THE HUMAN FACTOR IN BUSINESS SECURITY

Konstantin Poudin[1]

Introduction

In the most general sense business security suggests the absence of threat to business interests. It is a state of the internal and the external environment in which the firm/company/corporation (no matter of what kind of business entity it is) operates. This environment is characterized by absence of threats and dangers to its interests or if there are any, the business can tackle them. Business security could be further defined as a policy at organizational level aimed at foreseeing, avoiding and/or responding to the threats to the business interests and creating conditions for the achievement of business goals. In other words, business security eliminates the threats and creates opportunities.

Business security [1] to a great extent depends on the human factor. People actively participate in the process of building and maintaining business security but they are also able to compromise and "destroy'' this security and threaten organizational interests.

In this article the notion "human factor" should be understood as the staff/ employees of different business organizations. The main objective of the publication is to present the human factor's influence on business security. The achievement of this objective is based on the following tasks:

- Analysing the human factor's role in business security;
- Analysing the human factor's negative influence on business security;
- Describing the means/ways to restrict the human factor's negative impact [3] on business security;
- Presenting the results of a survey on the human factor's impact on the company security.

The analysis and conclusions are not based on observations of a particular type of business. They refer to the majority of the business practices.

At the beginning of the article, the author would like to express his gratitude to the 48 experts who voluntarily participated in the survey.

[1] Konstantin Poudin, PhD, Assoc. Prof., Department National and Regional Security, UNWE, email: kpoudin@unwe.bg

Human Factor's Contribution to Business Security

Business security goals could be the recognition of threats, their prevention or elimination, or creating of opportunities for normal functioning of the business. The achievement of these goals depends to a great extent on the human factor in the organization.

According to Boyko Mitev, the most important security factor for any company is the integrity of its staff. If an organization has a carefully selected, honest and loyal staff, the security risk, and in particular internal security breaches, is significantly low. (Toneva and Mitev, 2016)

The staff's contribution to the business security could be discussed from a broad and a narrow perspective.

Broad sense – In a broad sense business security means creating opportunities and achieving organizational goals. It depends on all the people working for the business entity that create opportunities with their knowledge, skills and motivation. As a human factor they improve with age and experience. The availability of appropriate people with appropriate training and motivation performing well their duties is a matter of security for the business entity.

Each member of the team could threaten the business security. Unqualified and unmotivated personnel with low morale and negative attitude to work can cause huge losses for the business organization.

In a very broad sense business security depends on the individual performance. No comprehensive conceptual framework of individual work performance exists and many studies have been conducted aiming at summarizing the various concepts (Koopmans L., Bernaards C.M., Hildebrandt V.H., Schaufeli W. B., de Vet H. C. W., van der Beek A. J., 2011, pp. 856-866).

John P. Campbell and Brenton M. Wiernik point out that individual job performance should be defined as things that people actually do, and the actions they take that contribute to the organization's goals.

The same authors also distinguish performance itself and (a) the determinants of individual differences in performance and (b) the outcomes of performance (e.g., results, goal achievement, the bottom line). The determinants include such factors as individual trait variables (e.g., cognitive abilities, personality, stable motivational dispositions, physical characteristics and abilities), state variables (e.g., relevant knowledge and skill, attitudes, malleable motivational states), and situational characteristics (e.g., the reward structure, managerial and peer leadership), as well as the interactions among them (Campbell and Wiernik, 2015, pp. 48-49).

According to Robert Mathis and John Jackson, there are three major factors that affect how a given person performs: (1) individual ability to do the work, (2)

effort expended, and (3) organizational support. (Mathis and Jackson, 2007, pp. 70-71) These factors are illustrated in Figure 1.

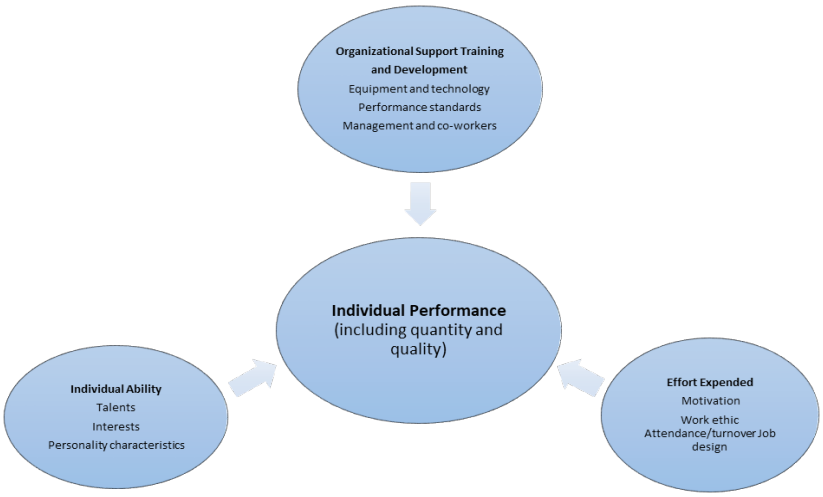

Fig. 1. Factors of Individual Performance

Human resource management in any business organization is essential to ensuring security in this very broad meaning. It is connected with all aspects of how people are employed and managed in organizations.

Narrow sense – In a narrow sense business security means the absence of threats or elimination of existing threats. There is staff in the business organization with specific responsibilities and functions regarding this aspect of security. The tasks of this staff are recognition, avoiding or elimination of threats to the business interests.

The big companies have their own security staff and security unit. The Director of Security, or Chief Security Officer (CSO), or Chief Information Security Officer (CISO) is the person responsible for the security in a big business entity. He/she is part of the top management. He/she is responsible for the security of personnel, physical assets of the corporation and the information stored in it on paper and/or electronic form.

The CSO participates in the development of corporate security strategy. He/she gathers, systematizes and analyses information about events and threats that might jeopardize the safety and security of personnel, assets and reputation of the corporation. The CSO is responsible for leading and building a strong security culture where people have a high degree of security awareness.

According to American Society for Industrial Security (ASIS) International, founded in 1955, a global community of security practitioners, having a role

in the protection of assets – people, property, and/or information, CSO has the following functions:

- *Relationship Manager* – Establishes and maintains relations of trust with the leadership of the organization, public officials and professional organizations. Advises all customers.
- *Executive Management and Leadership* – Establishes, motivates and leads a team of professionals who accept organizational culture, business needs and aspire to excellence.
- *Subject Matter Expert* – Provides expertise related to risks and effective security measures.
- *Governance Team Member* – As a part of the management team, he/she informs the management of any risks that could jeopardize the interests of the organization.
- *Risk Manager* – Identifies, analyzes and informs of the risks to the interests of the organization.
- *Strategist* – In cooperation with other departments in the organization and stakeholders develops security strategy that is oriented towards the identified risks.
- *Creative Problem Solver* – Supports adequate decision making in case of problems. Helps to reduce damage / losses in the case of accidents (ASIS Int., 2004, p. 6).

At a lower level a specific security staff (so called "security specialists'') working at a security unit of the organization fulfils a set of duties related to different aspects of security of each business organization. Their security related functions could be physical security, personnel security, information security, etc.

The rest of the staff of the business organization also contribute directly to the security, being security aware after trainings and briefings, demonstrating appropriate behavior, and following the security rules and procedures.

Human Factor's Negative Influence on Business Security

The staff that has to create opportunities could also intentionally or unintentionally compromise business security. Today's most damaging security threats do not come from malicious outsiders or malware but from trusted insiders – both malicious insiders and negligent insiders (Insider Threat Report, 2018, p. 3). Insiders' malicious activity could have bad consequences for the business organizations because it causes financial losses, creates distrust among staff and negatively affects the image of the organization.

Two-thirds of organizations (66%) consider malicious insider attacks or accidental breaches more likely than external attacks. Forty-four percent of the organizations believe all (malicious, external and accidental) attacks are as

equally damaging, while 31% believe malicious/deliberate insider attacks are more damaging than external attacks (14%). The low weight placed on accidental insider breaches (11%) seems too low, perhaps underestimating the potential damages (Insider Threat Report, 2018, p. 14).

In the 21 century, Noncho Dimitrov points out, every business uses the new opportunities given by the information technologies (ITs). Every business faces the vulnerabilities related to ITs (Dimitrov, 2019, p. 391). Users are one of these vulnerabilities. That is why it is most commonly spread that "insiders" are members of the staff who have access to ITs and work with specific organizational information, and use it inappropriately. This staff is a source of "insider threats".

In this regard, Nedko Tagarev claims that insider threats are a very interesting topic. On the one hand, the company, organization, etc. has to use IT specialists with IT knowledge. On other hand, they have at least the basic knowledge how to breach IT security systems. This topic becomes even more interesting if these professionals get physical access (Tagarev, 2019, p. 292).

Jeffrey Hunker and Christian Probst claim that a definition of what an insider threat is obviously depends heavily on the definition of what an insider is. If an insider is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure, the insider threat is (posed by) an individual with privileges who misuses them or whose access results in misuse (Hunker and Probst, 2011, pp. 6-7).

According to another definition, an "insider threat", or an "insider", is any person who exploits, or intends to exploit, their legitimate access to an organization's assets to harm the security of their organization, either willingly or unwillingly, through espionage, terrorism, unauthorized disclosure of information or loss or degradation of a resource (or capability) (Protective Security Requirements, 2018).

It has to be underlined that the insiders are not only members of the staff, particularly IT users and the insiders' attacks are not directed only to information assets through compromising information security.

Insiders can be members of the organization or associates (contractors, business partners or guests), anyone with authorization to perform certain activities, anyone who is authenticated by the system (including unauthorized users using valid credentials), or an unwilling or coerced accomplice to an external actor (Kont et al., 2015, p. 12). In this article, the term "insider" means first and foremost a person, who works or has worked in the organization.

Common insider acts include:

- Unauthorized disclosure of official, private, or proprietary information.
- Fraud or process corruption.
- Unauthorized access to ICT systems.
- Economic or industrial espionage.
- Theft.

- Violence or physical harm to others (Protective Security Requirements, 2018).

The insiders could have different motivation to commit malicious acts.

- *Financial benefits* – Some members of the staff tend to compromise the security of the business entity in order to gain financial benefits. This is the most commonly spread motivation. They steal and sell information to other stakeholders – competitors, state actors, individuals. Very often disloyal staff uses the confidential information to start their own business which is similar to the business of the employer. The personnel, having the same financial motivation, could sabotage the organizational activity in different ways – stealing or destroying equipment, refusing to fulfil its tasks or fulfilling them in a wrong way and not on time, creating conflict situations etc. in order to get money from competitors, states, criminal or terrorist organization.
- *Response for unjust attitude and dissatisfaction* – Usually every employee compares his/her efforts and contribution to the organizational activity to the recognition, career promotion and material benefits received by the business organization. Very often members of the staff believe that they are underestimated by the employer while some of their colleagues are unfairly favored and stimulated. This assessment and self-assessment could be objective, true, but it could also be subjective and inaccurate. In this case they start to protest by sabotaging the organization, stealing and selling information, creating conflicts etc.
- *Form of protest and convictions* – In many cases the staff is a threat to the company's interest due to moral reasons. The employee might be disappointed by the organization. Over time, they understand that its activity is harmful to the environment and/or society. Feeling guilty and angry at the company, they start to oppose it, creating problems and compromising its security. The motivation for terrorist actions is based on radical convictions.
- *Negligence and incompetence* – In many cases the staff compromises business security unintentionally. Some members of the staff make mistakes which could financially harm the organization due to insufficient experience and poor training. Irresponsibility and negligence also have bad consequences for the organization's activity.

The individuals pose threats for a variety of reasons (Combating the Insider Threat, 2014, p. 2). Dimitris Gritzalis sums up some of the theories explaining the malicious behaviour in Table 1.

Table 1. Human Behaviour Prediction – Insider Threat Understanding Augmentation

Theory	Behaviour
General Deterrence Theory (GDT):	Person commits crime if expected benefit outweighs cost of action.
Social Bond Theory (SBT):	Person commits crime if social bonds of attachment, commitment, involvement and belief are weak.
Social Learning Theory (SLT):	Person commits crime if associates with delinquent peers.
Theory of Planned Behavior (TPB):	Person's intention (attitude, subjective norms and perceived behavioural control) towards crime key factor in predicting her behaviour.
Situational Crime Prevention (SCP):	Crime occurs when both motive and opportunity exist.

Source: Gritzalis, 2014, p. 10

According to the 2018 Insider Threat Report, 90% of organizations feel vulnerable to insider attacks. The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%), and the increasing complexity of information technology (35%).

A majority of 53% confirmed insider attacks against their organization in the previous 12 months (typically less than five attacks). Twenty-seven percent of organizations say insider attacks have become more frequent (Insider Threat Report, 2018, p. 4).

Measures to Reduce Human Factor's Negative Influence on Business Security

Counteracting insider threats is rather difficult because they may remain unnoticed for years. It is not easy to distinguish the malicious actions from daily duties performance. This is especially true for IT specialists, though not only for them. The intentional malicious actions may be hidden.

Eliminating insiders' malicious acts and negative impact on the business activity is a part of the business security policy, which includes concepts, plans, programs, rules, procedures, measures, actions and resources. The purpose of business security policy is to ensure the personnel, physical and information security of the company in favor of protection of organizational assets and realization of the business goals.

The establishment of business security policy is the managers' responsibility. It is part of the management process. Tsvetan Tsvetkov points out that decision making is at the heart of the management process (Tsvetkov, 2014, p. 9). Elaboration of business security policy requires making many and different decisions, as well as prepared and experienced decision makers. The decision making process also needs information. Irrelevant or bad information leads to inadequate managerial decisions (Dragomirov, 2015, p.12).

Business security policy has three main dimensions – prevention, detection and response. Each of these elements is important to ensuring business security.

Prevention – Prevention has many aspects. It aims at eliminating or minimizing the risk of insider threats. Recruitment and selection of loyal and devoted employees, their proper motivation and training, which are part of human resource function, are aspects of the prevention. Building and maintaining appropriate business security culture can also be added as a preventive measure. The development of surveillance systems is another aspect of the prevention.

Detection – The purpose is detection of insider threats or intentions of malicious acts. It could be based on monitoring staff's behavior, establishing detection indicators, reporting. Business security culture is also important for detection of threats. Technical equipment and specialized software are used for this purpose as well.

Response – It includes the reaction of ongoing insider threats. This reaction may vary depending on the character of the adverse actions and the scale of the caused damages. For instance, if an insider has the practice to steal assets of the organization, he/she could be announced by the competent authorities, dismissed from work and the company may bring a lawsuit against him/her.

The employees must be familiar with the security policy of the organization and informed about the changes of this policy. For this purpose, they periodically participate in different trainings. Within these courses the staff becomes acquainted with the norms and the security requirements. The most important role of these trainings is the development of security awareness – knowledge about security matters, right attitude to security matters and behaviour, which does not underestimate security.

Organizational culture, as one of the potential cultural levels studied and summarized by Kiril Dimitrov, Ivaylo Ivanov and Marin Geshkov (Dimitrov, Ivanov, Geshkov, 2018, pp.121-123), and particularly its security aspects is extremely important. Building security culture and especially its maintenance is a constant and continuous process. Igor Khripunov points out that security culture is a vehicle to improve the human factor through a set of managerial, organizational and other arrangements that include not only the technical proficiency of the people entrusted with security but also their willingness and motivation to follow

established procedures, comply with regulations and take the initiative when unforeseen circumstances arise (Khripunov, 2008, p. 2).

Matthew Bunn and Scott D. Sagan give 10 lessons which is in the form of practical advice for managers, derived from the past experience, regarding to the insider threats and the counter measures (Bunn and Sagan, 2014, pp. 3-20). They are summarized in Table 2.

Table 2. Lessons from Past Mistakes

Lesson	Explanation
Lesson #1: Don't Assume that Serious Insider Problems are NIMO (Not In My Organization)	First, and most fundamentally, organizational leaders should never assume that their personnel are so loyal that they will never be subject to ideologies, shifting allegiances, or personal incentives that could lead them to become insider threats. Second, managers should understand that guards themselves can be part of the insider threat.
Lesson #2: Don't Assume that Background Checks will Solve the Insider Problem	The belief that personnel who have been through a background check will not pose an insider problem is remarkably widespread. There are two reasons why this belief is mistaken. First, background checks are often not very effective. Second, even completely trustworthy employees may become insiders, especially if they are coerced.
Lesson #3: Don't Assume that Red Flags will be Read Properly	Due to different reasons some of the red flags may go unnoticed. The individual incentive systems and information-sharing procedures encouraging people to report are important in that case.
Lesson #4: Don't Assume that Insider Conspiracies are Impossible	Conspiracies of multiple insiders, familiar with the weaknesses of the security system (and in some cases including guards or managers), are among the most difficult threats for security systems to defeat. Insider conspiracies routinely occur. In one database, they constituted approximately 10 percent of the crimes examined.
Lesson #5: Don't Rely on Single Protection Measures	Many security systems, however, are much more vulnerable to being defeated than they first appear—especially to insiders, who may be among the staff who know how they work. That is why several security measures need to be implemented and at least two persons have to operate with them.

Lesson #6: Don't Assume that Organizational Culture and Employee Disgruntlement Don't Matter	The culture of an organization and the attitudes of the employees have a major impact on security. Matthew Bunn and Scott D. Sagan have quoted General Eugene Habiger, former Department of Energy "security czar" and former commander of U.S. strategic forces, who said: "Good security is 20 percent equipment and 80 percent culture."
Lesson #7: Don't Forget that Insiders May Know about Security Measures and How to Work Around Them	Insider threats are a particularly dangerous form of reactive adversary because insiders are well placed to understand the organization's security procedures and their weaknesses.
Lesson #8: Don't Assume that Security Rules are Followed	Despite the presence of security rules the staff could not follow them strictly. Security-conscious organizations create rules and procedures to protect valuable assets. But such organizations also have other, often competing, goals: managers are often tempted to instruct employees to bend the security rules to increase productivity, meet a deadline, or avoid inconvenience. And every hour an employee spends following the letter of security procedures is an hour not spent on activities more likely to result in a promotion or a raise. Other motivations—friendships, union solidarity, and familial ties—can also affect adherence to strict security rules.
Lesson #9: Don't Assume that Only Consciously Malicious Insider Actions Matter	Some of the highest consequence threats that security organizations face are from malicious outsiders: for intelligence agencies this means an adversary's spies; for military units, it is enemy forces; for nuclear facilities, it is thieves and saboteurs. Security organizations may therefore focus on preventing attacks or theft by outsiders, and to the degree that they protect against insider threats, they focus on the danger that individuals inside the organization might be recruited by or become sympathetic to a malicious outsider group—hence the attention paid to preventing "penetration" through counterintelligence and personnel screening and monitoring.
Lesson #10: Don't Focus Only on Prevention and Miss Opportunities for Mitigation	The need to maintain both rigorous prevention programs and serious mitigation preparations is recognized by many experts. There can be a strong temptation to favor prevention efforts over mitigation efforts, especially when dealing with exercises in which the public is involved, in order to avoid public fears that security incidents are likely.

Source: Bunn and Sagan, 2014, pp. 3-20

Results of Survey *Human Factor's Impact on Security of the Company*

A blitz survey on *Human Factor's Impact on Security of the Company*, related to the studied topic has been conducted. More than 40 (48) persons, aged 18-47, mainly economists holding a Master's degree in Economics of Defence and Security with specialization in Corporate Security acquired within training course conducted by the Department of National and Regional Security at the UNWE have been asked to give their answers to questions related to human factor impact on business security, personnel motivation and loyalty, and the measures against insider threats.

The anonymous survey was conducted in early July 2019. The questionnaire was composed of 10 basic questions with multiple choice responses. The most interesting answers from a practical point of view are presented and commented below in the text.

At the beginning of the survey the experts were asked to point out the most important characteristic of the employees with which they mainly contribute to achieving company's goals (Question 1). At the top of this ranking are the following features of the staff: Motivation and willingness to work – 43,8%, Creativity and desire of self-improvement – 31,3%, Knowledge and experience – 16,7%. These first three characteristics are followed by Loyalty to organization and leadership – 4,2% and Discipline and compliance with rules and responsibilities in the company – 2,1%.

The results of the survey confirmed the results of other studies on the insider threats. The experts point out the insider threat as a main threat to the company's interests – Figure 2. The majority of the respondents – 77,1% – think that the insiders, including a company employee and any other person having some authorized access to company assets, are more likely to be a source of threat to the company. The rest – 20,8% – believe that outsiders, including different categories of persons, such as terrorists, criminals, hackers, competitors, etc., are more likely to make troubles for the enterprise. According to 2,1% of the respondents, a combination, a kind of cooperation between insiders and outsiders could threat the company's interests.

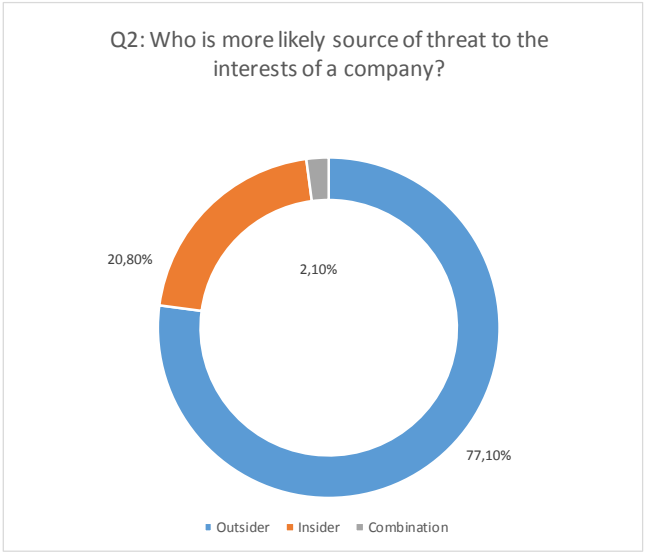

Fig. 2. Q2: Who is more likely a source of threat to the interests of a company?

Regarding the assessment of risk of malicious actions taken by employees there is not a big difference between the experts who think that a high risk exists – 45,8% and those who believe that a medium risks exists – 39,6%. Only 14,6% of the respondents are of the opinion that risk of insider threat is low. Nobody has given the answer "There is no such risk" – Figure 3.

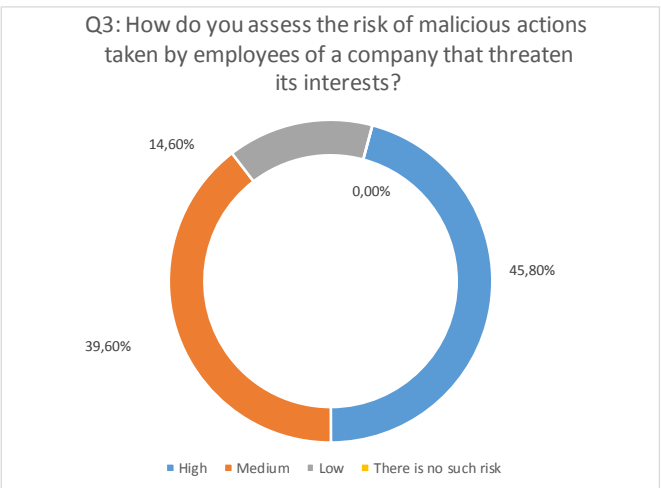

Fig. 3. Q3: How do you assess the risk of malicious actions taken by employees of a company that threaten its interests?

According to the respondents, the main reason for malicious actions is discontent, as shown by Figure 4. This is the answer given by 41,7% of the experts. The causes for discontent are not specified but they could vary from unjust reward and unjust promotion system to bad working conditions or conflicts with the managers and other employees. Money is another major motivator of insiders to commit malicious acts. This is what 22,9% of the experts believe. The insiders sell information or other assets belonging to the company for financial benefits. The following reasons are moral motives (12,5%) and unusual situations where the employee does not give a clear idea or he/she gives a wrong idea about his/her actions (10,4%). The respondents add an additional cause – lack of "moral compass". They also believe that the insider threat could be caused by a combination of two or more reasons (2,1%).

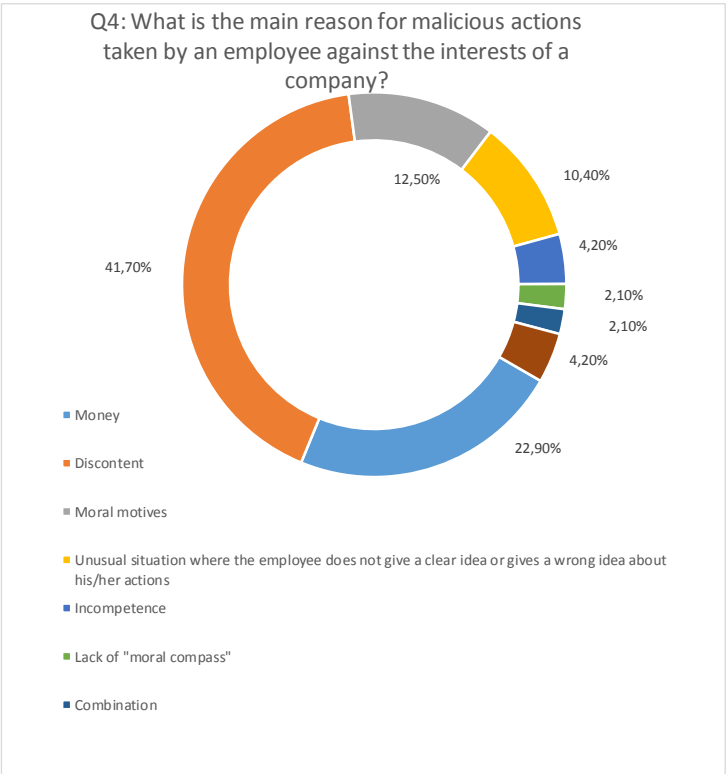

Fig. 4. Q4: What is the main reason for malicious actions taken by an employee against the interests of a company?

Question 5 gives additional information about the reasons for malicious actions. Its purpose is to study the employee's loyalty to a company. The respondents have given a priority to the following reasons for insider threats: leadership's

attitude to the staff – 29,2%, personal moral of each employee – 18,8%, and career opportunities – 10,4%. According to 8,3% of the experts, the staff's loyalty depends on salary and additional material and moral incentives.

Question 6 is about the measures for limiting insider threats. The main recommendations given by the experts are related to eliminating causes of discontent which corresponds to the answers to Question 4. According to 35,4% of participants in the survey, the fair assessment of working performance reduces the probability of insider threats. The other main measure is fair criteria for promotion – 20,8%. The regular salary update based on working performance is the third main measure – 18,8%. Only 10,4% of respondents think that the development and application of ethical standards is a solution to the problem. The share of experts who have shown the training on security culture as an appropriate measure is rather small – 6,3%. Experts have formulated other measures out of the given in the questionnaire, such as: additional mechanisms of control, monitoring the level of satisfaction, teambuilding etc. – Figure 5.

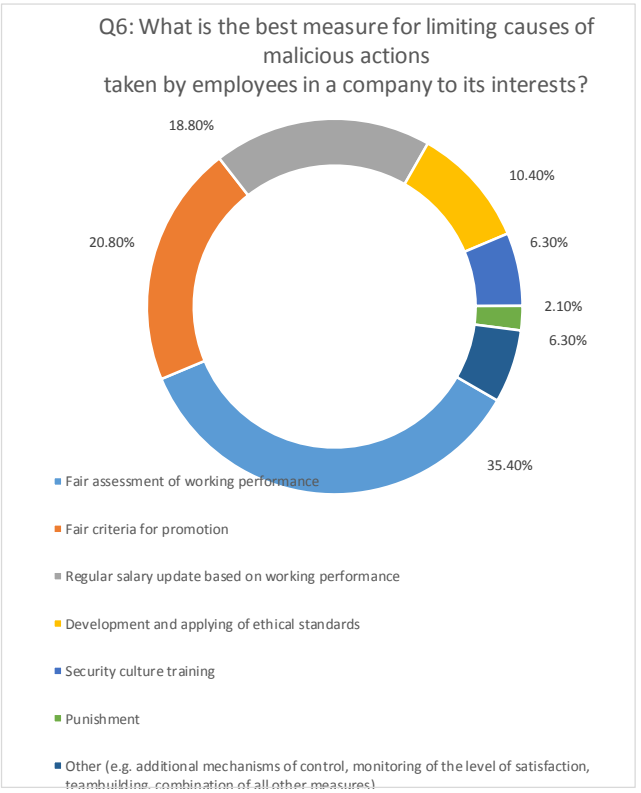

Fig. 5. Q6: What is the best measure for limiting causes of malicious actions taken by employees in a company to its interests?

Conclusion

The study presented in this article once again confirms the importance of the human factor for business security. The staff plays a crucial role for the achievement of the business goals but it can also threaten the company's interests.

The results have confirmed the conclusions of other studies on the insider threats. The experts have pointed out the insider threat as a main threat to the company's interests.

The results of the survey have shown that the staff's discontent is the main reason for disloyalty. The managers should introduce methods of employees' satisfaction assessment which will allow prevention of insider threats.

The leadership's behaviour and especially its attitude to each staff member is among the main reasons for disloyalty. It means that a probable "betrayal" is based on interpersonal relationships. Money is a cause which should not be neglected.

The experts have not given a priority of security culture training as a measure of reducing insider threats. They believe that fairness (fair assessment of working performance, fair criteria for promotion etc.) as a guiding principle in the relationship between management and employees is leading to the reduction of internal threats.

One of the most commonly additionally given answers by respondents is "combination". The negative impact of the staff depends on a combination of factors but the restriction of insider threats will also be achieved through a combination of measures.

Notes

[1] The notion "business security" is used to indicate security of different-sized business entities.

[2] The notions "impact" and "influence" are used as synonymous in this article.

Bibliography:

Димитров, Д., (2012), Приложение на сценарийното планиране в бизнеса, отбраната и сигурността. София, ИК-УНСС.
(Dimitrov, D., 2012, Prilozhenie na stsenariynoto planirane v biznesa, otbranata i sigurnostta. Sofia, IK-UNSS)
Димитров, К., Иванов, Ив., Гешков, М., (2018), Прокламираната фирмена култура във виртуалното пространство – тенденции и предизвикателства. ИК-УНСС, София. (Dimitrov, K., Ivanov, Iv., Geshkov, M., 2018, Proklamiranata

firmena kultura vav virtualnoto prostranstvo – tendentsii I predizvikatelstva, IK-UNSS, Sofia)
Драгомиров, Н, (2015), Информационни системи и технологии в логистиката. първо издание. ИК-УНСС, София.
(Dragomirov, N, 2015, Informatsionni sistemi i tehnologii v logistikata, parvo izdanie, IK-UNSS, Sofia)
Bunn M. and Sagan S. D., (2014), A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes. Cambridge, Mass.: American Academy of Arts and Sciences. Available at: https://www.amacad.org/sites/default/files/publication/downloads/insiderThreats.pdf, (Accessed: 7 July 2019)
Business Security (2018), Understanding Business Security. [Online] Available at: http://www.businesssecurity.net/ , (Accessed: 25 November 2019)
Campbell J.P. and Wiernik B. M., (2015), The Modelling and Assessment of Work Performance. Annual Review of Organizational Psychology and Organizational Behaviour. [Online] 2015. Vol. 2. pp. 47-74. Available at: http://psychology.psiedu.ubbcluj.ro/old/files/docs/Studenti/teza_licenta/2016_iulie/Campbell%202015.pdf, (Accessed: 6 July 2019)
Chief Security Officer Guideline (2004), ASIS International. Available at: https://cdn.fedweb.org/137/268/ASIS%2520Chief%2520Security%2520Officer%2520Guide-Public.pdf , (Accessed: 23 June 2019)
Combating the Insider Threat (2014), US Department of Homeland Security. Available at: https://www.us- cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf , (Accessed: 19 June 2019)
Dimitrov, N., (2019), Cyber Security and Contemporary World. In: 6th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE – 2016), December 3-4, 2016. [Online], Sofia, UNWE, pp. 391-395. Available at: http://icaictsee.unwe.bg/past-conferences/default.html, (Accessed: 26 June 2019)
Gritzalis, D., (2014), Holistic Information Security: Human Factor and Behavior Prediction using Social Media. Available at: https://www.infosec.aueb.gr/Publications/Security%20Project%202014.pdf , (Accessed: 19 June 2019)
Insider Threat 2018 Report. CA Technologies. Available at: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf, (Accessed: 20 June 2019)
Mathis R. L., Jackson J. H., (2007), Human Resource Management. 12th ed. Mason: Thomson. South-Western.
Khripunov, I., (2008), Russia's Security Culture and WMD Proliferation, Presented at: Tomorrow's Proliferation Pathways: Weak States, Rogues, and Non-States, July 17-18, 2008, Belfast (Accessed: 15 April 2015).
Kont M., Pihelgas M., Wojtkowiak J., Trinberg L., and Osula A.-M., (2015), Insider Threat Detection Study, The NATO Cooperative Cyber Defence Centre

of Excellence, Talin, Estonia, Available at: https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf, (Accessed: 23 June 2019)
Koopmans L., Bernaards C.M., Hildebrandt V.H., Schaufeli W. B., de Vet H. C. W., van der Beek A. J., (2011), Conceptual Frameworks of Individual Work Performance – A Systematic Review, Journal of Occupational and Environmental Medicine. [Online] 2011, 53(8). pp. 856-866 Available at: https://www.wilmarschaufeli.nl/publications/Schaufeli/358.pdf, (Accessed: 6 July 2019)
Pavlov, G., and Karakaneva, J., (2016), Additional Costs for Security in Handling Classified Information. Trakia Journal of Sciences, No 3, Trakia University , St. Zagora, Bulgaria, pp. 251-255.
Protective Security Requirements (2008), Personnel Security. [Online] Available at: https://www.protectivesecurity.govt.nz/personnel-security/why-personnel-security-matters/, (Accessed: 19 June 2019)
Poudin, K., (2018), Developing and Maintaining Business Security Culture. UNWE Yearbook, [Online] 2018, pp. 255-269. Available at: http://unwe-yearbook.org/en/journalissues/article/10068, (Accessed: 26 June 2019)
Poudin, K., (2019), Resources for Business Security. In: 6th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE – 2016), December 3-4, 2016. [Online], Sofia, UNWE, pp. 419-422. Available at: http://icaictsee.unwe.bg/past-conferences/default.html, (Accessed: 24 June 2019)
PSI Handbook of Business Security. Securing People and Processes. (2007), Ed. By W. Timothy Coombs, ABC-CLIO, Wastpoint, United States.
Tagarev, N., (2019), Basics of Management for Cloud Computing Security (Part 2 Physical Security). In: 6th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE – 2016), December 3-4, 2016. [Online] Sofia, UNWE, pp. 285-293, Available at: http://icaictsee.unwe.bg/past-conferences/default.html, (Accessed: 26 June 2019)

THE HUMAN FACTOR IN BUSINESS SECURITY

Abstract

Human resources have a crucial role in each organization. They are very important with their skills, abilities, motivation, moral and attitudes. The achievement of business goals and business security goals as well depends on a great extent on human factor in the company. Business security goals are the recognition of threats, their prevention or elimination, or creating of opportunities for normal functioning of the business. The article presents the human factor's positive and negative influence on the business security.

Key words: business security, human resources

JEL: M12, M14