European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.04.02.121

GCPMED 2020
Global Challenges and Prospects of the Modern Economic Development

THE IMPACT OF PERSONNEL THREATS ON THE ECONOMIC SECURITY OF THE ORGANIZATION

I. N. Makhmudova (a)*, A. A. Makhmudov (b)
*Corresponding author

(a) Samara State Economic University, Soviet Army Str., 141, Samara, Russia, Mahmudova.I@yandex.ru
(b) National Research Mordovian State University named after N.P. Ogarev, Bolshevistskaya Str., 68, Saransk, Republic of Mordovia, Russia, anvarik1997@yandex.ru

Abstract

The topic of company security is central to the work of the security service. This article describes the factors that pose a threat to the security of a modern organization. Possible directions of risks caused by the actions of the organization's personnel that create personnel threats are disclosed. The role of personnel security and elimination of personnel threats in the organization's security system has been determined. The article reveals the concept of competitive (business) intelligence, identifies the functions of this service. The concept of "industrial espionage" is disclosed. In operational practice, it turns out that a large number of personnel threats are represented by a wide variety. At the same time, in order to neutralize personnel threats, the powers and competence of the organization's security personnel are clearly not enough. In this regard, within the framework of this study, a set of measures that make up an integral security system is considered. The central place in the study is devoted to the issue of eliminating personnel threats. Since personnel threats are created by the organization's own personnel, the need for interaction of all personnel services within the framework of a single system for ensuring personnel security and the security of the organization as a whole is substantiated. The powers of each of the participants in this process in their relationship and interaction are delimited. Defined measures to counter personnel threats and neutralize the negative consequences of unauthorized actions in the organization.

Keywords: Competitive (business) intelligence, industrial espionage, methods of competitive struggle, organization security, personnel risks

https://doi.org/10.15405/epsbs.2021.04.02.121
Corresponding Author: I. N. Makhmudova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The digital economy has already made its own adjustments to the activities of modern enterprises. New competitive relations have developed in the business environment for sales markets, finances, human and material resources. Business survival is at risk from the uncontrolled influences of the external and internal environment. According to the PwC study, there is an approximately equal number of cases of fraud committed by internal and external criminals (40% each) (PwC, 2020). The rest of the crimes are associated mainly with collusion between them.

External risks are determined primarily by the fact that:

- the area of competitive relations is becoming extremely aggravated due to the introduction of new digital technologies in the activities of modern enterprises, and, therefore, more risky;

- many market mechanisms in the field of ensuring the economic security of enterprises do not work, since the enterprises have not formed an integral system of security measures, or it operates in fragments. Although total fraud losses (according to PwC research) amounted to US $ 42 billion over the past two years, only 56% of companies have investigated the worst case of fraud (PwC, 2020);

- the market of business information ensures economic and personnel security in organizations, due to the confidentiality of information that is not formed in sufficient volume. No enterprise is ready to share the secrets of organizing its own security service, so as not to be at risk of negative impact from the outside.

2. Problem Statement

The issue of eliminating personnel threats to ensure the security of the company is central to the work of the security service. However, in operational practice, it turns out that a large number of personnel threats are represented by a wide variety. Here are just some of the data. Employees were responsible for 62% of leaks, while contractors accounted for only 6%. In total, in the past year, there were 1556 cases of data breaches from organizations around the world, which is 3.4% more than in the previous year.

In 93% of cases, leaks were associated with theft of personal data and payment information. In 2020, in connection with the transition of companies to remote locations, Rostelecom recorded a 25% increase in personal data leakage, which exacerbates the issue of personnel security. The share of trade secrets leaks was 5.4%. Most of the stolen personal data (94.6%) accounted for 44 “mega-leaks”, as a result of which at least 10 million such records became available to attackers (General Director, 2017).

Many personnel threats are associated with the use of information technology. In the modern world, the problem of cyber terrorism and cyber-attacks hitting enterprises is widely discussed. Cybercriminals are most active in the following areas of cyberattacks: malware, web attacks, phishing, attacks on web applications, spam, DDoS attacks, identity theft, data security breaches, insider threats, botnets, physical manipulations, information leaks, ransom ware viruses, cyber espionage, cryptojacking (malicious mining) (McKinsey, 2020). Their speed, scale and breadth of coverage of economic sectors is impressive. Here are some statistics. Hackers tried to steal information: in 30% of attacks they stole personal data, in 24% - credentials, in 14% - payment information. Human resource security vulnerabilities are associated with the scale of distribution and the growing surface of cyberattacks. The difficulty lies in the localization of a given geographic space. There is also the organizational complexity of countering these attacks, since the

https://doi.org/10.15405/epsbs.2021.04.02.121
Corresponding Author: I. N. Makhmudova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

sources of cyber attacks are decentralized, and the network is represented by a wide cyber infrastructure. According to PwC research, the total number of information security incidents is growing at an average rate of 48% annually (42.3 million incidents meanthat, on average, 117,339 cyberattacks are committed every day.

With the rise of cyberterrorism, the cost of businesses rises to defend against cyber threats. In Russia, 22% of the “CEOs” of companies affected by this problem noted that the incurred loss exceeded $ 1 million, which is slightly higher than the average worldwide (19%). At the same time, 41% of respondents in our country reported that the loss did not exceed $ 100,000 (around the world, 45% of respondents named the same damage) (Bailey et al., 2020).

At the same time, in order to neutralize personnel threats, the powers and competence of the organization's security personnel are clearly not enough. In this regard, it is not necessary to consider individual measures, but a set of actions that ensure an integral and effective security system.

3. Research Questions

Within the framework of this study, it is necessary to delineate the powers of all participants in the process of ensuring personnel security in the organization in their relationship and interaction. It is important to define the role and content of the work of each security system participant. Determine the main risk areas of personnel activities that pose a threat to the security of the enterprise.

Before proceeding to the analysis of risks leading to personnel threats, it is necessary to get ahead of the very concept of "personnel security", what is it? It is worth paying attention to those factors that can destabilize the situation in the company, cause unauthorized actions by the staff.

In order to ensure the security of the enterprise, it is necessary to determine under what conditions the activities of the security service will be most effective in eliminating personnel threats? What services in the structure of the enterprise are able to provide real assistance in neutralizing personnel risks? How to form an integral personnel security system?

Moreover, it is important to determine the potential for the involvement of each particular employee in "industrial espionage". Why do their own personnel assist in such illegal actions, and why is such activity punishable by law in Russia? What personnel threats does the use of "industrial espionage" methods entail as opposed to "competitive intelligence" methods? Even more important is the question of how to preserve the intellectual capital and secure the intellectual property of the company, and why is it so important?

4. Purpose of the Study

In the profile of risk factors of any organization, personnel risks constitute a considerable part. That is why, before talking about the economic security of the organization as a whole, it is necessary to carefully build a system of personnel security.

The very concept of "personnel security" is twofold in its content. On the one hand, it is aimed at protecting the rights of employees from illegal actions of the employer, which cause them serious harm. There are still such violations on the part of the employer as: delays in the payment of wages; substitution of employment contracts for civil law contracts when employing citizens; violation of the work and rest

https://doi.org/10.15405/epsbs.2021.04.02.121
Corresponding Author: I. N. Makhmudova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

regime of employees (for example, not providing a well-deserved vacation or, on the contrary, sending an employee on a forced (unpaid) vacation); illegal dismissal and much more.

On the other hand, personnel security includes protecting the organization from unauthorized actions or inaction of its personnel. These include: theft, registration, collusion with competing parties, forgery, damage to the employer's property, theft, disclosure of confidential information and much more.

At the same time, since it is important for each organization to take its rightful place in a competitive environment in relation to other organizations, then one of the most expensive and difficult to ensure advantages of an organization is its intellectual capital and intellectual property protection. Intellectual capital can multiply the market value of the organization itself, and therefore the organization becomes quite attractive for investors. In addition, the intellectual capital of an organization is a potential target for attracting attention from both competitive intelligence and industrial espionage and other unfair competitive methods. There are cases of theft of a patented product and its use for personal purposes for profit. Such an example was told by Kostaniants, professor of the department of firm management at the Graduate School of Corporate Governance, RANEPA: a manager was invited to a Russian company to develop a patented product. He stole the company's computer codes, left for the United States, where he registered his company, and then began to promote the modified product on the Russian market. As a result, he was convicted under Article 147 of the Criminal Code of the Russian Federation for illegal use of patent rights (Tolstoukhova, 2018).

Functions of the competitive (business) intelligence service

To ensure the economic well-being of the organization, it is necessary to timely identify and adequately respond to the identified personnel threats. For this, an independent information and analytical security service or a competitive (business) intelligence service should be organized in the organization's structure. Its tasks include collecting and providing the heads of the relevant structures with complete and relevant business information. Thanks to the availability of such information, the management decisions taken will be timely and optimal. The tasks of the service include:

- collection, analysis and systematization of data from the business environment and personnel threats within the company, that is, the identification of external and internal threats to the functioning of the organization;

- identification of risks and preparation of recommendations on the issues of legal protection from illegal personnel threats;

- work with financial documents in the investment field in Russia and abroad;

- application of competitive intelligence methods in collecting information on competing firms (analysis of processes and trends in their development, as well as drawing up a psychological portrait of their leaders-leaders);

- development of the concept of economic security of the organization, preparation of a strategic plan for the development of the organization;

- development and implementation of individual organizational, managerial and financial projects and technologies.

System for ensuring personnel security in the organization

https://doi.org/10.15405/epsbs.2021.04.02.121
Corresponding Author: I. N. Makhmudova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Personnel threats to the security of an organization can be formed in all areas of personnel activity. That is why the competitive intelligence service needs, first of all, to establish close contact with the personnel management service represented by its director (not the personnel department!). It should be separately noted that it is the HR director (HR department) that deals with HR. The personnel department has nothing to do with operational work with personnel. He conducts documentary work with personnel, records the results of each employee's work in personal affairs (i.e. work with documents). And structurally, the HR department is subordinate to the HR director, along with the department of labor organization and motivation), the training center (or the personnel development department), the department of personnel assessment and certification and social service. The recruiting department in the structure of the organization can be an independent element, but it can also be a service in the structure of the personnel department. As you can see, almost all areas of personnel work are represented by separate structural divisions or services. The production staff is controlled by line managers and their superiors.

In this regard, the organization's security system should not work independently from all the named services if it wants to be effective. In other words, the security system in the organization is provided not only by the security service, but by the entire personnel department and each individual employee of the organization. The functions of the directorate (service) for work with personnel directly include the detection of various kinds of personnel threats.

Since we are talking about a competitive intelligence service, the concept itself should be defined. "Intelligence" is "the collection of information about an enemy or competitor to ensure their security and gain advantages in the field of armed forces, military operations, politics or economics". Intelligence can use both legal methods of collecting information (for example, collecting and analyzing data from open sources, listening to radio channels from abroad, surveillance using reconnaissance satellites) and illegal operations that fall under the concept of "espionage" or " theft of information ”.

Competitive intelligence is both appropriate and legitimate. The intelligence collects its transformed into new directions and projects for the effective development of the organization. Unlike competitive intelligence, industrial espionage uses methods of illegal secret theft of information using special equipment (technical devices) or a personal computer (Kravtsov & Zhelnov, 2014). Data stored on a server or in the "cloud", by e-mail, telephone conversations - that is, any information and on any medium, becomes available. To protect the business sector from industrial spies, it is necessary to make serious investments in technical means of information security: the purchase of video cameras, voice recorders, so-called "jammers" that protect the confidentiality of information. In Japan, companies spend almost $ 200 million a year on such equipment, while American corporations spend up to $ 0.5 billion. In Russia, companies use the human factor instead of purchasing expensive spy equipment. Nevertheless, the volume of the domestic market for information security products, according to some sources, is about $ 150 million (HR Director, 2015). The information received, constituting commercial, tax or banking secrets, may be disclosed or used illegally. In Russia, industrial espionage is punishable by law (Federal Law of July 21, 1993 No. 5485-1 "On state secrets"; Federal Law of 27.07.2006 No. 149-FZ "On information, information technologies and information protection"; The Criminal Code of the Russian Federation; Federal Law of 12.08.1995, N 144-FZ "On operational investigative activities"; Federal Law of 29.07. 2004 No. 98-FZ "On commercial secrets"; Federal Law of 26.07. 2006 No. 135-FZ "On protection of competition"; Federal Law of

https://doi.org/10.15405/epsbs.2021.04.02.121
Corresponding Author: I. N. Makhmudova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

28.12.2010 No. 390-FZ "On Security".). In particular, Article 183 of the Criminal Code provides imprisonment for up to ten years for the use of industrial espionage.

5. Research Methods

Directions and measures to counter personnel threats. How to counter personnel threats and industrial espionage? How to ensure the economic security of the organization?

First of all, it is necessary to carry out a set of measures to manage personnel security, starting with the formation of a strong personnel policy. To protect your organization from potential intruders, you need to put the first hurdle in the selection process when hiring. This requires highly professional recruiters who are able to carry out high-quality express diagnostics using all available assessment methods, both in working with the applicant and with the documentation provided to him. It is important to double-check the information. When working with a resume, use the techniques of "finding bottlenecks", "reading between the lines", if necessary, conduct "content analysis". When conducting an interview, use the technique "if not a secret", "interception", ask clarifying questions - UCQ (universal clarifying question - "Please clarify what you mean when you say ...") and, the main rule, do not think out for the applicant is what he wants to say! Another direction in neutralizing personnel threats to ensure the security of an organization is working with existing personnel. And in this direction, it is necessary to ensure the conduct of high-quality briefing, supported by regular monitoring of performance. It is also required to regularly inform the staff about understanding which information does not pose a security threat, and which is highly confidential and not subject to disclosure. Up to the signing of documents on non-disclosure of commercial secrets. It is at this stage that the precise work of the security service is important, which must monitor and timely prevent (using IT services and other possible means) cases of information leakage.

A well-thought-out system of staff motivation can play a good role. At the same time, it is important to achieve not only complete satisfaction of employees with work and work results (read - fair pay), but also provide an opportunity to openly “speak out” (feedback system), without fear for their position and the threat of being fired. Because there is always a "well-wisher" ("random interlocutor") who is ready to listen to everything secret and use the information received to break up the organization.

Since today electronic document circulation is carried out everywhere, electronic storages with databases (necessary for the successful and efficient operation of an enterprise) are being created, an important direction of ensuring the security of an organization in terms of storing and transmitting information is the formation of a powerful IT service that can withstand various kinds of technical failures and hacker attacks. In October 2018, the Corporation for the Management of Domain Names and IP Addresses (ICANN) carried out the first-ever replacement of cryptographic keys that protect the Internet Domain Name System (DNS) (RG.RU, 2018). This Key Signing Key (KSK) is necessary for any Internet user. It increases the level of information security. And in organizations, within the framework of ensuring the security system, it is also recommended from time to time with a certain regularity to monitor the change of passwords on the personal computers of specialists and employees.

It is impossible to ignore the legal aspect of ensuring the security of the organization. It is important to have not only a legal department in the structure of the organization, but also to form the legal literacy of specialists and managers who are able to foresee and eliminate potential threats to personnel security at

https://doi.org/10.15405/epsbs.2021.04.02.121
Corresponding Author: I. N. Makhmudova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

their level. An example can be - incorrectly accrued wages; errors in the execution of contracts when hiring (terminological, first of all) and when employees are fired; errors in maintaining financial documents; mistakes in making management decisions resulting in a conflict with staff, etc.

6. Findings

To summarize, the following should be noted:

1.Methods of "competitive intelligence", in contrast to "industrial espionage", are completely legal, and the information collected by it is transformed into new directions and projects for the effective development of the organization. Industrial espionage, on the other hand, uses methods of illegal secret theft of information using special equipment, and the information obtained, constituting commercial, tax or banking secrets, can be divulged or used illegally. In this regard, the security service should actively identify subjects as a source of personnel threats, involved in activities or carrying out industrial espionage in the organization.

2. A set of measures for managing personnel security is proposed, including the formation of a strong personnel policy, primarily at the stage of recruiting personnel. As part of the work with the existing personnel - high-quality briefing, supported by regular monitoring of performance. Regularly inform staff about understanding what information is highly confidential and not subject to disclosure. As part of increasing staff motivation - to focus on organizing a feedback system. To conduct electronic document management and ensure the security of electronic storages with databases, it is necessary to form a powerful IT service capable of withstanding various kinds of technical failures and hacker attacks. Additionally, form the legal literacy of specialists and managers who are able to foresee and, at their level, eliminate potential threats to personnel security.

3. It is proposed to create a collective system of personnel security in order to ensure operational and tactical actions that have a positive impact on the coordination and synchronization of the functioning of individual services for the localization, neutralization and elimination of personnel threats.

7. Conclusion

The main factor that creates a threat to the security of the organization is personnel of the organization. Real threats to personnel security do not occur deliberately, but due to illiteracy, poor awareness of personnel about how to store confidential information. Among the deliberate security threats, industrial espionage is distinguished, using unauthorized methods of collecting information. Some of these methods pose a cyberthreat to an organization called cyber terrorism. Another part of the methods is related to the recruitment of personnel who become an active supplier of trade secrets. The security system in the organization is provided not only by the security service, but by the entire personnel directorate and each individual employee of the organization. In this regard, the organization's security system should not work independently of the services involved in working with personnel if it wants to be effective.

https://doi.org/10.15405/epsbs.2021.04.02.121
Corresponding Author: I. N. Makhmudova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

References

Bailey, T., Maruyama, A., & Wallance, D. (2020). The energy-sector threat: How to address cybersecurity vulnerabilities. https://www.mckinsey.com/business-functions/risk/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

Federal Law of 12.08.1995, N 144-FZ "On operational investigative activities". http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1001995033000&docid=106

Federal Law of 26.07. 2006 No. 135-FZ "On protection of competition". http://www.consultant.ru/document/cons_doc_LAW_61763/

Federal Law of 27.07.2006 No. 149-FZ "On information, information technologies and information protection". http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1002006031000&docid=104

Federal Law of 28.12.2010 No. 390-FZ "On Security". Edition of: 02/06/2020. http://www.consultant.ru/document/cons_doc_LAW_108546/

Federal Law of 29.07. 2004 No. 98-FZ "On commercial secrets". http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1002004032000&docid=26.

Federal Law of July 21, 1993 No. 5485-1 "On state secrets". http://docs.cntd.ru/document/9004687

General Director (2017). The number of data leaks from Russian companies increased by 80% in 2016. https://www.gd.ru/news/7175-qqn-17-m3-23-03-2017-chislo-utechek-dannyh-iz-rossiyskih-kompaniy-vyroslo-na-80-v-2016-godu?utm_source=www.gd.ru&utm_medium=refer&utm_campaign=Rubrcontentblock_news

HR Director (2015). Counteraction to industrial espionage. https://www.hr-director.ru/article/65692-qqq-15-m9-protivodeystvie-promyshlennomu-shpionaju

Kravtsov, A. A., & Zhelnov, I. I. (2014). On industrial and economic espionage, as well as unfair competition. *World of Science, 1*, 1-10.

McKinsey (2020). IIF/McKinsey cyber resilience survey. Cybersecurity posture of the financial services industry (2020) https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/the%20cybersecurity%20posture%20of%20financial%20services%20companies%20iif%20mckinsey%20cyber%20resilience%20survey/iif-mckinsey-cyber-resilience-survey-vf.pdf

PwC (2020). PwC's global economic crime and fraud survey 2020 Fighting fraud: A never-ending battle. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

RG.RU (2018). Protection of domain names. https://rg.ru/2018/10/11/chem-grozit-internet-polzovateliam-pervaia-v-istorii-smena-kriptograficheskih-kliuchej.html

The Criminal Code of the Russian Federation. http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1001996025000&docid=4886

Tolstoukhova, N. (2018). Commercial secrets are most often extracted through employees. https://rg.ru/2018/12/05/kommercheskie-tajny-chashche-vsego-vyvedyvaiut-cherez-sotrudnikov.html