The Competence "Information Security" in human resources management - a key factor for competitiveness and digital transformation

Dimitrina STEFANOVA[1*] and Valentin VASILEV[2]

To cite this article:

Stefanova, D., Vasilev, V. (2024). The competence "Information security" in human resources management - a key factor for competitiveness and digital transformation efficiency. Romanian Journal of Economics, 58(1), pp. 5 - 17

***Abstract. Objective**: The challenges of the labor market related to the new qualities and competencies in Human Resources Management (HRM) are currently in exceptional dynamics. In relation to this, the subject of information security is an essential part in the transformation of society, business processes and the competitiveness of organizations. Proof of this is the widespread penetration of information technologies into all business processes, which placed the creation and use of information at the center of economic activity, the so-called information economy, in which information, in addition to being a product, is also a tool for carrying out the activity. **Method**: Through a comparative methodology, including a study of literature sources, identification of good practices and a comparative analysis of current studies, answers to key questions on the topic will be sought, aimed at identifying the challenges of the labor market related to the new qualities and competencies in HRM are currently in exceptional dynamism. **Results**: In relation to this, the topic of information security is an essential part in the transformation of society, business processes and the competitiveness of organizations, the expected results are related to the identification of key moments and characteristics of competences in the studied topic. This will be realized with the clear awareness that proof of the importance of the topic is the wide penetration of information technologies in all business processes, which has placed the creation and use of information at the center of economic activity, the so-called information economy, in which information, in addition to being a product, is also a tool for carrying out the activity. **Originality**: The scientific research and its expected results are innovative and applied in nature. This is linked to the understanding that the human factor is a cornerstone in the information security of the organization, especially in the context of the search for sustainability and competitiveness of national economies - under the sign of creativity, crisis and conflicts, which is related to increasing the opportunities for success of the initiatives (undertakings) and is related to effective development of human capital in the organization.*

***Keywords**: Competence "Information security"; Human resource management (HRM); Crises; Digital transformation; Transformations*

***JEL classification**: O30; O31; M10; H12*

[1] "South-West University "Neofit Rilski"; Blagoevgrad; Bulgaria; *Corresponding author: d.stefanova.swu@gmail.com

[2] "Higher School of Security and economics, Plovdiv, Bulgaria; valentin.vasilev@vusi.bg

1. Introduction

The challenges of the labor market related to the new qualities and competencies in Human Resources Management (HRM) are currently in exceptional dynamics. In relation to this, the subject of information security is an essential part in the transformation of society, business processes and the competitiveness of organizations. Proof of this is the widespread penetration of information technologies into all business processes, which placed the creation and use of information at the center of economic activity, the so-called information economy, in which information, in addition to being a product, is also a tool for carrying out the activity. This imposes new, high requirements for the knowledge, skills and qualifications possessed by both managers at all levels and the employees of the organizations whose identification is the key objective of the development.

According to sustainable conceptual thinking in the direction of information security, the need for information storage is growing as a result of an increase in data volume, its reach, and information technologies. On the one hand, this relates to how information has evolved in terms of quality and volume, becoming a very significant and priceless resource or object for business and society. On the other hand, commitment to organizational and administrative rules as well as the normative and legal criteria for the protection of personal data. All organizations and businesses today that perceive organizational information as a valuable asset and view it in the context of their competitive advantage must practice information security management. Information security is frequently equated with cyber security, a field that is quickly evolving on all fronts—technological, governmental, and programmatic. According to its human aspect, it relates to the transfer of knowledge, the development of competencies, and the learning of digital skills. By taking preventative measures to protect the organization's physical, financial, and human resources, reputation, and upholding confidence among clients and counterparties, etc., as well as compliance with regulatory requirements, etc., the support for the organization's mission and goals will be ensured. Information security, in this sense, is a system of interconnected components, and in its management role, critical knowledge, skills, and competencies are searched after and identified by every employee for the particular demands of the corporate organization. We believe that in this broad-spectrum and interdisciplinary activity, the application of GAP analysis for information security is a relevant tool. We note that GAP analysis or tool describes a process for identifying where there are gaps and what differences exist between the current situation of the organization and 'what it should be'.) The use of information technologies in all or most of an organization's business processes, the placement, creation, and use of information at the heart of economic activity, and a focus on the so-called information economy—where information is not only good but also a tool for carrying out activities—are initial requirements. The accepted GAP analysis approach calls for generating a set of questions, the answers to which will form the actual information security procedures and, in turn, describe the human factor's capabilities and the sustainability of the results.

2. Literature review

Scientific correctness obliges us to consider the leading concepts used in the article. Different researchers derive similar definitions of the concept of information security, expanding or narrowing their range and scope depending on the clarification of the related basic elements. Information security is usually understood as technical and within the purview of narrow specialists. Conceptual clarification that (Committee on National Security Systems (CNSS) Glossary, 2022). The Instruction offers a combination of an aggregated definition of information security and a clarification of the meaning of explaining its structural elements:

- **Information security.** The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.
- **Information security architect.** Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.
- **Information security continuous monitoring (ISCM).** Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Note: The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. See continuous monitoring and automated security monitoring.
- **Information security continuous monitoring (ISCM) process.** A process to:
  - Define an ISCM strategy;
  - Establish an ISCM program;
  - Implement an ISCM program;
  - Analyze data and Report findings;
  - Respond to findings; and
  - Review and Update the ISCM strategy and program.
- **Information security continuous monitoring (ISCM) program.** A program established to collect information in accordance with preestablished metrics, utilizing information readily available in part through implemented security controls.
- **Information security policy.** Aggregate of directives, regulations, and rules that prescribe how an organization manages, protects, and distributes information.
- **Information security program plan.** Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
- **Information security risk.** The risk to organizational operations. (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. See risk.
- **Information sensitivity level.** See security level.
- **Information sharing environment (ISE).** The people, projects, systems, and agencies that enable responsible information sharing across the national security enterprise, sharing information on terrorism, homeland security, and countering weapons of mass destruction. Note: ISE in its broader application enables those in a trusted partnership to share, discover, and access controlled information, and it promotes partnerships across federal, state, local, and tribal governments, the private sector, and internationally.

Information security is understood to be the protection of data and the supporting infrastructure from unintentional or intentional impacts of a natural or artificial nature. Information security refers to a condition of information that forbids the possibility of viewing, altering, or destroying information by people who do not have the authority to do so, as well as information leakage caused by accompanying electromagnetic radiation and interference, and the use of specialized devices for interception (destruction) during transmission between computer technology objects. Information security is a set of measures aimed at ensuring the confidentiality

and integrity of processed information, as well as the availability/accessibility of information to users" (Andress, 2014). Andress develops concepts of information security in the context of which he identifies it as a daily concern of organizations of all sizes and especially those that process different types of personal information, financial data, health data, educational data, or other types of data that are regulated by the laws of the country. He asserts that information security incidents are entwined with the circumstances of their impact, such as breaches of email message confidentiality or validity. Information security, in other words, is a vital aspect of modern business.

In the light of the "knowledge economy", the concept of information security undergoes its development and is the subject of research and definition in various interdisciplinary studies. Information security is defined as "a set of actions that protect information systems and the data stored therein (David & Solomon, 2018). In terms of organizational development and competitiveness, "information security is seen as part of risk management, specifically information risk management in the organization" (McDermott & Geer, 2001).

In a similar context, scientific developments have seen its definition as a set of "processes of information protection and minimization of the risk of already implemented vulnerability" (Venter & Eloff, 2003). Hence the conclusion that the processes of providing information security are directly dependent on risk management for the confidentiality, integrity and accessibility of information and knowledge in the form of innovation to ensure the sustainability of an organization and to create value for it and its customers.

ISO/IES 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005), with related terms and definitions, have been developed in comparable logic (ISO, 2023).

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system. Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

The information security management system becomes a strategic decision for an organization and the implementation of the information security management system is in line with the needs and objectives of the organization, the security requirements, the organizational processes used, the size and structure of the organization.

Ensuring information security is seen as part of risk management, in particular information risk management in the organization. Naturally, the focus of attention is on information protection processes and minimizing the risk of vulnerability. Information systems of organizations based on information technology and communications are a tool for creating and operating information assets that provide benefits and value formation for organizations by offering information services to internal users and implementing information services for external users. This is an indicator that indicates that creating conditions for the implementation and management of information systems and for offering and maintaining security of information in them is vital for organizations. The ability to ensure quality, efficiency and effectiveness of information security depends on the quality of information services, which leads to an increase in the degree of satisfaction and trust of users, allows achieving a high level of competitiveness and ensures the fulfillment of business objectives.

Semerdzhiev and Mitev propose a framework that suggests that the maintenance of information security is such a state of the organization in which it is ensured, maintained, and guaranteed: (a) continuity of work processes; (b) minimization of risks to the organization; (c) maximizing return on investment; (d) increasing the opportunities for the success of initiatives (endeavors) and success depends heavily on the entire human resource of the organization (Semerdzhiev and Mitev, 2023).

From the above, we can summarize that information security is associated with protecting the confidentiality, integrity and availability of information assets, whether they are in the process

of being created, stored, processed or transmitted. It is achieved through the implementation of policy, education, training, communication, auditing, technology and is a vital component for the era in which data refers to countless individuals and organizations that are stored in various computer systems, often not under our direct control. At the same time, information security is a complex process that combines risk management, assessment and use of management mechanisms, policies, procedures, guidelines, good practices, experience and organizational structures that can be of an administrative, technical, managerial or legal nature to ensure and ensure the security of information. These processes apply to organizations in which the production, preservation, processing, sale and use of information are the main activity and, especially in its highest form, knowledge, but also to organizations that are not strictly specialized. Thus, in the case of an organization that does not take the time to properly put itself on a good footing in terms of information security, the consequences can be serious in terms of reputational impact, fines, lawsuits, or even the inability to continue conducting business if critical data is irretrievably lost.

3. Methodology and data

In connection with the main purpose of the research material, we will present secondary data that draw attention to proving the hypothesis, namely that information security can provide a competitive advantage to the organization.

Detailed and insightful report ENISA Threat Landscape (ETL) (ENISA, 2022) identifies the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis. It also describes relevant mitigation measures. This year's work has again been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL). During the reporting period of the ETL 2022, the prime threats identified include:

1. Ransomware
2. Malware
3. Social Engineering threats
4. Threats against data
5. Threats against availability: Denial of Service
6. Threats against availability: Internet threats
7. Disinformation – misinformation
8. Supply-chain attacks

We are particularly interested in conclusions and findings related to Social Engineering. „Social engineering encompasses a broad range of activities that attempt to exploit human error or human behaviour with the objective of gaining access to information or services. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information. In cybersecurity, social engineering lures users into opening documents, files or emails, visiting websites or granting unauthorized persons access to systems or services. And although these tricks can abuse technology, they always rely on a human element to be successful. This threat canvas consists mainly of the following vectors: phishing, spearphishing, whaling, smishing, vishing, business e-mail compromise (BEC), fraud, impersonation and counterfeit, which are analyzed in the relevant chapter" (ENISA, 2022).

Social engineering and especially phishing remain a popular technique for attackers to conduct their malicious activities. According to the Verizon Data Breach Investigations Report (DBIR) about 82% of breaches involve a human element and no less than 60% of the breaches in Europe, the Middle East and Africa include a social engineering component. The underlying reason for the criminals' interest in social engineering is obvious. Email is where their potential victims are easiest reachable. And despite awareness raising campaigns and exercises, users still fall for these tricks. Also, according to the DBIR, attackers continue to use stolen credentials to obtain

more details on a target via company emails. Their final goal is then to use this information to craft realistic pretexts, for example as part of BEC attacks (ENISA, 2022).

This reinforces the view that for an organization, an accidental or intentional act or incident of information loss and damage can seriously degrade its business processes. Information, together with the supporting systems, networks, and procedures, is crucial to the success of any organization. Information security must be defined, assessed, attained, maintained, and improved if an organization is to become more competitive, financially successful, legally compliant, and maintain a positive reputation. Their information systems and networks are exposed to security threats from a wide range of sources, such as management and employee noncompliance with established information protection policies, rules, and procedures; improper or careless staff use; computer fraud; espionage; sabotage; vandalism; fire; flood; or other disasters, accidents, and catastrophes. Information security is becoming more crucial in this setting for the protection of vital management information infrastructures as well as the public and commercial sectors of the economy. Many information systems are not built with security in mind. The degree of security that can be obtained by technical methods is constrained, and it must be preserved through proper management and set protocols for the application of information processes. Careful planning and attention to detail are necessary when deciding which controls to utilize. All company personnel must participate in information security management at a minimum, but it may also involve shareholders, suppliers, third parties, customers, or external organizations (Semerdzhiev and Mitev, 2023).

The Foundation - Human Factors and Its Impact on Information Security - focuses on examining employee digital skills, which are the cornerstone of how we communicate, carry out modern work, and implement information protection policies.

Digital transformation is on the rise and affecting every aspect of life. Digital skills are important because they underpin how we interact and how modern work is conducted. For many modern professions, digital skills are simply essential life skills. The digital skills required in the workplace are more advanced, and companies and institutions – public and private - expect most of their employees to have them. As dependence on the internet and digital technology increases, the workforce must keep up with the evolving skill demand. Without a firm command of digital skills, there is no way to propel innovation and remain competitive. The same applies to the public that will need digital skills in the day-to-day professional or personal context. Today, 54% of Europeans have at least basic digital skills 26 percentage points below the target with stark differences among countries. Some Member States like the Netherlands and Finland approach the target with 79% of people with at least basic digital skills in 2021. In eight Member States, the share of individuals with at least basic digital skills is lower than 50%. Romania, Bulgaria, Poland and Italy rank the lowest (Digital Economy and Society Index (DESI), 2022).

In this environment, knowledgeable employees and the digital shift are essential for conducting a company. This focuses attention on enhancing the workforce's qualifications and retraining to deal with digital data, so that it meets the needs of business in contemporary settings, primarily in the "hands" of the businesses themselves. The necessity for people to learn how to seek, analyze, synthesize, evaluate, store, and preserve information in a digital world is evident as a result. According to researcher Ala-Mutka, being "competent" involves having the necessary knowledge and abilities to carry out a task successfully, which in a digital environment refers to the capacity to use digital technology (Ala-Mutka, 2011).

The assessment of digital competence identifies the level of proficiency while taking into account the strengths and weaknesses of each employee or target audience. Management can evaluate training needs and orientations by objectively assessing the level of digital competence in order to understand where and what gaps need to be filled in order to achieve their personal or professional goals. The assessment method supports both the overall evaluation of the success of the performed trainings, internal connections and communications, and the consequences on an organization through repeatability over a certain period of time. These abilities involve processing a lot of information, thinking accurately and logically, and improving communication skills. HRM contributes hugely during crises and uncertainties because of the several roles it plays in relations

with people and work management in tandem with organizational strategic decisions (Gigauri, 2020).

We conclude that the individual and his digital competence play a crucial role in the organization's expectations for information security as well as improving his knowledge of and understanding of the problems presented by digital technologies.

The other increasingly important component of information security is the availability of qualified employees to work with information and data. Don't forget that managers in the organization must be more qualified in today's digital world, and they must also place more demands on the level and depth of education of their staff.

When viewed from an organizational perspective, the key elements for ensuring information security are primarily connected to the balanced participation, management, training, communication, and strengthening of human resources by establishing the organizational culture and commitment to ensuring information security at all levels of management. Such management requires managers who have high morals, values and patterns of behavior, consistent with the stated values of the organization, who understand the significant effect of improving management and who work to improve the human resources system to achieve better results (Icheva and Vasilev, 2021).

Other authors come to similar conclusions by summarizing that information security was defined as the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. The careful implementation of information security controls is vital to protecting an organization's information assets as well as its reputation, legal position, personnel, and other tangible or intangible assets. An organization's inability to select and implement appropriate security rules and procedures is likely to have a negative impact on the mission of the organization. However, well-chosen security rules and procedures that are put in place to protect important assets support the overall organizational mission. In today's environment of malicious code, system breaches, and insider threats, publicized security issues can have dire consequences, especially to profitability and to the reputation of the organization**.** Private and public-sector organizations improve both profit and service to customers when appropriate security protections are in place. Information security, therefore, is a means to an end and not an end in itself (Nieles et al., 2017).

It can be seen that the risks and threats related to the information assets of the organization are by no means small in terms of scope, distribution, and seriousness of the damage. In the crisis management and PR literature, cyber-terrorism, information, and reputational crises are separated into the portfolio of crises in separate categories. The so-called "new forms" (Chuturkova, 2012) of the crisis, such as cyber-terrorism, is associated with identity theft through the Internet - usernames, passwords, bank accounts, addresses, e-mails, violation of copyright and related rights, production, possession and distribution of pornographic materials with minors, preaching or inciting discrimination, violence, hatred based on race, nationality or ethnicity, etc., infrastructure failures, disinformation and fake news, etc. .n., which are also on the organizational agenda. Some leading authors will take advantage of this consensual vacuum to define Corporate Social Responsibility as the voluntary self-regulation of a company's business practices to minimize the negative impact, in the present and in the future, on society and human beings and also to maximize the positive potential on the environment, local communities, employees and other categories of stakeholders (Panait, Ionescu, Radulescu & Rjoub, 2022).

Organizations by themselves would barely be able to handle these crisis events. Such crises are not confined to a particular area of the organization's internal or external environment; rather, they spread from one area to another, exposing issues whose recombination can result in excessive dangers. They are also not framed in a specific time frame and appear to have an inherent vulnerability that manifests, disappears, mutates, and then strikes the system once more. The scope of these crises is considerably greater, and as a result of the loss of financial resources, the number of people impacted, and the repercussions, the legitimacy of the institutions is completely attacked,

eroding their competence and confidence in effective management (Vasilev, Stefanova and Cherkezov, 2019).

Understanding the organization's mission and how each system contributes to that mission is crucial in such a situation. According to this reasoning, information security needs to be a fundamental component of sound leadership and organizational structure. Management is in charge of calculating the acceptable risk level for a specific system and the company as a whole while taking security expenses into account. Finding the best balance between safeguarding the data or system and making efficient use of the resources is the objective because information security risk cannot be entirely avoided.

Information, financial assets, physical assets, and personnel must all be protected by systems and related processes, while also taking resource availability into consideration.

Other authors also come to similar conclusions, summarily defining "information security as a multidisciplinary field that combines professional activity engaged in the development and implementation of mechanisms to ensure information security in all possible ways (Cherdantseva & Hilton, 2013).

Perceived as an interdisciplinary field and in terms of its content workload, information security management will require the involvement of management, the specialized information security unit, all employees in the organization, but may include shareholders, suppliers, third parties, customers, or external organizations.

The applied secondary data and deductive reflections on the information security management system point us to confirming the idea of applying information security as a key competence to achieve competitiveness. On the one hand, because competitiveness is a relative characteristic reflecting the differences of the organization compared to others that give it an advantage. The factors determining the competitiveness of the organization in the field of information security are: organizational, technical, regulatory, economic and, on the other hand, by ensuring information security, it is possible to avoid or reduce risks, to ensure information superiority, to effectively exploit information assets and, ultimately, to achieve a competitive advantage.

All this is relevant to the knowledge economy, where information becomes the greatest value, strategic resource and the main productive force that creates value, while at the same time it is a product, as well as a service, the main source of income and profits for modern organizations.

The research placed in this course becomes a topic of an interdisciplinary nature and requires a relevant tool to assess the value, confidentiality, integrity, availability, possession or control, authenticity and usefulness of information, as well as the concepts of risk to determine the types of competences for different employees and modes of control - physical, logical and administrative. This, in turn, is the requirements for human resource management to determine the parameters of the necessary competence for information security on a wider scale, related to all employees of the organization. It can be said that the competitive advantage in the field of information security is a process of knowledge management in the organization, involving the purposeful establishment, development, creation, maintenance, and updating of capabilities and resources.

As a result, there are new, high standards for the knowledge, skills, and certifications held by both managers at all levels and employees of firms whose identity can be reduced to the particular organization.

When viewed from this angle, research takes on an interdisciplinary character and necessitates the use of an appropriate tool to evaluate the worth, confidentiality, integrity, availability, possession or control, authenticity, and usefulness of information, as well as the concepts of risk, toto identify the different employee skill sets and the various physical, logical, and administrative control methods. Information management systems can be assessed about their current state and their ideal state using the GAP analysis technique that has been established. In order to perform a GAP analysis, a list of questions about strengths and weaknesses must be compiled. The answers to these questions will help to clarify the actual information security

processes and, in turn, will outline the human factor competencies necessary to ensure the long-term success of each particular organization's results. By comparing the existing condition to the desired state with important audiences, the tool, in particular, clarifies the significance of information security for a business.

The organization uses GAP analysis to plan its upcoming actions. It involves outlining the future state (of the business, the product, the process, etc.), assessing the present state, and figuring out how to get from the present condition to the future one. It is used in many different processes, including operational management and strategic management of established or new organizations (Gurova and Tsolova, 2015).

By exposing them, it goes beyond the advantages and disadvantages of the digital sphere. The success of the business (such as turnover and profit development), the use of technology, the degree of importance of information (such as how developed IT infrastructure and information security programs) as well as company culture (such as the use of online communication opportunities and risks) will all be assessed in many areas of the analysis, in addition to the specific assessment. A common method of strategic control is GAP analysis. The fundamental concept is based on a goal-performance assessment where intended values for a given quantity, such as revenue, sales, profit, process results (innovation, diffusion, level of security), or strategic goals (competitiveness, internal values, infrastructure), are contrasted with actual conditions. This allows for the recognition of differences between the strategic goals and the actual status of the respective operational performance. The process provides a strong foundation for identifying potential reasons for deviations as well as a place to begin for operational and strategic initiatives to close the gaps that have been found.

In the context of information security, GAP analysis evaluates the present degree of compliance with the intended to identify and rank the organization's most important work areas. Companies can use this to analyze the stability of compliance with standards, identify high-risk and weak parts of the information management processes, and reduce risks that could have unfavorable effects. The GAP analysis is a large-scale project that begins with the so-called "inventory" of information security procedures, within which all information movement activities and their real extent are recognized, including the company's relationships with customers, workers, contractors, and many other parties. executing video surveillance operations, among many other things. The organization under analysis should ensure that all internal units participate to meet the project's objectives. The team that implements the study is crucial; it needs to include experts from many fields at various stages, as well as senior management, HR, IT, the sales department, marketing, public relations, supply, and logistics department representatives. The completed GAP analysis offers a structured picture of the primary information management processes while also taking risks into account. It also includes recommendations for particular actions to be taken to bring about or achieve compliance with the regulations and organizational standards. The qualifications needed for each level of employee competency will be based on the breadth of the positions and tasks. The level of qualification arranges employees in a hierarchical sequence, expressed in a qualification group and purposeful work with it.

4. Results and conclusions

Organizational growth is greatly accelerated by digital transformation, hybrid crises, and impacts, but they also provide significant problems. Information security has grown to be a top concern for enterprises as a result of the rising emphasis on digitization. This is not a coincidence, as the vulnerability to cyber assaults grows significantly with the adoption of new technology and the relocation of crucial business operations online. The human factor is the risk factor in an information security breach. The truth is that inside assistance is nearly always used in the largest system breaches, whether they involve banks or governmental organizations like the US Department of State. Even unconsciously. In addition to the above research and numerous others,

it was discovered that legitimate authorized users who lack competence for the tasks they undertake pose the biggest threat to the accuracy and integrity of the information. Information that is crucial to the business may be lost, modified, or destroyed as a result of their mistakes and omissions. Crisis management in the modern organization is undoubtedly in a new situation (Vasilev, 2021). Users that commit violations through unintentional mistakes in their routine job do so for no particular reason or objective. The security risks in the installed application programs and system software that have been identified in this group are what cause unintentional errors. It is important to remember that intentional human behavior includes threats of deliberate harm from inside or outside the business, whether they are current or former employees with malicious intent. Factors such as: human resources management; labor market pressures, equality and social justice and accountability; demographic factors; the increased need for decentralization; the role of social responsibility; social entrepreneurship; the role of information and smart technologies in management, crises, fake news and others, were presented in new aspects to business and public executives (Vasilev and Stefanova, 2021).

It is clear that establishing the limits in the field of information security is a more challenging issue. To minimize risks to organizational operations, including mission, functions, image, reputation, organizational assets, individuals, and other organizations from potentially unauthorized access, use, disclosure, disruption, alteration, or destruction of information and/or information systems, a narrow definition of information security is being developed (at the level of department and organization). Every organization's goal is to establish competence across its whole human resource by integrating the organization's structure with its ingrained principles of business operation. Competence is defined in this context as a certain set of digital knowledge, abilities, and experience, along with critical thought and information perception, that enables the company to raise its value. Competitors cannot readily copy or make up for competencies because they are an integrated system of values, and uncommon operational capabilities. The creation of a model of information security as a critical competence for business, which reflects the general perception and understanding of the reality in this sphere, the events taking place in it, processes, events, and views on interests, threats, and the need to take specific actions, is one possible approach that is discussed in the present study as a potential approach for its resolution. Information and communication security context-competence. It is essential to update, change, and prepare some internal documents so that they may be implemented with the rest of the business operations and foster a culture that conforms to the criteria for information security, documentation, and reporting. Three major sets of interconnected activities - technical, people-centered, and organizational - are involved in ensuring information security. The role of human resource management also is increasingly important (Stoykov and Vasilev, 2021).

It is a threat and a weak link to information security that the human aspect is frequently overlooked and undervalued. The human subject concurrently serves as a producer, carrier, distributor, and information security guardian. Protection against unintentional or intentional damage or information loss requires policies, training, motivation, familiarity with technology, and communication. When viewed in the context of controlling people's behavior and getting access to specialized information for a particular system, social engineering can be eliminated. Studying the interactions between man and information systems based on the foundation of computer and communication technologies constitutes one part of the human factor in the creation, use, and management of information systems and data. Although implicitly included, the competency of "information security" extends beyond the bounds of digital competence. In the context of information protection, the human factor – a generic definition of human activity – is seen as an active and deliberate effort on issues related to the security and dependability of information systems. On the other hand, today’s complex societal challenges call for a government of bridgebuilders. These bridgebuilders transcend boundaries, partner across sectors, and solve problems (Eggers and Kettl, 2023).

To ensure the development of competence in "Information security," it is important to identify key factors such as management, training, and strengthening of human resources, effective

internal communication, reputation and values in a system of business processes and culture, and clarifying and communicating with a purpose for sustainability. Modern organizations of science, education, and qualifications in the security system are becoming more and more dependent on knowledge because they have to become "knowledge factories" and their basic product has predominantly become ideas rather than tangible products (Stoykov, 2018). On the other hand, It is more than the aggregation of individual needs with deliberation as to what constitutes public value at its core (Bojang, 2021).

5. Conclusions

The article's research mentions a badly designed collaboration paradigm. There has been an attempt to highlight some of the basic changes brought on by digitalization. This viewpoint leads to the conclusion that the human factor is a key component of the organization's information security, particularly in the context of the search for national economies' sustainability and competitiveness - under the sign of innovation, crises, and conflicts. The globalization of information also causes the effects of "information crises" to become more globalized, opening up possibilities for a step change in the repercussions' degree of action to reach strategic proportions. This establishes a characteristic reliance and transforms the contemporary information security environment into a tool for achieving strategic objectives. Information security is powerful and important; thus, it demands a reasonable, logical, and practical systems approach with people, people management, organizational structures, training, communication, reputation, and values at its core (Turell, 2017). Every employee is responsible for maintaining security, not just management and designated specialized units. This turns the modern information security environment into a means to achieve strategic goals and defines a characteristic dependency. The power and importance of information security require a reasonable, rational, and practical application of a systems approach, with a central element of people, people management, organizational structures, training, communication, reputation, and values. Security is not only a commitment of management and authorized specialized units, but it is also a commitment of every employee. Therefore, an efficient framework should be created to protect the data contained in information systems or networks, as well as their capacity to ensure the confidentiality, integrity, and accessibility of that data, as well as other capabilities, such as ensuring the information's authenticity, accountability, and dependability. Both CSR and Sustainability address the responsible and sustainable use of resources while considering social, ecological, and economic dimensions of business practice. To increase sustainability and satisfy the demand for energy, countries should develop and utilize renewable resources as well as efficiently use energy sources (Gigauri and Vasilev, 2022).

In summary, scientific research places the concept that the human component is a foundation in the information security of the company and follows the logic of applied nature. Under the covers of creativity, crisis, and conflict, the search for sustainability and competitiveness of national economies is related to enhancing the chances for undertakings (initiatives) to succeed as well as to the efficient development of human capital within the organization. The identification of the crucial elements for ensuring the development of "Information Security" competence, which are primarily connected to balanced participation, management, training, and strengthening of human resources, effective internal communication, reputation, and values, expresses the innovative element and originality of the article. The idea of cooperation across organizational boundaries offers solutions for support, communication, shared organizational design, and knowledge sharing on the one hand, and solutions for cooperation with an information security focus on the other. Communication and knowledge exchange are important components of a workable vision for the sector. "Human" maturity and digital maturity go hand in hand. Risk management will directly affect how environmental, social, and governance (ESG) initiatives are developed, making ESG a top business concern. And while creating the strategy is challenging due

to the numerous elements that must be taken into account, implementing ESG in enterprises is even more challenging. Particularly when the perception of ESG aim is not thought to influence the outcomes. The common denominator for everything is the search and discovery of business models that create a culture of cooperation, support and development of the information economy. The following years are years of change, uncertainty and search for new and innovative solutions in all areas of individual and organizational everyday life (Vasilev & Ognyanski, 2020).

The present study does not pretend to be exhaustive in clarifying the possibilities in the direction of information security-sustainability. The scientific and practical discussion is presented in the broad plane from current to desired state, based on the balanced interweaving, participation and understanding of information technology, human resource, internal communication, reputation and values for knowledge economy and ESG.

References

Ala-Mutka, K. (2011). Mapping Digital Competence: Toward a conceptual understanding. Joint Research Centre - Institute for Prospective Technological Studies. Luxembourg: Publications Office of the European Union

Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. — Syngress, ISBN 9780128008126)

Bojang, M. B. (2021). Public Value Management: An Emerging Paradigm in Public Administration. International Journal of Business, Management and Economics, 2(4), 225 - 238. https://doi.org/10.47747/ijbme.v2i4.395

Cherdantseva, Y., & Hilton, J. (2013). Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. Organizational, Legal, and Technological Dimensions of Information System Administrator

Chuturkova, M. (2012). Krizisen PR, Sofia

Committee on National Security Systems (CNSS) Glossary, CNSSI 4009, Protected Distribution Systems March 2, 2022; https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf)

David, K., & Solomon, M. (2018). Fundamentals of Information Systems Security. Jones & Bartlett Learning

Digital Economy and Society Index (DESI) (2022) Human Capital, https://digital-strategy.ec.europa.eu/bg/policies/desi-human-capital)

Eggers, W.; D.F. Kettl (2023). Bridgebuilders: How Government Can Transcend Boundaries to Solve Big Problems; Harvard Business Review Press

ENISA (2022). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Gigauri, I., Vasilev, V. (2022). Corporate Social Responsibility in the Energy Sector: Towards Sustainability. In: Khan, S.A.R., Panait, M., Puime Guillen, F., Raimi, L. (eds); Energy Transition. Industrial Ecology. Springer, Singapore. https://doi.org/10.1007/978-981-19-3540-4_10

Gigauri, I. (2020). Organizational Support to HRM in Times of the COVID-19 Pandemic Crisis. European Journal of Marketing and Economics, 4(1), 16–30. https://doi.org/10.26417/492dnl43d

Gurova, E.; S. Tsolova (2015). Strategy of the organization of knowledge, Sofia

Icheva, M., V. Vasilev (2021). The time for the next steps is here – from classic to modern paradigms in motivation; International Journal of Social Science & Economic Research /IJSSER/; vol. 6, no. 3; https://ijsser.org/more2021.php?id=58

ISO (2023), https://www.iso.org/obp/ui#iso:std:iso-iec:27000:ed-5:v1:en

McDermott, B., & Geer, D. (2001). Information security is information risk management. Workshop on New Security Paradigms, 97 - 104.

Nieles, M., Dempsey, K. and Pillitteri, V. Y. (2017), An Introduction to Information Security, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-12r1

Panait, M., Ionescu, R., Radulescu, I. G., & Rjoub, H. (2022). The Corporate Social Responsibility on Capital Market: Myth or Reality?. In I. Management Association (Ed.), Research Anthology on Developing Socially Responsible Businesses (pp. 1721-1754). IGI Global. https://doi.org/10.4018/978-1-6684-5590-6.ch085

Semerdzhiev, Tsv., Mitev, N. (2023). Norms and standards for management of information systems and protection of information, Sofia

Stoykov, S.; Vasilev, V. (2021). Prerequisites for efficiency of human resources management in crisis situations (from classic theories to a new vision). Politics & Security, 5(3), 15–21. https://doi.org/10.5281/zenodo.6402953

Stoykov, S. (2018). Scientific Knowledge – Source of a Competitive Advantage in Security," 2018 International Conference on High Technology for Sustainable Development (HiTech), Sofia, Bulgaria, pp. 1-3, doi: 10.1109/HiTech.2018.8566548

Turell, A. (2017). Applying Public Value Management Theory to Procurement. CIPS Knowledge download that displays a CIPS CPD icon. Policy paper

Vasilev, V., D. Stefanova (2021) Complex communication barriers in the organisitaions in a crisis context; KNOWLEDGE International Journal; Vol. 49.; №1; Institute of Knowledge Management; Skopje; ISSN:1857-923X (Printed); ISSN:2545-4439 (Online); p. 29-33; https://ikm.mk/ojs/index.php/kij/article/view/4617

Vasilev, V., D. Stefanova, V. Cherkezov(2019). Crisis management. Propeller, Sofia

Vasilev, V. (2020). From a crisis of confidence to effective crisis management in the public administration. KNOWLEDGE - International Journal, 43(1), 229–232. Retrieved from https://ikm.mk/ojs/index.php/kij/article/view/371

Vasilev, V., & Ognyanski, D. (2020). The new face of public management – about the "smart city" and its impact on the future development of society. KNOWLEDGE - International Journal, 42(1), 91–93. Retrieved from https://ikm.mk/ojs/index.php/kij/article/view/540

Venter, H., & Eloff, J. (2003). A taxonomy for information security technologies. Computers & Security, 299-307.