Alina Wołoch, MA
WSB University in Dąbrowa Górnicza
e-mail: alina.woloch@wp.pl
ORCID: 0000-0003-0032-4825

Věra Holubová, PhD
VSB TU Ostrava
e-mail: vera.holubova@vsb.cz
ORCID: 0000-0001-8198-3157

Bernardo Amorim
Lusófona University of Porto
e-mail: bernardoooliveiraamorim@gmail.com

Andrea Plauter
Budapest Business School
e-mail:plauter.andrea@gmail.com

DOI: 10.26410/SF_2/22/12

THE IMPORTANCE OF WHISTLEBLOWERS FOR THE ORGANIZATION'S SECURITY SYSTEM

Abstract

The security of an organization is influenced by a number of processes that take place in it and also by internal, external factors, or the all-important human factor. Therefore, the implementation of even the best procedures does not 100% guarantee the security of the organization and does not provide protection against irregularities that may be committed by its employees, contractors or subcontractors. The implementation of a whistleblowing management system (hereafter WMS) in a company

can be an effective preventive barrier for the company and a tool for obtaining information from so-called whistleblowers, verifying the information received about violations of the law and issuing recommendations for action, the implementation of which will protect the organization from future abuses, which in turn should have a positive impact on minimizing financial or image losses.

Keywords

whistleblower, whistleblowing, organization security

Introduction

The purpose of this article was to present the importance of whistleblowers in the functioning of the organization's security system, to introduce the role they play and the potential that lies within them. Every organization, in addition to its statutory purpose, which defines the directions of its activities, development, struggles with the problem of ensuring the security of these activities. It is a broadly understood concept, as it relates to the sphere of physical, technical security, but also to ensuring the security of systems, protecting personal data, ensuring business continuity or production. Also extremely important is the financial security of the organization or image, which is often decisive in ensuring the high market position of the company. The introduction of numerous regulations in force in an organization is aimed at ensuring maximum security. It is usually preceded by estimating risks, defining areas that are key to the operation of the organization and introducing barriers that will prevent their materialization. However, there are no procedures that are effective in every field. There is always the human factor, which may not adapt to these regulations and, driven, for example, by the desire to achieve its own benefit, may commit irregularities that will consequently expose the organization to various types of losses. Contrary to appearances, however, these financial ones, although often huge, are not the most significant from the point of view of the organization. The most severe are those that negatively affect the image of the company, as it can be very difficult and sometimes even impossible to rebuild trust and position in the market[1]. Therefore, it is important to detect irregularities at the stage of their planning or shortly after their occurrence, which will allow to minimize losses and implement protective barriers against the occurrence of similar irregularities in the future. Such an element of "protection" of the organization is the Whistleblowing Management System, which allows whistleblowers, i.e. people with knowledge of irregularities to report them[2], through internal channels established in the organization, verification of information and corrective actions.

Methodological and methodical assumptions

The purpose of this publication was to present the role of the whistleblower and its impact on organizational security. Important from the perspective of the research problem was the demonstration of both the capabilities and requirements of the Whistleblowing Management System, as well as the presentation of the results of research conducted to date, showing the important role of the whistleblower institution for the security of the organization. This publication used the method of analyzing the literature on the subject and legal acts, which resulted in expanding the

[1] K. Stopczyńska, *Rola kreowania wizerunku firmy w kreowaniu silnej pozycji rynkowej*, „Przedsiębiorczość i Zarządzanie" 2014, tom XV, zeszyt 5, część II, s. 250.

[2] A. Pietruszka, *Ochrona sygnalistów (whistleblowers) w kontekście wolności wypowiedzi*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny"2020, Rok LXXXII, Zeszyt 1.

state of knowledge and made it possible to identify areas for further research. The comparative method showed what effects the lack of an implemented Whistleblowing Management System can have on an organization, while the synthesis method used led to a combination of the facts and literature examined in the process of analysis, leading to the formulation of conclusions.

A whistleblower in the organization

Whistleblowing in its definition involves an individual reporting irregularities that have occurred in an organization[3]. None of the actions against the organization happen in a vacuum. So there is a good chance that one of your co-workers will witness the incident or come into possession of documents that will confirm the violation. The whistleblower does not have to be an employee of the entity in question. It could just as well be a former employee, contractor, contractor, intern or volunteer. Anyone in the course of his or her activities for the organization can become a witness, come into possession of information crucial to ensuring its security. In order to enable such individuals to provide the knowledge they possess in accordance with Directive 2019/1937 of the European Parliament and of the Council (EU) Companies are required to establish internal whistleblowing channels to safeguard the public interest[4]. In order to convince as many potential whistleblowers as possible, both private and public entities should put in place at least one confidential channel for making reports, while these forms can be many more – from passing a report directly to an employee of the relevant unit implementing WMS in the organization, to reporting by email, telephone, in the form of traditional correspondence or through special platforms for recording reports. Regardless of the form chosen, however, the key is to ensure that the whistleblower's data is protected from outsiders. Of course, this will not apply in the case of anonymous reporting, although the content of the report, including the personal data of other employees contained in the information provided, will also be protected. Whistleblowers are very keen to choose the anonymous form of reporting due to the low psychological barrier. The awareness of remaining anonymous gives them a sense of security, although for the organization it is the least effective form in seeking to clarify the matter and prevent the escalation of irregularities. This is primarily due to the inability to obtain additional information from the whistleblower, to verify certain facts or included wording.

A much higher quality is offered by named and confidential reports. Knowing the identity of the whistleblower, there is the possibility of obtaining additional information, evidence, but most importantly, the organization is able to provide protection against retaliation against the person

[3] See: Ł. Bolesta, *Sygnalizacja jako przejaw obowiązku lojalności wobec pracodawcy?*, „Annales" 2018, Vol 65 No 2.

[4] See: Dyrektywa Parlamentu Europejskiego i Rady Europy (UE) 2019/1937 *w sprawie ochrony osób zgłaszających naruszenia prawa Unii* (Dz.U. UE I.305 z 26.11.2019 r.).

making the report. According to the Directive introduced, the protection should include, first of all, protecting the whistleblower from threats, negative actions from colleagues, but also prevent termination of employment as a result of making a report, deterioration of working conditions or pay, restriction of access to training. Importantly, this protection should extend not only to those who made the report, but also to those who contributed to the disclosure of information and to the whistleblower's relatives. These are significant changes in the legislation, as previously the whistleblower was protected only by certain provisions of the Labor Code or the Criminal Code, but the burden of proof was on the whistleblower[5]. It was the whistleblower who, until now, had to prove in court that the employer had retaliated as a result of the report, which was usually doomed to failure[6].

The key to building an effective WMS in an organization is to make employees aware of the essence of the whistleblower's role. Emphasizing his loyalty, concern for the common good and the desire to safeguard the interests of the organization when confronted with the person of the perpetrator, who, in order to achieve his own benefits, commits fraud, demonstrating a lack of loyalty and posing a risk to the safe operation of the entity. As shown by the results of the "Global Economic Crime Survey 2020", conducted by PWC in the field of economic crime, more than 60% of companies in Poland as a result of fraud reported losses of 400,000 PLN, and more than a third declared losses of about 4 million PLN.

At the same time, the same research points to huge deficiencies in companies in terms of implementing anti-corruption procedures (72% of entities), as well as the failure to utilize the potential of the Compliance Officer, who is employed in only 6% of all companies[7]. This also contributes to the fact that nearly three-quarters of organizations fail to leverage the fraud information they have. The person of a Compliance Officer would enable proper handling of whistleblower reports, verification of the information provided and implementation of follow-up actions. These are clearly deficits of Polish companies that threaten the security of the organization in a real way. The most common abuses according to the survey include corruption and fraud. They affected almost half of the entities taking part in the survey. It is worth noting at this point that it is precisely these types of irregularities that other employees, employed, for example, as assistants to members of the board of directors, those who approve financial documents, HR staff or controllers, often have knowledge of. Abuses will occur, even at the highest level, whether among executives or the Board of Directors. This is supported by the results of EY's 2021 Global Business Integrity Survey, according to which 42% of board members believe

[5] R. Szymczykiewicz, *Miejsce tzw. sygnalistów w polskim systemie prawnym,* Warszawa 2018, s. 14.

[6] A. Kobylińska, M. Folta, *Sygnaliści – ludzie, którzy nie potrafią milczeć,* Warszawa 2015, s. 9.

[7] *Price Waterhouse Cooper 2020 – Global Economic Crime Survey* na: https://www.pwc.pl/pl/media/2020/2020-03-05-badanie-przestepczosci-gospodarczej-2020.html (dostęp: 15.07.2022 r.).

that unethical behavior by senior executives is tolerated in their organization, even 33% of executives would be willing to commit irregularities for their own benefit, and as many as 57% of board members would have concerns if the public could take a closer look at the decisions they make[8]. When fraud occurs, direct financial losses are just the beginning. They are often accompanied by other costs that are less quantifiable but potentially much more damaging – from damage that affects the brand, to loss of market position, to negative impact on employee morale"[9].

Implementing a WMS is designed to minimize reputational risk by responding to communicated irregularities at an early stage. The perpetrator planning the irregularity may abandon his plans after balancing possible gains and losses. If this does not happen, however, awareness of WMS and the institution of the whistleblower in the organization can act as a second, often effective barrier before deciding to commit a violation. However, if the risk materializes, thanks to an effective system, there is a good chance to react quickly and prevent escalation of the abuse or image losses. Whistleblowers can, of course, harm the organization, but this only happens if the information goes directly to the public or the media. This is why it is so important for whistleblowers to be aware of internal whistleblowing. To this end, organizations should establish and actively inform employees about the solutions that have been put in place. This helps to reduce the risk of scandals and thus prevent far-reaching damage to the organization's reputation.

According to the Directive, whistleblowers have the option of reporting through internal channels within the organization. These are usually the most effective because they provide the ability to respond quickly to the information provided, the cell responsible for verifying the signal provided is familiar with the work environment and is able to take effective action to clarify the events described[10]. However, this generates the risk of bias. The next step is external reporting to the President of the OCCP or the Consumer Ombudsman. This type of notification ensures full impartiality. However, it is not advisable for the security of the organization primarily because the information gets out and there is no possibility of quick intervention against the detected irregularity.

The last rung in the hierarchy of available channels for whistleblowers is the so-called public disclosure. It is justified in cases where reporting through earlier channels has not produced the intended results, or where the whistleblower has reasonable grounds to believe that the violation will pose a direct or obvious threat to the public interest, there is a risk of destruction of evidence, or there is suspicion of collusion between the authority and the

[8] *Ernst & Young 2020 – Światowe badanie uczciwości w biznesie* na: https://www.ey.com/pl_pl/news/2020/06/covid-19-utrudnia-prowadzenie-przedsiebiorstwa-w-sposob-etyczny (dostęp: 16.08.2022 r.).

[9] *Price Waterhouse Cooper 2020…*

[10] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937.

perpetrator[11]. Whistleblowers choose to go public mainly when they do not trust their organization's investigative or reporting procedures, and when they have already tried unsuccessfully to disclose their position internally, or when there is no whistleblowing system in place. If a whistleblower reports his or her observations directly to an external body (e.g., the media), however, he or she can be held criminally liable if, for example, he or she reveals trade secrets in the process. Exceptions apply if the whistleblower acts in the public interest[12].

Communication and training are an important component of WMS. Increasing employee awareness of the reporting options available and the benefits to both employees and the organization of disclosing such information has a real impact on the effectiveness of the entire system. As a 2019 study by the Batory Foundation shows, as much as 36% of the public has concerns about being perceived as a whistleblower, 23% of employees believe that information provided in a report is difficult to prove, which shows the lack of faith of a sizable percentage of employees in an effective and well-functioning WMS system, and 18% show fear of retaliation[13].

The directive shows us the areas that require an absolute response when a report is received. These have been identified as key to security: public procurement, product services and financial fish and AML prevention, product safety and compliance, transportation safety and environmental protection, radiological and nuclear safety, food and feed safety, public health, consumer protection, privacy and personal data protection[14]. However, it is up to each entity separately to decide whether to expand this catalog to include irregularities relevant to its business, such as, for example, unethical actions by its employees. It is worth noting that a whistleblower can provide information not only about violations that have already occurred but also those that are yet to occur or for actions or omissions that the person making the report has reasonable grounds to believe constitute a violation. Legitimate concerns and suspicions do not have to be supported by evidence[15].

As a 2020 Report to the Nations study covering the entire world shows, for companies with more than 100 employees, as much as 56% of information about irregularities in the organization was provided by whistleblowers, and the introduction of channels for reporting fraud realistically reduced the average amount of losses in the company. For entities with functioning channels, these losses settled in the neighborhood of $100,000, and were three times higher

---

[11] Rezolucja Parlamentu Europejskiego z dnia 24 października 2017 r. w sprawie uzasadnionych środków ochrony sygnalistów działających w interesie publicznym podczas ujawniania poufnych informacji posiadanych przez przedsiębiorstwa i organy publiczne (2016/2224(INI)) (Dz.U. UE. C-346 z dnia 27.09.2018 r.).

[12] Projekt ustawy *o ochronie osób zgłaszających naruszenia prawa* na: https://www.legislacja.gov.pl/projekt/12352401 (dostęp: 12.06.2022 r.).

[13] M. Waszak, *Strażnicy demokracji. Nowe perspektywy ochrony sygnalistów,* Warszawa 2020, s.18.

[14] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937…

[15] See: M. Wurm, *Die Whistleblower-Richtlinie der EU: Was sind die Konsequenzen für Unternehmen?,* na: https://se-legal.de/die-whistleblower-richtlinie-der-eu-was-sind-die-konsequenzen-fur-unternehmen/ (dostęp: 12.05.2022 r.).

in the absence of channels[16]. In addition, research shows that 95% of all overt filings in Poland were made by Company employees, and only 5% by people outside the organization. This shows how much potential there is for whistleblowers – employees of the organization who can make a real difference in improving the security of the organization.

Conclusions

An important element in building an organization's security is a well-functioning system for handling whistleblower reports. At the time of an incident, the organization's operational security is at risk, whether corruption, theft, conflict of interest or money laundering is involved. The transmission of information from a whistleblower about fraud demonstrates the ability of the crew to identify risks and also awareness and trust. This makes it possible to verify the information provided by a properly trained team, which, if violations are confirmed, will recommend disciplinary consequences and preventive barriers to minimize the risk of similar abuses in the future. The purpose of this article has been achieved due to the indication of the potential of whistleblowers and the demonstration of their importance in the functioning of the organization's security system.

Bibliography

Association of Certified Examiners 2020 – Report to the Nations na: https://www.acfe.com/report-to-the-nations/2020/.

Bolesta Ł., *Sygnalizacja jako przejaw obowiązku lojalności wobec pracodawcy?*, „Annales" 2018, Vol 65 No 2.

Czupryński A., *Aksjologiczne aspekty bezpieczeństwa*, „Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2015, No 4(35)/2015.

Dyrektywa Parlamentu Europejskiego i Rady Europy (UE) 2019/1937 *w sprawie ochrony osób zgłaszających naruszenia prawa Unii* (Dz.U. UE I.305 z 26.11.2019 r.).

Ernst & Young 2020 – **Światowe** *badanie uczciwości w biznesie* na: https://www.ey.com/pl_pl/news/2020/06/covid-19-utrudnia-prowadzenie-przedsiebiorstwa-w-sposob-etyczny.

Kobylińska A., Folta M., *Sygnaliści – ludzie, którzy nie potrafią milczeć,* Warszawa 2015.

Lubiewski P., *Bezpieczeństwo państwa w ujęciu systemowym*, „Zeszyty Naukowe SGSP" 2020, No. 3.

Lubiewski P., *Krótka historia terroryzmu*, „Perspektivia. Legnickie Studia Teologiczno-Historyczne" 2018, No. 2(33).

Lubiewski P., *Systemowe ujęcie współdziałania w sferze bezpieczeństwa publicznego – szkic problemu*, „Zeszyty Naukowe SGSP" 2020, Vol. 75, No. 3

Nauki o bezpieczeństwie. Wybrane problemy badań, A. Czupryński, B. Wiśniewski, J. Zboina (eds), CNBOP, Józefów 2017.

Pietruszka A., *Ochrona sygnalistów (whistleblowers) w kontekście wolności wypowiedzi*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2020, Rok LXXXII, Zeszyt 1.

[16] *Association of Certified Examiners 2020 – Report to the Nations* na: https://www.acfe.com/report-to-the-nations/2020/ (dostęp: 12.09.2022 r.).

Price Waterhouse Cooper 2020 – Global Economic Crime Survey na: https://www.pwc.pl/pl/media/2020/2020-03-05-badanie-przestepczosci-gospodarczej-2020.html.

Projekt ustawy *o ochronie osób zgłaszających naruszenia prawa* na: https://www.legislacja.gov.pl/projekt/12352401 (dostęp: 12.06.2022 r.).

Rezolucja Parlamentu Europejskiego z dnia 24 października 2017 r. w sprawie uzasadnionych środków ochrony sygnalistów działających w interesie publicznym podczas ujawniania poufnych informacji posiadanych przez przedsiębiorstwa i organy publiczne (2016/2224(INI)) (Dz.U. UE. C-346 z dnia 27.09.2018 r.).

Stopczyńska K., *Rola kreowania wizerunku firmy w kreowaniu silnej pozycji rynkowej*, „Przedsiębiorczość i Zarządzanie" 2014, tom XV, zeszyt 5, część II.

Szymczykiewicz R., *Miejsce tzw. sygnalistów w polskim systemie prawnym,* Warszawa 2018.

Waszak M., *Strażnicy demokracji. Nowe perspektywy ochrony sygnalistów,* Warszawa 2020.

Wurm M., *Die Whistleblower-Richtlinie der EU: Was sind die Konsequenzen für Unternehmen?,* na: https://se-legal.de/die-whistleblower-richtlinie-der-eu-was-sind-die-konsequenzen-fur-unternehmen/

About the Authors

Alina Wołoch, combining his professional work with scientific activity, she tries to find innovative solutions to use the institution of a whistleblower to ensure the security of facilities and build a positive image of whistleblowers in society.

Věra Holubová, Ing., Ph.D., specialises in security of persons and property, protection of buildings and national security. Researcher and co-researcher of several security research projects and author of security related articles.

Bernardo Amorim, tudent at the Lusófona University of Porto. The representative of the International Scientific Society for Security "Save the Word" in Portugal.

Andrea Plauter, student at the Budapest Business School. The representative of the International Scientific Society for Security "Save the Word" in Hungary.