenie-v-cifrovuyu-ekonomiku-na-poroge-cifrovogo-budushhego.pdf

Lang, J. (2003). The protection of commercial trade secrets. *European Intellectual Property Review*, 25(9), pp.462–471.

Lemley, M. A. (2011). The surprising virtues of treating trade secrets as IP rights. In R. Dreyfuss & K. Strandburg (Eds.), *The law and theory of trade secrecy* (pp. 311–353). Edward Elgar Publishing.

Mali, P. (2019). *GDPR articles with commentary & EU case laws*. Cyber Infomedia.

Margoni, L. G. (2025, April 8). *Enquiries into intellectual property's economic impact*. Institute for Information Law. Retrieved 02 2025. Available online: https://www.ivir.nl/publicaties/download/1625.pdf

Maskus, K. E. (2012). *Private rights and public problems: The global economics of intellectual property in the 21st century*. Peterson Institute.

Miranda, B., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024, April 10). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE, 19*(4). DOI: 10.1371/journal.pone.0297312

Morgan, S. (2024, February 5). Top 10 cybersecurity predictions and statistics for 2024. *Cybercrime Magazine*. Retrieved 04 2025 Available online: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

Ohrimenco, S., Bortă, G., & Cernei, V. (2024). The digital world has a long shadow. In Daphne R. Raban & Julia Wlodarczyk (ed.). *The Elgar companion to information economics* pp. 481–504. Edward Elgar Publishing.

Ohrimenco, S., Orlova, D., & Cernei, V. (2023). Cyber threats modeling: An empirical study. *Business Management*, *3*, pp.90–106. DOI: 10.58861/tae.bm.2023.3.06

Pasquale, F. (2011). The troubling consequences of trade secret protection of search engine rankings. In R. Dreyfuss & K. Strandburg (Eds.), *The law and theory of trade secrecy*. pp. 427–445. Edward Elgar Publishing.

Peskova, D., Vasileva, Y., & Nazarov, M. (2017). Commercial secret as an instrument of company competitive strategy effectiveness increase. In *SHS Web of Conferences*, vol.35, p. 01060. EDP Sciences. DOI: 10.1051/shsconf/20173501060

Petrova, M., Popova, P., Popov, V., Shishmanov, K. and K. Marinova. (2022). Potential of Big Data Analytics for Managing Value Creation. International Conference on Communications, Information, Electronic and Energy Systems (CIEES), pp. 1-6, DOI: 10.1109/CIEES55704.2022.9990882

Png, I. (2012). Trade secrets, non-competes, and mobility of engineers and scientists: Empirical evidence. *SSRN Electronic Journal*. DOI:10.2139/ssrn.1986775

Popova, P., Popov, V., Marinova, K., Petrova, M. and K. Shishmanov. (2024). The Digital Platform — new opportunities and implementation strategy. 1*6th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Iasi, Romania, 2024, pp. 1-9, doi: 10.1109/ECAI61503.2024.10607401

Popova, P., Popov, V., Marinova, K. and M. Petrova. (2023). The Role of Digital Platforms and Big Data Analytics as a Base for Digital Service Innovation. *2023 4th International Conference on Communications,*

Information, Electronic and Energy Systems (CIEES), Plovdiv, Bulgaria, 2023, pp. 1-8, doi: 10.1109/CIEES58940.2023.10378780

Porcedda, M. G. (2023). *Cybersecurity, privacy and data protection in EU law*. Bloomsbury Publishing.

Quinto, D. W., & Singer, S. H. (2009). *Trade secrets: Law & practice*. Oxford University Press.

Risch, M. (2011). Trade secret law and information development incentives. The law and theory of trade secrecy: a handbook of contemporary research, Rochelle C. Dreyfuss, Katherine J. Strandburg, eds., Edward Elgar Publishing, 2010, DOI:10.4337/9780857933072.00014

Robertson, K. M. (2015). The secret to protecting trade secrets: How to create positive secrecy climates in organizations. *Business Horizons*, *58*(6), pp.669–677. DOI:10.1016/j.bushor.2015.07.004

Schneider, I. (2017). Can we trust measures of political trust? Assessing measurement equivalence in diverse regime types. *Social Indicators Research, 134*(3), pp.963–984. DOI:10.1007/s11205-016-1400-8

Sherwood, R. M. (2008). Trade secret protection: Help for a treacherous journey. *Washburn Law Journal, 48 (3)*, pp.67–86.

Taal, A. (2021). *The GDPR challenge*. CRC Press.

Tairov, I. & Petrova, M. (2022). Challenges and opportunities in electronic business during the Covid 19 pandemic. IEEE International Conference "Problems of Infocommunications. Science and Technology" (PIC S&T'2022). 10.1109/PICST57299.2022.10238561

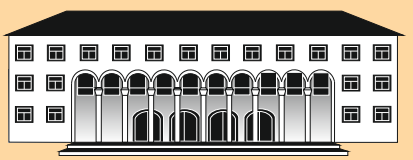
Varv, A., Pisuke, H., Mets, T., Vasamae, E., & Kelli, A. (2010). Trade Secrets in the Intellectual Property Strategies of Entrepreneurs: The Estonian Experience. Review of Central and East European Law, 35(4), pp.315-339. DOI:10.1163/157303510X12650378240476

Vergara, E., & Cakir, S. (2025, May 7). *A review of the economic costs of cyber incidents*. World Bank. Retrieved 05. 2025. Available online https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf

West, J. K. (2015). Synthesis of 'Enquiries into Intellectual Property's Economic Impact' chapter of a larger OECD report entitled 'Enquiries into Intellectual Property's Economic Impact' 2015. (pp. 7–27). OECD Publishing .Retrieved 04 2025. Available online SSRN: https://ssrn.com/abstract=2652044.

ISSN 0861 - 6604
ISSN 2534 - 8396

BUSINESS management



PUBLISHED BY
D. A. TSENOV ACADEMY
OF ECONOMICS - SVISHTOV

2/2025

BUSINESS management 2/2025

The printing of the issue 2-2025 is funded with a grand from the Scientific Research Fund, Contract KP-06-NP6/29/04.12.2024 by the competition "Bulgarian Scientific Periodicals - 2025".

Submitted for publishinq on 27.06.2025, published on 30.06.2025,
format 70x100/16, total print 80

BUSINESS management

D. A. Tsenov Academy of Economics, Svishtov

Year XXXV * Book 2, 2025

CONTENTS