The Concept of a Subsystem to Support the Management of the Protection of Intangible Assets of Companies from a Behavioural Perspective

Paweł Kobis
Faculty of Management, Czestochowa University of Technology, Poland

pawel.kobis@pcz.pl

Abstract: The human factor is the biggest challenge for enterprises in providing the expected level of security, whereas the lack of educated personnel is one of the key problems in building an effective system for protection against data and information threats. A human being is a non-programmable element of the system and it is difficult to predict his or her behavior in information management processes and in the face of a specific event. Humans cannot be programmed like some security applications or hardware solutions with predictable performance. Human actions very often have a stochastic effect on the operation of the system. They can be ill-considered, haphazard, affected by emotions, and taken without due attention and adequate knowledge and experience (Pham et al., 2019). All these imperfections are exploited by those whose goal is to destroy or obtain information. According to data published by several information security companies, attacks carried out by purpose-built bots and web applications that exploit a technical factor (e.g., system vulnerabilities) are becoming increasingly rare, and are being replaced by attacks in which human interaction is a key factor. The curiosity and trust, leading well-meaning individuals to click, install, open, and send information, are being exploited by cybercriminals who are increasingly adept at using social engineering techniques. The aim of the present paper is to discuss the theoretical basis of information security issues from the behavioral perspective and to present the concept of a subsystem that implements measures to minimize the impact of the human factor on the emergence of threats to the intangible resources of a business entity. The concept is to create an information and organizational space to support the operation of the traditional information security management system in small and medium-sized enterprises. The concept is presented using the object-oriented approach which focuses on the functional elements of the system, and the subject-oriented approach, which takes into account the relationships between the various individuals who affect the security of the information system. The author's models of each approach were presented along with a description of how they work.

Keywords: Information management, Information security, Human factor, Data protection, Information security management system

1. Introduction

The concept of information security is strongly correlated with the information security management process and the established security policy (Kim and Han, 2018; Paananen et al., 2020). In the case of modern enterprises, this management occurs at the level of information systems, taking into account the security of data and computer devices themselves, software, and the security of the communication network connecting computer devices, where information is in the form of a string of bits. Information can be represented by a text, graphics, video, or a binary file in the form of a computer application. Analysis of information security in this aspect translates into an analysis of the security of the system in which the information is processed. A huge challenge for information systems today is also the excessive amount of data and information that needs to be analyzed (Jabir et al., 2022; Maroufkhani et al., 2020).

The security of digital information resources boils down to the development of a specific information security environment (Mirtsch et al., 2021; Nel and Drevin, 2019). The concept of information security is now very broad, and its dimension is proportional to the development of information systems. It should be approached as a parallel system that ensures effective and uninterrupted information management. The security system consists of certain components, with the most important including (Kobis, 2021):

- security devices;
- security software;
- procedures, regulations, ordinances, analyses, policies, etc. concerning the ways, requirements, and scope of information protection;
- humans.

The information security system represents a part of the IT system (its subsystem). It is inherent in this system and shares hardware and software resources.

2. Theoretical Background

Modern information security system considers people as the most risky element of the system (D'Arcy and Teh, 2019; Karjalainen et al., 2020). Employees of business entities are increasingly exposed to social engineering activities (Aldawood and Skinner, 2019; Salahdine and Kaabouch, 2019). It is easier for attackers to deceive people than a professionally designed security system (Al-Shanfari et al., 2020; Steinmetz et al., 2021).

How can we make the term "humans" more specific? For business organizations, we can classify human resources as employees, business partners, customers, and third parties (Figure 1). One can, of course, extend this classification, for example, to include positions held by employees, define types of business partners, etc. However, for the purpose of the present paper, the above-mentioned division was adopted. It defines specific groups of people who influence the management of intangible resources in an organization.

The employee is understood to mean any person who performs any information management activities for the benefit of an enterprise and is paid by that entity for such work. Therefore, we are talking about employees who work based on employment contracts, so-called "junk contracts," management contracts, self-employed, etc. Furthermore, the described meaning of the employee is also extended to CEOs, directors, owners, and system administrators.

The term 'business partner' defines any person or group of persons who cooperate with an enterprise on a mutual benefit basis. Therefore, these can be franchisees, all suppliers, and subcontractors.

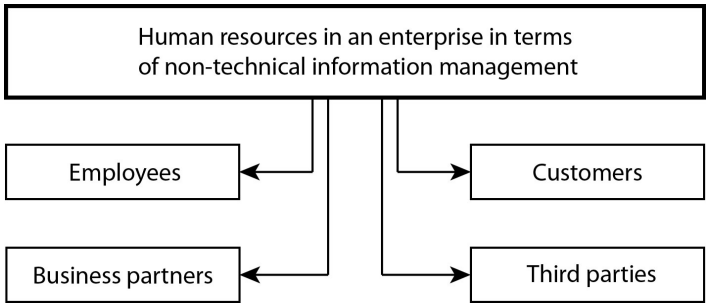

Figure 1: Human Resources in the Process of Non-Technical Information Management

Third parties that influence the management of information resources are: opinion-forming individuals that influence certain activities within the organization, and those seeking to acquire, either legally or illegally, information held by the enterprise. They can also be outsourcing entities (Benaroch, 2020; Feng et al., 2020).

The term customer refers to an entity that purchases a good to be consumed by them or for further distribution and acquires rights to its ownership. According to Encyclopedia of Management (Polish: Encyklopedia Zarządzania), customers are not only individuals but also legal entities and government entities that purchase goods and services offered on the market (Encyklopedia Zarządzania, 2023).

Analysis of human behavior in a business entity and in its closer and farther environments allows for outlining the relevant influences of the human factor on individuals, characterized by specific relationships (Figure 2). Security of information resources requires taking into consideration every person who more or less has or can have an impact on information management (Hadlington et al., 2020; Wiafe et al., 2020). This involves both positive aspects related to the experience of working with customers and business partners, and negative aspects, usually related to third parties classified as potential aggressors, employees of competing entities, individuals or groups of individuals who want to extort and destroy information or blackmail the enterprise while expecting potential profits from such acts (e.g., ransomware) (Kobis and Karyy, 2021; Masuch et al, 2021; Reshmi, 2021). Figure 2 shows feedback communications to third parties marked intentionally with a dashed line. This is because, on the level of information protection, these actions are usually defensive in nature. There is no full interaction with the potential aggressor. These are only specific responses, *ad hoc* actions, or those planned and predicted by prior risk analysis.

The various actors shown in Figure 2, despite the different scales of the human factor in both positive and negative aspects, cannot be easily classified as "good" or "bad." Anyone, whether a customer, business partner, third party, or employee, can, through certain intentional or accidental actions, contribute to both threatening and strengthening the structures of the information system. Hence, it is necessary to develop and

implement a systematic solution that, in addition to purely technical and software risks, will also take into account the behavior of humans who are the main element of the information system.

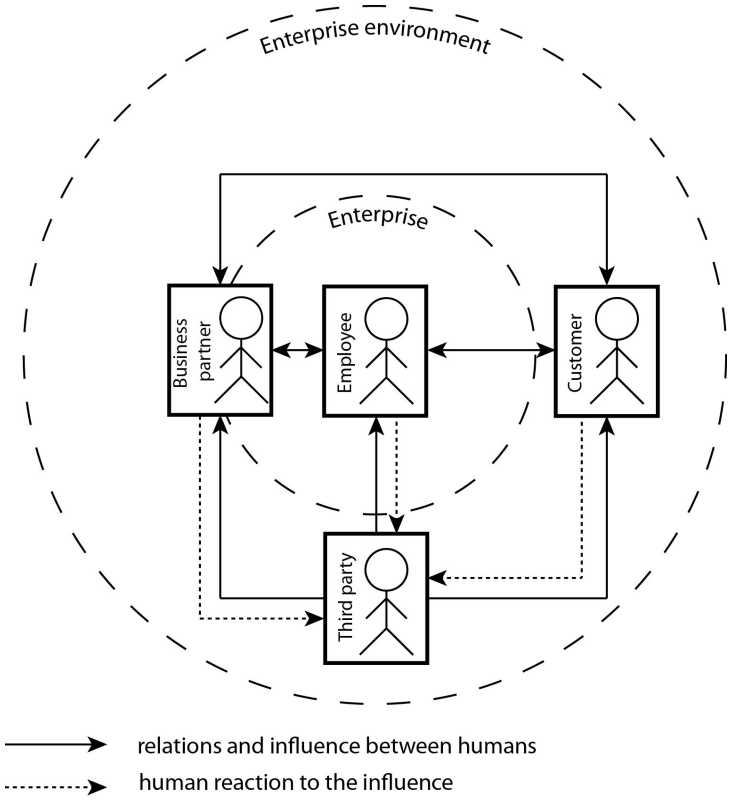

Figure 2: Possible Relationships and Influence of the Human Factor on Information Security Between Individuals

As can be seen in Figure 2, the employee is at the center of the human factor's influence. It is as much a symbol of rank-and-file employees who process certain information resources as of managers of any level, a security system administrator, an owner, or a CEO. These are the individuals with the greatest access to intangible resources, and in the event of a threat, these people are most often exposed to the potential influence of social engineering.

3. Concept of the Subsystem for the Management of Non-Technical Aspects of Information Security

3.1 General Assumptions

To counter information threats, in which humans are a key risk factor, it is necessary to develop the concept of a system solution. The solution should complement the existing information security management system (ISMS) in business entities as its subsystem. The subsystem should include all activities aimed at minimizing the risks associated with the occurrence of threats to information resources. It should include non-technical aspects of security directly related to humans. It should be positioned on the behavioral plane. The author named the system Subsystem for Management of Non-Technical Aspects of Information Security (MNTAIS subsystem). It is a proprietary solution addressing the impact of the human factor on information security. Therefore, the MNTAIS subsystem should be viewed as the implementation of activities and procedures to minimize the risk of threats caused by the human factor within the information security management system in enterprises. The MNTAIS subsystem is a supplement to the ISMS with elements concerning the impact of human beings and human groups on information security. The MNTAIS subsystem is intended to be an additional component of the ISMS, being its extension to include aspects of human impact on information security. It should be noted that modern ISMSs used in enterprises, to varying degrees, consider the human factor as a potential threat to intangible resources, tying it 'incidentally' to procedures, rules, and regulations for traditional security solutions. Thus, there is a lack of systemic solutions that would meet the assumptions of a coherent concept of information protection in an orderly manner. The subsystem presented below is a proposal to fill this gap.

3.2 Implementation and Operation at the Object-Oriented Level

At the object-oriented level, the Subsystem for Management of Non-Technical Aspects of Information Security (MNTAIS subsystem) can be defined as a set of hardware and software solutions that achieve the stated objectives of securing the information resources of a business entity against threats caused by the human factor. These solutions interfere with the information system in a certain way, minimizing the risk of an incident. Figure 3 shows a diagram of the relationship between the components of the MNTAIS subsystem and the components of the information system. The components can be characterized as follows:

- Enterprise Internal Network (EIN): a LAN computer network of a business entity, both physical (cable network) with a specific topology, and wireless, with a specific standard used for data and information exchange.
- Fixed and Cellular Telephony (FCT): all telephone communication systems used in the entity.
- Individual Information Processing Stations (IIPS): all workstations where information resources are processed. These include desktops, laptops, tablets, smartphones, and other devices that allow for processing.
- Collective Information Processing Stations (CIPS): all stations that support individual stations to a certain extent. These include file servers, database servers, application servers, email servers, and other systems with similar functions.

The above components form relationships with elements of the MNTAIS subsystem. Most relationships (except for reporting connections) are bidirectional, as there is a mutual exchange of signals, data, or information in each case. They are as follows:

- Software and hardware solutions for blocking specific services work in cooperation with three components: EIN, IIPS, and CIPS. In the case of EIN, data is collected on services being run in the internal network or computer devices being connected to the network. In the case of IIPS, data is collected on both local and cloud computing applications, and connected peripherals e.g., to USB ports (Universal Serial Bus). In CIPS, on the other hand, the component controls users' privileges of using specific resources, monitors their flow, and checks the external devices connected by employees.
- Detection of illegal actions by employees or third parties that attempt to illegally obtain information triggers a mechanism to block them immediately. This component can operate according to two scenarios, by either blocking predefined attempts or, using artificial intelligence mechanisms, making independent decisions to allow or block the service. Artificial intelligence can also be a complementary solution, similar to the way it works in some antivirus programs, which, using built-in intelligent mechanisms, recognize suspicious codes, even though officially the code is not in the signature database.

The component reports its activities in an automated reporting system.

- Remote access control systems work only with EIN by real-time monitoring connections between the global network and the LAN. They mostly concern remote workers, assigning them specific rights to access resources. At the same time, they block illegal attempts by third parties to connect to the network. It should be noted that these systems are not solutions designed to block malware and other threats automatically distributed by Internet bots. They are complementary to them and are intended to eliminate unwanted intentional or accidental human actions from the Internet. The operation of the component is reported.
- Automated control systems work with EIN, IIPS, and CIPS. They are primarily tasked with watching employees in terms of establishing proper safeguards for information resources. This includes monitoring the passwords for network devices, wireless networks, computing devices, local applications, cloud access, or monitoring users in terms of opening communication ports, etc. All human errors are reported. The reports include both the error identifier itself and detailed information about the person who made the error. Therefore, these systems make it possible to establish a base of training needs.
- Automated identification systems work with FCT and IIPS. These are the two components of the information system that allow communication with the enterprise. The systems identify the people who contact the enterprise. The operation of the component is reported to the extent permitted by law, especially under the provisions of the GDPR.

- Knowledge bases are connected only to IIPS, working simultaneously with online and artificial intelligence systems. This cooperation is expected to make it possible to search the database for information through the mechanisms of the network communicator, which is equipped with a search module. Artificial intelligence mechanisms, also equipped with instant messaging options, can be directly used by ISPI. Furthermore, artificial intelligence tools supported by a knowledge base can "suggest" specific solutions. This synergy allows employees to use a single tool when interacting with an information security supervisor, with an artificial intelligence messenger, and with a knowledge base. It also allows instant messengers to refer users to specific electronic documents during a conversation.
- Systems for controlled, targeted attacks that enable the identification of employee vulnerabilities work with all components of the information system. In the case of EIN and IIPS, they allow simulation that allows for the identification of gaps in the knowledge and experience of employees dealing with the enterprise's IT system. Indirectly, they also allow for checking the reliability of other components of the MNTAIS subsystem that provide security to EIN and IIPS.

In the case of IIPS and FCT, they are used to test the knowledge and experience of employees, especially in social engineering techniques. They allow for drawing a detailed map of training needs.

All elements, both in the information system and the MNTAIS subsystem, are monitored.

Implementation of the subsystem at the object-oriented level requires the following steps:

1. analysis of all elements of the information system;
2. adaptation of elements of the MNTAIS subsystem to the existing configuration of the ISMS system;
3. implementation of individual components.

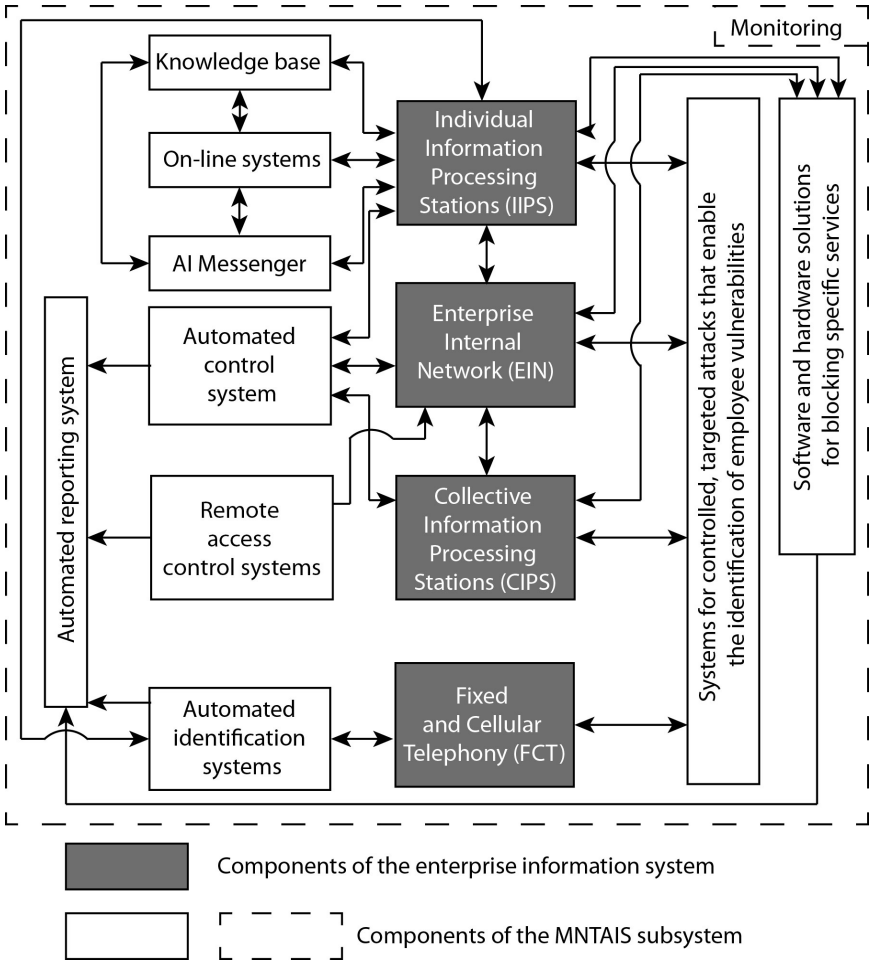

Figure 3: Components of the MNTAIS Subsystem and Relationships Between Components Of The Information System

The first step is used to determine all technical aspects of the existing system, including:

- configuration of devices in the local network;
- existing operating systems;
- existing computer software.

These aspects are necessary to adapt all elements of the MNTAIS subsystem so that data and information can be exchanged between components of the existing information system and those of the solution being implemented (Step 2). The systems for identification, control, and reporting, knowledge bases, and other parts listed in Figure 3 should function using the same communication protocols, encryption algorithms, file formats, and other technical parameters. This is the only way to achieve integrity of information.

Step three, which concerns the implementation process, should include two levels: technical implementation of the new solutions and familiarization of employees and system operators with the new functionalities. These two levels should correlate with each other. Although the individual components of the MNTAIS subsystem are autonomous (hence the order of implementation is not particularly important), their implementation without training may result in the overall deterioration of the operation of the information security system. Therefore, it is necessary to ensure systematic implementation. Each component should be implemented on two levels simultaneously, then the next one, and so on. This allows for regular learning of new solutions, thus fully utilizing the potential of the MNTAIS subsystem. In general, it is important to implement the MNTAIS subsystem into the information system in a comprehensive manner, as only by this method can a coherent and efficient information protection system be developed.

3.3 Implementation and Operation At The Subject-Oriented Level

At the subject-oriented level, the Subsystem for Management of Non-Technical Aspects of Information Security can be defined as a set of relationships between the intangible elements of the subsystem and the individuals who influence the security of the information system, and individuals pursuing the stated objectives of securing the information resources of the business entity against threats caused by the human factor.

A detailed diagram of the relationships is shown in Figure 4. The diagram presents two types of relationships: between individuals, marked by dashed lines, and between subsystem elements and individuals, marked by solid lines.

In the case of interpersonal relations, the following relationships can be defined for the prevention of threats to information resources:

- Between the person responsible for information security and other people. They are of the following nature:
    - with an employee: they concern broadly defined support for the security of processed information, analysis of the employee's actions in terms of compliance with regulations and rules of conduct;
    - with a customer: they concern the imposition of certain rules of conduct when the customer uses the enterprise system (e.g. when creating an account), the assignment of access rights to the information system, definition of customer service policies, and analysis of customer activities in the enterprise system;
    - with a business partner: they concern the imposition of certain rules of conduct when a business partner uses the enterprise system (e.g., when registering a reseller account), the assignment of access rights to the information system, the analysis of business partners' activities in the enterprise system;
    - with a third party: they concern the determination of the level of security against access to the information system, monitoring attempts to breach security, and phishing attempts using social engineering.
- Between the employee and other people, especially:
    - with a customer: they concern maintaining certain standards of customer service in terms of eliminating potential situations in which there may be a possibility of intentional or accidental disclosure of protected information and the ability to counteract social engineering;
    - with a business partner: they concern senior employees responsible for business relations. The scope of the relationships is analogous to that with customers;

- with a person responsible for information security: they concern the employee's reporting of irregularities and suspicious behavior of applications and the operating system during the performance of assigned activities;
- with a third party: they concern the ability to detect a situation in which a third party uses social engineering techniques to obtain information and the ability to counter them.

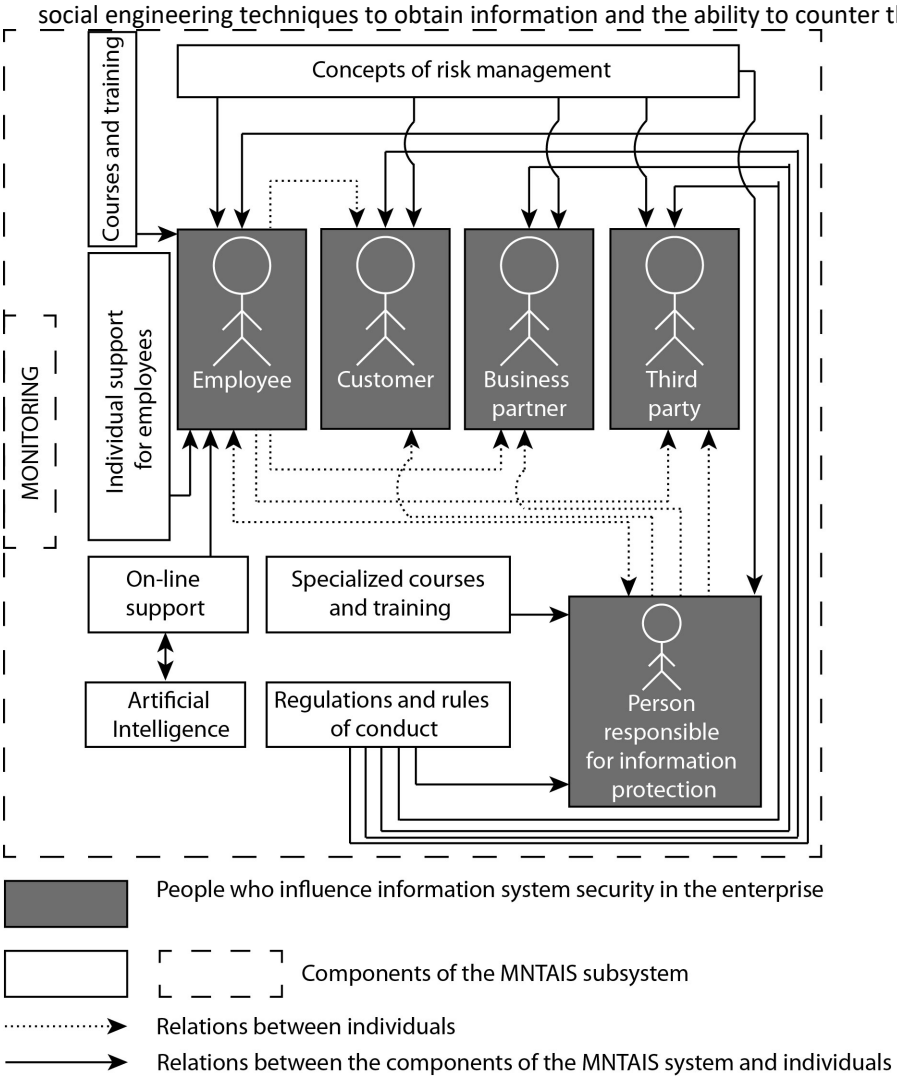

Figure 4: Relationships Between the Components of the MNTAIS Subsystem and Individuals who Influence the Security of the Enterprise Information System

Relationships between individuals in terms of the prevention of information risk are affected, among other things, by components of the MNTAIS subsystem. They influence individuals directly or indirectly. Direct actions are understood to mean performing certain actions in the presence of the person or communicating information or knowledge directly to them. Indirect actions include developing regulations, rules of conduct, and risk management concepts that apply to the person and should be followed by employees who have or may have any contact with such persons. In other words, these activities are aimed to create an area of security in dealing with these persons. Consequently, there are the following components with their respective impact as shown in Figure 4 based on the intangible components of the MNTAIS subsystem:

- Courses and training: organized periodically in the field of information security. Problems discussed can be determined by current issues presented in the literature or as a result of the operation of automated reporting systems (Figure 3). They are aimed at all employees with access to the enterprise's information resources.
- Specialized courses and training: held periodically for those involved in information security. In addition to issues directly related to the positions of these individuals, training can be extended to include human resource management in selected aspects needed to achieve the goal of adequate preparation of employees for secure information management.

- Risk management concepts: regular risk analyses and rules for dealing with risks related to the human factor, taking into account all persons who have access to information resources and those who pose a potential threat.
- Regulations and policies: these are communicated to information security officers and all employees only directly. In the case of customers or business partners, these components may affect them and be communicated both directly (e.g., through a web platform during account registration in the form of terms and conditions to be accepted) or may affect them indirectly by providing guidelines to the business entity's employees on how to contact them. In the case of third parties, there can be only indirect action.
- Individual support for employees: a component that relates to any activities aimed at providing direct support to an employee in a situation of danger or inability to cope with a given situation while processing information resources.
- Online support: a component that relates to any employee provided by an electronic communication system with an intra-organizational chat room using optional artificial intelligence solutions.

All these components are monitored. Monitoring means the supervision of the correct functioning of the subsystem, the proper execution of tasks by its various components and persons who are both part of and beneficiaries of the MNTAIS subsystem. This supervision can be the responsibility of information security professionals (in the specialized area) and managers, owners, directors, and CEOs (in the logistics area).

Subsystem implementation at the subject-oriented level is more difficult and time-consuming than that at the object-oriented level. This is primarily due to the fact that this level involves directly humans. The knowledge acquisition processes, the information contained in regulations, rules, and training are extended over time. Full implementation of the subsystem should not be expected after certain content and documents are presented to employees. Simply familiarizing with them is only the prerequisite for actually following and understanding them. The meaning of understanding refers to the employee's ability to link the acquired theory to the practice of processing information resources.

During the implementation of the subsystem, the individual predisposition of employees to acquire knowledge should also be taken into account. For example, a certain group of employees may understand certain phenomena after studying the prepared documentation and more quickly relate them to the practice, while another group, in order to understand, will have to relate them to daily work and to some extent learn from mistakes. This is inevitable and leads to an extended process of full implementation and comprehensive operation of the MNTAIS subsystem.

3.4 Comprehensive approach to the MNTAIS subsystem

The MNTAIS subsystem is intended to comprehensively encompass safeguards against all types of threats originating in human behavior. Aware of the pace of change in information management processes, the author proposed a subsystem where components can function independently. Therefore, the subsystem is an open solution to which further components (modules) can be added to protect against threats that may emerge in the following years. The only inseparable structure, according to the author, is the need for both planes to coexist (Figure 5). Only in this way, by combining human actions with tangible and intangible components that prevent the loss or destruction of information, can a comprehensive solution be achieved to minimize the risk of threat to intangible resources.

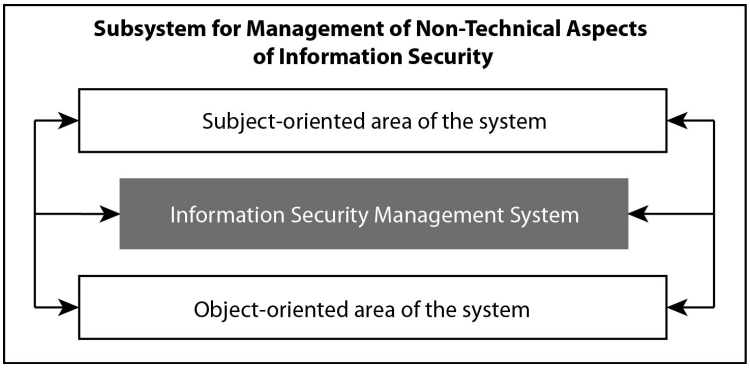

Figure 5: A Holistic View of the MNTAIS Subsystem Against the Background of the Relationships With The Information Security Management System

According to the author, very important and inseparable is the cooperation of the MNTAIS subsystem with the existing security system. This allows for the comprehensive elimination of potential incidents. Furthermore, the spectrum of modern threats is so broad that the various techniques of attacks and attempts to obtain information are beginning to intermingle. The resulting hybrid techniques can only be effectively combated through close cooperation between the MNTAIS subsystem and the ISMS.

4. Conclusion

The subsystem concept presented in this study is in line with contemporary solutions in the field of information resource protection. Its structure and operation use the mechanisms of the information security management system and are a kind of extension with components that take into account the human factor. This approach simplifies the management of the security system in the enterprise as it does not change the current state of affairs, and there is no need to build a parallel hardware and software infrastructure and structure for managing it. The synergy of these two systems allows for holistic risk management and considering potential events comprehensively: according to the existing rules of threat identification and classification, supplemented by factors related to the behavior of employees, customers, business partners, and third parties.

The visualization of the subject-oriented and object-oriented areas of the subsystem and its entirety is only a proposal. The subsystem, according to the author, is coherent and achieves the goal of minimizing risk in enterprises. It can also inspire further modernization of the subsystem or the development of a new solution.

References

Aldawood, H., and Skinner, G. (2019) "Reviewing Cyber Security Social Engineering Training and Awareness Programs - Pitfalls and Ongoing Issues", *Future Internet*, No. 11(3), 73.

Al-Shanfari, I., Mohamed, W., and Abdullah, R. (2020) "Identify of Factors Affecting Information Security Awareness and Weight Analysis Process", *International Journal of Engineering and Advanced Technology (IJEAT)*, Vol. 9, Issue 3, pp. 2249–8958.

Benaroch, M. (2020) *Cybersecurity Risk in IT Outsourcing—Challenges and Emerging Realities*, in: R. Hirschheim, A. Heinzl, and J. Dibbern (eds*.), Information Systems Outsourcing: The Era of Digital Transformation*, Springer International Publishing. pp. 313–334.

D'Arcy, J., and Teh, P.-L. (2019) "Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization", *Information & Management*, No. 56(7), p. 103151.

Encyklopedia Zarządzania (Encyclopedia of Management) (2023) *Meaning of the term 'customer'* [online], https://mfiles.pl/pl/index.php/Klient

Feng, N., Chen, Y., Feng, H., Li, D., and Li, M. (2020) "To outsource or not: The impact of information leakage risk on information security strategy", *Information & Management*, No. 57(5), p. 103215.

Hadlington, L., Binder, J., and Stanulewicz, N. (2020) "Fear of Missing Out Predicts Employee Information Security Awareness Above Personality Traits, Age, and Gender", *Cyberpsychology, Behavior, and Social Networking*, No. 23(7), pp. 459–464.

Jabir, B., Noureddine, F., and Rahmani, K. (2022) *Big Data Analytics Opportunities and Challenges for the Smart Enterprise* in: M. Elhoseny, X. Yuan, & S. Krit (eds.), *Distributed Sensing and Intelligent Systems*, Springer International Publishing, pp. 833–845.

Karjalainen, M., Siponen, M., and Sarker, S. (2020) "Toward a stage theory of the development of employees' information security behavior", *Computers & Security*, No. 93, p. 101782.

Kim, H. L., and Han, J. (2018) "Do employees in a "good" company comply better with information security policy? A corporate social responsibility perspective" *Information Technology & People*, No. 32(4), pp. 858–875.

Kobis, P. (2021) *Information security management in information systems os small and medium-sized enterprises taking into account the human factor*, Towarzystwo Naukowe Organizacji i Kierownictwa. Stowarzyszenie Wyższej Użyteczności „Dom Organizatora", Toruń, Poland.

Kobis, P., and Karyy, O. (2021) "Impact of the Human Factor on the Security of Information Resources of Enterprises During the Covid-19 Pandemic", *Polish Journal of Management Studies*, No. 24(2), pp. 210–227.

Maroufkhani, P., Tseng, M.-L., Iranmanesh, M., Ismail, W. K. W., and Khalid, H. (2020) "Big data analytics adoption: Determinants and performances among small to medium-sized enterprises", *International Journal of Information Management*, No. 54, p. 102190.

Masuch, K., Hengstler, S., Schulze, L., and Trang, S. (2021) "The Impact of Threat and Efficacy on Information Security Behavior: Applying an Extended Parallel Process Model to the Fear of Ransomware", Proceedings of the 54th Hawaii International Conference on System Sciences, [online], https://scholarspace.manoa.hawaii.edu/items/c71f0907-cb19-434e-855b-0e04e2dc5349

Mirtsch, M., Blind, K., Koch, C., and Dudek, G. (2021) "Information security management in ICT and non-ICT sector companies: A preventive innovation perspective", *Computers & Security*, No. 109, p. 102383.

Nel, F., and Drevin, L. (2019) “Key elements of an information security culture in organisations”, *Information & Computer Security*, No. 27(2), pp. 146–164.
Paananen, H., Lapke, M., and Siponen, M. (2020) “State of the art in information security policy development”, *Computers & Security*, No. 88, p. 101608.
Pham, H. C., Brennan, L., and Furnell, S. (2019) “Information security burnout: Identification of sources and mitigating factors from security demands and resources”, *Journal of Information Security and Applications*, No. 46, pp. 96–107.
Reshmi, T. R. (2021) “Information security breaches due to ransomware attacks - A systematic literature review”, *International Journal of Information Management Data Insights*, No. 1(2), p. 100013.
Salahdine, F., and Kaabouch, N. (2019) “Social Engineering Attacks: A Survey”, *Future Internet*, No. 11(4), Article 4.
Steinmetz, K. F., Pimentel, A., and Goe, W. R. (2021) “Performing social engineering: A qualitative study of information security deceptions”, *Computers in Human Behavior*, No. 124, p. 106930.
Wiafe, I., Koranteng, F. N., Wiafe, A., Obeng, E. N., and Yaokumah, W. (2020) “The role of norms in information security policy compliance”, *Information & Computer Security*, No. 28(5), pp. 743–761.