Economic Alternatives, 2018, Issue 3, pp. 311-324

Identifying and Managing Protected Information Types in Information Society

Nikolay Krushkov*

Summary

With the cosmic development of information technology and global information connectivity, there was a new transformation at the turn of the 21st century when the transition of "industrial society" into an "information society" has begun. A new characteristic feature of knowledge-driven labor in the information society was the application of new knowledge to existing knowledge as the main source of productivity. Information management requires proper identification of the type of information its provision and protection, both at state and corporate level. On the one hand, it is of crucial importance to obtain information on prices, quantity and quality of goods and services (at corporate level) or on the development of state-relevant internal and external processes and threats (at state level). On the other hand, it is equally important that the provision of information from individuals, enterprises and the state is realized with the guarantees of preserving the personal rights of individuals, the competitive advantages of business entities and national interests. The efficiency of the management requires a flawless recognition of the types of information: state and official secrets; industrial and commercial secrets; intellectual property; know-how; general (day-to-day) business information; other protected personal information.

* Assistant Profesor,. PhD at Creative Industries and Intellectual Property Department at the University of National and World Economy.

Key words: information, intellectual, property, secret, management

JEL: A20, C8, D23, D83, F52, L51, L86, M14

Introduction

"Of course there is no need to tell academics that information is a valuable resource: knowledge is power. And yet this occupies a slum dwelling in the town of economics. Mostly it is ignored" (Friedman M., 2014). This observation of one of the greatest economists of the 20th century, George Stigler[1], is also largely applicable to reality in the 21st century. In the same time information is ignored as classification, meaning, and protection at both national and corporate level. This reality is particularly incomprehensible in the context of the common understanding that we all live in an information society.

If society in the 19th century was in the so-called agricultural age when natural exchange was at its peak and the basic formula in the economy was commodity-money-commodity, then in the next 20th century "the agricultural society" was clearly transformed into "industrial society". In the middle of the 20th century, villages were rapidly and systematically depopulated to develop the class of urban workers. Above all, due to the clearly expressed necessity for technically qualified workers for the needs of the increased role of industry under the money-commodity-money formula.

[1] US economist (1911 –1991) who won the Nobel Memorial Prize in Economic Sciences in 1982, a key leader of the Chicago School of Economics, along with his close friend Milton Friedman

With the cosmic development of information technology and global information connectivity, there was a new transformation at the beginning of the new 21st century when the transition of "industrial society" into an "information society" has begun. A characteristic feature of the new, knowledge-driven labor in the information society was the application of new knowledge to existing knowledge as the main source of productivity. In the period of transformation from industrial to information society, the borderline between the industrial sector and the service sector started blurring. "Dominant position was taken by the new knowledge-dependent production increase - in agriculture, industry and services, which broke the boundary between "goods" and "services" (Collection, edited by Boryana Gagova, 2009).

Different scientists focus their research on specific national security issues as follows: ethnic minorities and national security (Hristo Tutunarov); risk management in the field of security (Yuliy Georgiev); information security (Tsvetan Semerdjiev, Todor Tagarev, Georgi Pavlov, Yuliya Karakaneva); economic security (Nikolay Tsonkov); strategic analisys for the needs of security (Dimitar Yonchev, Yuriy Tarkalanov, Valeri Lazarov, Rumen Gyurov); economy of defance (Tilcho Ivanov, Dimitar Dimitrov), sociocultural security (Evgeni Sachev); counterterrorism (Ivan Stanchev, Aleksey Petrov); phylosphy of security (Stefan Michev, Nikolay Slatinsky); national security protection (Dimitar Ivanov, Todor Todorov); international security (Plamen Pantev, Velizar Shalamanov); intelligence (Yordan Nachev, Todor Boyadjiev); corporate security (Emil Vasilev).

Severe gap of academic interest is currently seen in the field of corporate security and especially in the field of corporate security management as well as in the field of interaction between national security and corporate security management and expertise.

Another academic liability is represented with the fact that most of the scientists interpret the dynamics of the new (information) economy on the basis of categories of already outdated labor paradigm and thus underestimate the revolutionary potential of the new e-reality. Potential which "is created by the possibility of direct on-line communication between different types of activities - development, production, management, application and distribution, in the conditions of collapsing territorialized industrialization. Conversely, the new virtual space places completely new dimensions that lack boundaries and many restrictions" (Collection, edited by Boryana Gagova, 2009)

The thesis of current survey may be described with the assumption that modern information society (and the new ecomomy) requires strict distinction and identification of the types of information searched, acquired, stored, protected and used in modern business activity and together with this strong need for implementation of an integrated system of information security for every government, business entity, manager or any living person on the bases of which all competitive caracteristics are protected.

Effective information management requires a flawless recognition of the types of information, knowledge of the legally guaranteed protection, experience in the implementation of the "necessary measures" for information protection and, together with this, proper accessibility and high speed in the use of the information.

This article's scientific contribution is in the field of the classification of the types of information and in the management of information as an integrated system assuring protection of competitiveness and critical advantages of any activity.

I. General classification of types of protected information according to its main purposes

For the purpose of effective management in a state and corporate context, *classification*

of types of information according to the main purposes of use is mandatory. The classificaion of information according to its main purposes may take the following distinction:

1. *State and official secrets* **which can not be subject to sharing, provision or use outside the circle of a certain number of employees**, who have gained access to it after they have been checked for reliability under a complex legally regulated procedure.

2. *Industrial and commercial secrets* **include any information that is defined as such by its holder according to specific internal regulations, specific measures have been taken to protect it and prevent its dissemination outside the circle of people working with it, which would lead to a loss of competitiveness**. It is an object of the strictest protection because it is not intended for "sale" or licensing under any circumstances.

3. *Intellectual property* **which is protected by law and is an exclusive property of its owners, but is intended to be licensed by the rights holders**. The protection is fixed-term. Resources are invested in reaching the creative outcome. The investments made should be returned within the term of protection and a profit should be realized. It should be advertised and marketed.

4. *Know-how* is **information accumulated on the basis of knowledge, skills and experience that is practicable in manufacturing or professional practice and which is protected by the fact that it has not been given publicity but is kept secret by its holder**. At his own personal responsibility because there are no regulatory acts or internal rules to protect it. It is usually intended for "sale" or licensing but does not benefit from legal protection. It is intended for licensing because its provision should not infringe the holder's degree of competitiveness but rather restore the investments made. "Whole industries have been generated on the basis of know-how, as well as chains of hotels, restaurants and service companies with world-famous names" (Borisov, B., Borisova, Vl., 2015).

5. *General (day-to-day) business information, including IT connectivity, networks, and access of staff to data*, **that is relevant for the effectiveness of business processes and which is typically unprotected or has only a limited protection** by partial procedural decisions (such as prohibitions on use of personal communicators and personal emails in a business environment; requirements for coordination of proposals and decisions with legal and budget units, requirement for RFID cards for access to buildings, premises, and printer devices; surveillance cameras in offices; personal password requirements for access to business information, and storage of log files) and other solutions that divide administrative levels of employees rather than protect information.

6. *Other protected personal information* such as *personal data, bank secrecy, tax and insurance secrecy*, etc., **which information usually does not affect business processes, but is intended to protect the privacy of individuals from unjustified interest, malice or mere curiosity**.

II. Management of protected information

Protected information management technology from practical perspective is an integrated system of actions that necessarily includes the following set of functions:

➨ Determining the systematic place, hierarchical and functional dependecies of the competent authority (at national level), respectively the unit (at corporate level) that will be responsible for planning and implementing information security policies, delegating powers and budgeting relevant activities.

➨ Identification of information representing state and official secrets (in the field of state security), identification of information

representing industrial and commercial secrets (in the field of corporate security), identification of intellectual property and know-how (in business), identification of other types of information.

➨ Establishment and implementation of a system of rules and procedures in accordance with the requirements of the security environment (at national level or for a particular enterprise) for protection of information, including in the IT field.

➨ Informing all employees concerned of this part of the rules and procedures intended for their level.

➨ Staff training on protected information identification

➨ Performance control

➨ Accountability of all processes connected to protected information use

➨ Periodic testing of the information security system and of the staff members with access to protected information, and upgrading it by eliminating the identified weaknesses.

The exchange of information has three different forms of manifestation:

➨ In electronic form (stored in data centers, distributed on public and private electronic networks, processed on official and personal workstations (stationary and mobile) and communicated through various electronic mails and applications).

➨ In analogue form (stored, processed and exchanged on paper).

➨ In oral form (verbal exchange between individuals).

Rules and procedures for information protection are applicable in all three cases mentioned above.

Information security officer should create internal rules and procedures and conduct training for all employees, taking into account the above circumstance.

Different types of information are protected under different regulations and its different nature imposes relevant managerial practices as follows:

1. State secret is regulated by the Classified Information Protection Act. The list of categories of information subject to classification as a state secret is legally established in Annex 1 to Art. 25 of RICIPA (Regulation on the Implementation of the Classified Information Protection Act) and exhaustively lists all types of information constituting state secret in three sections:

Section I – National defence-related information which includes:

➨ Structure, organization and functioning of the state bodies and of the Supreme General Command of the Armed Forces of the Republic of Bulgaria in a war, military or other emergency situations.

➨ Location, equipment, maintenance, operation and organization of the security of the central and territorial administration headquarters of the executive power and of the Armed Forces of the Republic of Bulgaria, intended for use in a war, military or other emergency situations.

➨ Organization and functioning of communication and information systems for connection of the state authorities and the Armed Forces of the Republic of Bulgaria under different conditions and levels of combat readiness and war.

➨ Information on bringing the country to a higher condition and level of combat readiness, wartime plans and estimates, projects and events related to ensuring national defence capabilities of the central and territorial administration of the executive power and of the trading companies producing military products. Information on the planning, organization and functioning of the mobilization deployment of the Armed Forces of the Republic of Bulgaria.

➨ and other information exhaustively listed in Annex 1 of RICIPA.

Section II Information related to the country's foreign policy and internal security, including:

➨ Foreign policy information, unauthorized access to which would seriously jeopardize the national security or could harm or threaten to cause significant damage to the country's positions in negotiations with another country.

➨ Information and documents on the internal political and military situation of other countries based on unpublished data whose disclosure could jeopardize the country's national security.

➨ Information on the organization, methods and means of performing specific tasks carried out by the operational and search and operational intelligence activities of the security and public order services as well as data about their special facilities and the information and objects obtained as a result of these activities, as well as data allowing the identification of persons who have assisted or assist them in these activities.

➨ Detailed organizational and staff structure of the security and public order services, as well as summary data on the personnel.

➨ Set-up data or data that can help identify persons who are not employees but cooperate or have cooperated with security and public order services.

➨ And other information, exhaustively listed in Annex 1 of RICIPA.

Section III Information relating to the economic security of the country, which includes:

➨ Documents for negotiations concerning the conclusion of financial contracts of nationwide importance, the disclosure of which could harm the national security.

➨ Research work of particular importance to the interests of the national economy commissioned by state authorities.

➨ Information on technical, technological and organizational decisions the disclosure of which would threaten to damage important economic interests of the country.

➨ Information on the operation of control and signaling devices, alarm systems and security regime, the knowledge of which could harm the national security.

➨ Political, economic or military information concerning foreign countries, the information being obtained provided that it will be protected as classified information.

➨ And other information included in the cited Annex of RICIPA.

2. Official information is the category of information that various regulatory acts declare an „official secret".

LIST OF CATEGORIES OF INFORMATION DECLARED BY VARIOUS REGULATORY ACTS AN OFFICIAL SECRET

➨ secret under the Underground Natural Resources Act – Art. 92 - the control authorities are obliged to observe the official, industrial and commercial secrets, not to disclose data from the inspections before their completion, and not to use the information from the inspection beyond its purpose;

➨ secret under the Judiciary Act (jury secrecy during deliberations) - Art. 136(2)

➨ secret under the Civil Servants Act - Art. 25

➨ secret under the Medicinal Plants Act - Art. 76 – information representing a trade or business secret

➨ secret under the Protection Against the Harmful Impact of Chemical Substances and Preparations Act - Art. 28(2) – production or trade secret

➨ secret under the Cadastre and Land Register Act - Art. 20

➨ - secret under the Public Procurement Act - Art. 9, item 9 - ensuring the protection of the trade secret of the candidates for public contracts and their proposals; Art. 38(2)

➨ secret under the Act on the Control of Foreign Trade Activity in Arms and in Dual-Use Goods and Technologies - Art. 19(4)

➨ secret under the Labor Code (the official information of the control authorities) - Art. 403

➨ secret under the Telecommunications Act (secret of telecommunications and communications) – Art. 5

➨ secret under the Energy and Energy Efficiency Act - Art. 142(3)

➨ secret under the Road Transport Act - (the official information provided by the carriers to the General Directorate „Automobile Administration“) – Art. 3(3)

➨ secret under the Act on Protection against Unemployment and Employment Promotion (secret of control authorities for official information and sources of information about violations) - Art. 105(3)

➨ secret under the Consumer Protection and Trading Rules Act (information on checks required by the Act) Art. 76, item 5

➨ secret under the Defence and Armed Forces Act (existing internal list of facts and information)

➨ secret under the Patent Act (the secret of the Patent Application) - Art. 83(3)

➨ secret under the Customs Act (an instruction specifies the facts and information constituting a customs secret) - Art. 17, item 5

➨ secret under the Transformation and Privatization of State-owned and Municipal Enterprises Act (the Council of Ministers defines and classifies the stages and documents on privatization deals)

➨ secret under the State Financial Control Act (official information on the inspected sites) - Art. 3, item 4

➨ secret under the Public Offering of Securities Act (facts and circumstances affecting the balances and operations on the securities accounts) - Art. 71(2)

➨ secret under the Radio and Television Act (information on sources of information) - Art. 10(1), item 3

➨ secret under the Tax Procedure Code

➨ secret of investigation under Penal Procedure Code

➨ secret under the Statistics Act - Art. 22

➨ secret under the National Audit Office Act (information on inspections) - Art. 4(2)

➨ secret under the Corporate Income Tax Act - Art. 69

➨ secret under the Personal Income Tax Act - Art. 60

➨ bank secrecy - Bulgarian National Bank Act

➨ bank secrecy under the Credit Institutions Act - Art. 52

➨ secret under the Currency Act (official information on currency transactions) official information - Art. 13(2) of APIA

➨ medical secret - Medical-Treatment Facilities Act;

➨ medical secret under the Code of Professional Ethics - Art. 51, Art. 55

➨ secret under the Social Security Code (personal information for the insured persons)

➨ secret under the Refugee Act (personal information on refugees)

➨ secret under the Access to Documents of the Former State Security Act

➨ secret concerning the identity of the voluntary MI assistants - Ministry of Interior Act

➨ secret under the Public Health Act (the secret of the patient)

➨ secret under the Social Assistance Act (secret about the identity of the assisted person and the amount of aid)

➨ secret concerning the information and data of companies on supplementary social insurance and of depository banks - under the Supplementary Voluntary Pension Insurance Act - the - Art. 36(2)

➨ secret of information in administrative or judicial proceedings, concerning the child, under the Child Protection Act - Art. 16.

➨ secret of correspondence under the Postal Services Act.

3. Intellectual property includes innovative technologies, creative works, new selection achievements all protected by various laws in three main categories, as follows:

Intellectual Property

Establishment of WIPO (UN), 1967

Industrial property	**Artistic property**	**New objects**
Paris Convention, 1883 Paris Union	Berne Convention, 1886 Rome Convention, 1961 Berne Union	
- Invention - Utility model - Trade marks - Industrial design - Indication of origin - Designation of origin - Pursuit of unfair competition - Know-how	- Works of literature, science and art - Performances of artists - Phonograms - Movie recording - Programs of radio and TV organizations - Data bases	- Topology of integrated circuits - New animal breeds - New plant varieties

Law on Copyright and Related Rights, 1993

Law on Patents and Utility Model Registration, 1993
Law on Marks and Geographical Indications, 1999
Law on Industrial Design, 1999
Law on Protection of Competition, 1998 (cancelled), 2008 (new)

Law on Topology of Integrated Circuits, 1999
Law on Protection of New Animal Breeds and Plant Varieties, 1996

Intellectual property is based on human creative work that generates innovative economic goods intended for market consumption with a limitation of use, which is realized only after permission of the right holder. Knowledge materialized in innovation, which intellectual property protection laws recognize as protected object, is a resource that should be recognized and viewed as a market manifested asset. On the one hand, the preparation and implementation of innovative solutions should be kept under the care of a good owner in secret from „competitive eyes and ears“ up to the moment the innovations become „intellectual property“ objects, when the laws will already protect the right holder. On the other hand, the intellectual property objects must be globally manifested and widely offered for marketing in each territory where the protection is realized.

Particular attention is needed with regard to „patent information“, which is made available to

the public which is always subject of interest for the corporate intelligence units of the competing entities. The same care is needed for the „works of science", which fall within the general protection of literary and artistic works, but have an independent role and significance, unbound in essence with literature or art. „The works of science are included in the broad range of intellectual property objects but have not been researched and clarified as such" (Tzakova V., 2009). Moreover, none of the international or national acts provides a legal definition of the term „works of science". The latter have been defined as „the objectified results of human research work that represent the achievements of his scientific work" (Tzakova V., 2009, p. 10). In addition, scientific results could be further developed into inventions, industrial designs or utility models, while „the works of science contain knowledge that is potential for know-how" (Tzakova V., 2009, p. 258) . This reality of the absence of a legal definition, coupled with the fact that the rights to scientific results have the potential for invention, utility model, industrial design or know-how, the scientific results always being of a particular scientist (researcher) but not of the state or the enterprise, places an emphasis, in the field of national and corporate security, on science and technology outcomes on the one hand and on the person who creates science and technology - on the other hand. In a contemporary context, „the strategy for successful development is in functional dependence on the new products designed and produced in the company" (Markova M., 2015). In particular, „the ideas for new products and their development into a project to be implemented in production must be based on the latest achievements in the field of science, technology and design in the relevant product and technology field" (Markova M., 2015).

In the field of scientific results, scientific and technical information and technology, intellectual property protection guarantees return of investment. However, from a security point of view, the person (scientist, inventor, designer, or creator) plays a central role and should be protected by the national and / or corporate security system as a „producer" of economic development and competitiveness at national or corporate level.

Intellectual property is protected by several laws at national level:

- *Inventions and utility models* under the Law on Patents and Utility Model Registration.
- *Marks, indications of origin and designations of origin* under the Law on Marks and Geographical Indications.
- *Industrial Design* under the Law on Industrial Design.
- *Works of literature, science and art, performances of artists, movie recordings, sound recordings, programs of radio and TV organizations, and databases* under the Law on Copyright and Related Rights.
- *New plant varieties and animal breeds* under the Law on Protection of New Plant Varieties and Animal Breeds.
- *Topology of integrated circuits* under the Law on Topology of Integrated Circuits.

4. Industrial and commercial secrets are protected by the Law on Protection of Competition. For two reasons, substantial attention should be paid to *industrial and commercial secrets*:

Firstly, the concept of industrial and commercial secrets is amazingly wide and can largely protect many and very different aspects of competitiveness.

Secondly, this method of protection is becoming increasingly important in the business world.

It is worth noting that insufficient understanding of intellectual property, as well as industrial and commercial secrets, leads to the loss of a competitive advantage amazingly quickly. From the point of view of corporate security, each enterprise can and should identify, describe and take the necessary

measures to protect its industrial and commercial secrets. The exemplary listing of the types of corporate information that, from a security point of view, should be included in the list of information defined as industrial and commercial secrets comprises:

- Business goals and enterprise development strategies
- Annual plan of the enterprise and its structure
- Price formation process
- Data from concluded / prepared contracts
- R&D activity
- Market research data
- All directions of the enterprise's IT security
- Systems and measures for site security
- System of measures for collection of data
- Schedule of cash transportation
- Information Network Security Systems
- And many other types of business information could be defined as a production or trade secret.

The definition of production or trade secret is given in the Law on Protection of Competition: „Production or trade secret shall mean facts, information, decisions and data related to the economic activities, the preservation of confidentiality of which is in the interest of the rightful holders thereof, and for which the latter have undertaken appropriate measures"[4].

The expression „appropriate measures" is an element of information security management technology and includes:

➨ First, the identification of this information in a list (which all employees with access to such information should be aware of), and

➨ Secondly, the establishment of internal rules for handling such information (usually with a special order of the Chief Executive Officer), the rules being valid for all employees who have access to corporate information defined as industrial and commercial secrets.

The exemplary order to approve a list of information defined as industrial and commercial secrets of the enterprise and the rules for handling such information in a corporate context is shown in Figure No. 1 representing an „Order to Approve Company's Industrial and commercial Secrets".

As can be seen from the attached exemplary order (Figure No. 1), an integral part of the order is the corporate information identified in the list, that is precisely defined as the industrial and commercial secrets of the enterprise (item 1 of the attached exemplary order).

A list of exemplary key corporate information by directions of the company's activity, that from the point of view of corporate security should be defined as a industrial and commercial secret, is shown in Figure No. 2 representing a „List of key information of the enterprise". Key corporate information should be defined as a industrial and commercial corporate secret, precisely because its knowledge of competitors would lead to a loss of competitive advantages of the enterprise, including loss of suppliers, customers, markets, employees, and ultimately money, which in turn guarantees a reduction in the period of market functioning of the enterprise.

[4] § 1, item 9 of the Transitional and Final Provisions of the Law on Protection of Competition

Figure No. *1. Order to approve a list of categories of information constituting trade and production secrets*

O R D E R

Subject: Approval of the list of categories of corporate information constituting industrial and commercial secrets of enterprise X

Pursuant to § 1, item 9 in conjunction with Art. 37 of the Law on Protection of Competition

I HEREBY ORDER:

1. I approve a list of the categories of information constituting industrial and commercial secrets of enterprise X, according to Appendix 1 of this Order.

2. I forbid the provision of the information under item 1 to persons whose official duties or specific tasks do not impose access to it.

3. Employees having access to the information under item 1 shall be obliged to protect subject information and not to use it or to disclose it beyond their official duties.

4. The employees who have been asked to provide information under item 1 to external organisations or individuals outside of their official duties shall notify the Corporate Security Officer on the interest in the enterprise's industrial and commercial secrets.

5. The Human Resources Directorate shall include a requirement for the protection of the information under item 1 in the job descriptions of the employees and ensure that all new employees of the enterprise are introduced to the order.

6. The Directors of Directorates shall ensure that all employees are aware of this Order as well as the attached list of the categories of information constituting industrial and commercial secrets of the enterprise.

01.01.2017 Executive Director

Figure No. *2 List of key information of the enterprise*

Trade information
- Contracts with key suppliers
- Contracts with key customers
- Formation of key prices
- Preparation of new products
- Preparation for a new market penetratiom
- Preparation for large-scale public campaigns

Production information
- Key equipment used
- New and existing key machines, technologies, recipes used in production
- Content of authorisation (licensing) documentation of the machines, technologies, recipes

Budget information
- List of the key institutions delivering services for the enterprise
- Bank accounts and names of employees operating the accounts
- Budgeting concept and processes
- Dislocation of cash-boxes / cartridges with large volumes of cash available
- Schedule of the cash transportation (irrespective of volume).
- Authorized persons and the vehicles carrying out cash transportation

Information on legal and regulatory affairs
- Negotiations and information on negotiations with key customers
- Enterprise employee official authorization data
- Data and information on current key industries

Human Resources information
- Personal data of company's senior management: home address, mobile phones, family member data
- Data on salaries, dividends, bonuses, financial compensation for company's senior management

Transport and storage information
- Lists of volumes and items in stock
- Routes of vehicles when transporting valuable items

IT and corporate communication information
- Dislocation and security systems of company servers
- Access and content of databases with key company information
- IP Address data
- Access and content of mailboxes of company's senior management

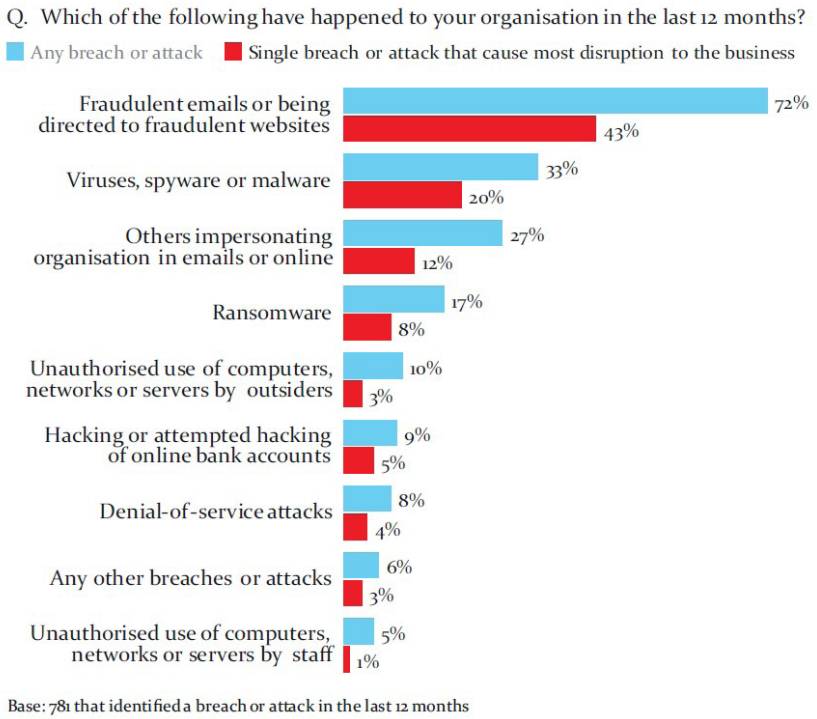
Security Information
- Type and number of technical security systems implemented,
- Number of security guards per shift, type and hours of work shifts
- Patrol routes

The key information of the enterprise must be protected as industrial and commercial secrets by establishing the "needed measures" including the identification of the key information and adopting internal rules and procedures not to disclose such information.

5. General (day-to-day) business information, including IT connectivity, networks, and access of staff to data, that is relevant for the effectiveness of business processes and which is typically unprotected or has only a limited protection by the internal rules and procedures.

Figure No. *3 Types of security breaches among the victim companies for 2017*

(See: https://www.gov.uk/government/uploads/system/uploads/attachment_data_Cyber_Security_Breaches Survey_2017).



Information security management has paid particular attention to the security of computer technology and networks (IT) over the past few years. This part of the business information needs priority protection. Its daily use by all employees is also at the root of its vulnerability. Both state-level and corporate-level secure communication channels, access control, effective rules and procedures for exchanging information inside and outside the organizational unit, as well as employee training.

Technology of IT infrastructure protection measures generally tends to focus on the following main areas, each with its own importance but always in an integrated system:

- Providing and maintaining secure data centers. Duplicated at a primary location and at a disaster location in case the primary location falls out of use for a certain period due to emergency situations, accidents and natural disasters.
- Establishing and maintaining a high-speed and reliable network connectivity

between the units in the organization, while maintaining a primary and disaster connectivity in this direction for the purpose of a high level of security.

- National and corporate rules and procedures for access to the IT network as well as for information backup, that are adequate to the dynamics of threats and risks of the environment.
- Training and periodic testing of systems, rules, procedures, employees.

In the Figure below, these directions can be covered in 10 basic (fundamental) steps to provide high IT security to the enterprise.

Figure No. *4 Percentage of companies that have taken steps to ensure IT security*

(See:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf)

	10 Steps to Improve IT Security	%
	Safe configuration and use of software – the company installs software updates as soon as they are available	88%
	Network security – securely configured firewalls	86%
	Malware Protection - installing and regularly updating protection (antivirus software)	83%
	User (End User) rights management – restrictive administrator control and providing access only to users that need such	77%
	Monitoring – surveillance of user actions or regular system checks in order to identify possible security breaches	51%
	Information risk management regime – through written cyber security rules and procedures or other type of documentation, the board of the company being aware of the measures taken	34%
	User training – recurrent staff training starting from the moment of recruitment, as well as introducing strict rules regulating how to use the company IT devices (computers, tablets, etc.)	28%
	Control of portable information storage devices (USB flash drives, hard drives, SD cards, etc.) – strict policy for what can be recorded on portable devices	21%
	Opportunities for the user to work at home or while traveling – strict rules defining how to do it (VPN, SSH, certificates and passwords for access, etc.)	20%
	Cyber incident management – a written plan how to respond to a cyber security breach	10%

Only half (exactly 51%) of all surveyed enterprises have taken the 10 steps.

6. *Other protected personal information* such as *personal data, bank secrecy, tax and insurance secrecy*:

Personal data of employees and customers. These are: data that directly or indirectly identify an individual. The protection of personal data is regulated by the Personal Data Act, and all organizations that operate personal data of employees and persons should be registered as *personal data controllers* in the information system of the Commission for Personal Data Protection (CPDP). Registration is free of charge. The CPDP keeps a Register of the personal data controllers and the personal data registers kept by them. Personal Data Controller (PDC) shall refer to any individual or legal person, or a central or local government authority

which determines separately or jointly with another person the purposes and means of personal data processing. In case the type of personal data processed, the purposes and means of processing are determined by law, the data controller or the specific criteria for its determination can be regulated by a legal act. The personal data controller shall process the personal data separately or by assignment to a data processor. The personal data controller or his / her representative shall be required to submit an application for registration and documents in a form approved by the Commission before the beginning of personal data processing.

The process of globalization, which covers all spheres of public life, also leads to the globalization of the threats and challenges facing the protection of personal data. This necessitates the integration of personal data protection into the overall information security policy. Of course, the major challenge to personal data protection in the 21st century is the digital revolution.

Tax and insurance information. These are: bank accounts; the amount of income; the amount of taxes and obligatory insurance contributions charged and paid; as well as any other data collected by an authority of the National Revenue Agency. The protection is regulated in the Tax and Insurance Procedure Code. The persons obliged to keep tax information in secret are the authorities and officials of the National Revenue Agency, the specialists and attracted assistants at the National Revenue Agency, the public servants, the experts carrying out tax expertise and all other persons who have been provided with such information or have become familiar with it for another occasion. Tax information can be used by the officials of the National Revenue Agency only for the direct implementation of their official duties and they are not allowed to use the information for purposes other than their direct duties.

Bank secrecy. It includes: bank account balances and bank account movements and its protection is governed by the Credit Institutions Act (CIA). Bank secrecy shall be facts and circumstances concerning the balances and transactions on accounts and deposits of the bank's customers. With the protection of bank secrecy, both the interests of individuals and the bank itself are guaranteed, as the credibility of its activity is also dependent on the way it protects the data of its customers. The obligation to protect bank secrecy consists in non-disclosure and prohibition of the use of such information to the personal benefit of the liable person or to the benefit of the members of his family. The circle of liable persons is specified in Art. 62, para. 1 of CIA - bank employees, members of the bank's managing and controlling bodies, BNB officials, liquidators, receivers, as well as any other persons working in the bank. When taking office, all bank employees shall sign a declaration regarding the keeping of bank secrecy. The obligation of said persons shall apply not only to the time they occupy the respective position but also to cases where their relations with the bank have ceased or its activity has been discontinued.

Conclusion

The new economy requires that a balance of access and protection of information is needed in order to maintain competitivness or strategic advantage, both at state and at corporate level. Modern management necessarily suggests information management.

On the one hand, it is essential that information about prices and quality of goods (at corporate level) and about the trends of relevant internal and external processes (at state level) should be obtained. On the other hand, it is equally important that the provision of information from individuals, business entitites and the state should be realized with the guarantees of respect for the human rights

of the individuals, the competitive advantages and national interests of the state, and the competitiveness of the business entities. This balance represents an increasing challenge for the information society in the era of global information connectivity. The efficiency of the management requires a flawless recognition of the types of information, knowledge of the legally guaranteed protection, experience in the implementation of the „necessary measures“ (within the meaning of the Law on Protection of Competition) and, together with this, quick accessibility and speed in the use of the information.

In is only under such conditions of an effective management of information that interests of the state, of any particular enterprise, of any manager or an individual can be guaranteed.

REFERENCES

Borisov, B., V. Borisova, 2015, Intellectual Property, University of National and World Economy Publishing, Sofia (in Bulgarian)

Friedman M., 2014, The Irreplaceable Milton Friedman, Selected Essays on Politics and Economics, UNWE, Sofia (in Bulgarian)

Gagova B., 2009, Traditions, continuity and development in the state management of economic life, Collection, edited by Associate Professor Boryana Gagova, “St. Kl. Ohridski” Sofia University Publishing House (in Bulgarian)

Markova, M. 2015, “Policies in Design as Intellectual Property”, “Innovation Based on Design in Europe: Political Framework, Priorities and Challenges”, Applied Research and Communications Foundation, Sofia, (available at: www.arcfund.net/fileSrc.php?id=22389) [Accessed 27 September 2017]

Tzakova, V., 2009, The Works of Science as Intellectual Property, University of National and World Economy Publishing, Sofia (in Bulgarian)

Cyber Security Breaches Survey, 2016, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf