Research and Science Today
WWW.RSTJOURNAL.COM

DOI: 10.38173/RST.2022.24.2.4:49-70

Title:	*SECURITY AND DIGITAL TRANSFORMATION IN ROMANIA- SECURITY STRATEGIES IN PRIVATE ORGANIZATIONS IN THE ERA OF DIGITAL TRANSFORMATION*
Author:	Larisa-Geanina BORCA

Section: International Relations

Issue: 2(24)/2022

Received: 29 August 2022	**Revised:** 16 September 2022
Accepted: 9 November 2022	**Available Online:** 15 November 2022

Paper available online HERE

RST Research and Science Today
WWW.RSTJOURNAL.COM
AUTUMN 2022
No. 2(24)/2022
ISSN-P: 2247-4455 / ISSN-E: 2285-9632

International Relations

SECURITY AND DIGITAL TRANSFORMATION IN ROMANIA: SECURITY STRATEGIES IN PRIVATE ORGANIZATIONS IN THE ERA OF DIGITAL TRANSFORMATION

Larisa-Geanina BORCA[1]

ABSTRACT:
IN THE CURRENT CONTEXT, THE IMPACT OF THE CRISIS CAUSED BY THE NEW CORONAVIRUS HAS PROMPTED ORGANIZATIONS TO RETHINK HOW THEY NEED TO WORK WITH CUSTOMERS AND EMPLOYEES, ACCELERATING THE DIGITIZATION OF ACTIVITIES IN THE FORM OF IMPROVED CONNECTIVITY, ADOPTING ONLINE BUSINESS MODELS, IMPLEMENTING NEW DIGITAL SECURITY STRATEGIES, CHANGING THE CYBERSECURITY CULTURE, PROMOTING ONLINE PAYMENTS, INCLUDING IMPROVING DIGITAL SKILLS TO SOME EXTENT.
PRIVATE ORGANIZATIONS WERE FORCED TO INVEST QUICKLY IN SOFTWARE PLATFORMS THAT FACILITATE COMMUNICATION AND MEETINGS (SUCH AS ZOOM AND MICROSOFT TEAMS), WHILE ALSO MAKING CHANGES TO SERVICE DELIVERY TO REDUCE FACE-TO-FACE INTERACTION. LOOKING AS A WHOLE, TECHNOLOGY HAS THE ROLE OF FACILITATING INTERACTIONS IN AND BETWEEN DIFFERENT HUMAN ACTIVITIES. AT THE SAME TIME, TECHNOLOGY AND ESPECIALLY TECHNOLOGICAL PROGRESS STIMULATES THE ADAPTATION OF LIFE TO THE NEW REQUIREMENTS GENERATED BY TECHNOLOGICAL PROGRESS. IN RECENT YEARS, THE ADAPTATION AND ADOPTION OF DIGITAL RESOURCES IN VARIOUS PROCESSES HAS BEEN CONSIDERABLE AND CLOSELY RELATED TO THE HEALTH CRISIS. AS A RESULT, THE DIGITAL TRANSFORMATION DEMONSTRATED ON THE ONE HAND THE ABILITY TO CONTRIBUTE TO MITIGATING AND COMBATING THE PANDEMIC AND ON THE OTHER HAND IT HIGHLIGHTED THE IMPORTANCE OF DIGITAL STRATEGIES WITHIN ORGANIZATIONS.

KEY WORDS: DIGITALIZATION, SECURITY, SECURITY STRATEGIES, DIGITAL TRANSFORMATION

INTRODUCTION

The current cyber environment is ever-changing and needs to be understood quickly, so that organizations can operate and adapt easily, without facing problems that could hinder evolution and reputation. Regular review of the security strategy and its improvement are paramount because it helps to achieve the objectives both now and in the future. As the

[1]Borca Larisa-Geanina, MA student, Security management in contemporary society, Faculty of History and Philosophy, Babeș-Bolyai University, e-mail: larisaborca3@gmail.com

change takes place, organizations need to consider certain risks and vulnerabilities that are present in the online environment, which is why cybersecurity must be put first when organizations decide to move to the current shift in terms of digitalization.

In our research, we will start from the following questions: How does the digital transformation process apply and evolve within private organizations? And why should the security strategy of private organizations be changed in the context of digital transformation? Agile approaches are not only a trend, but also a necessity. If we were to think from a leader's personal perspective, the leader must be prepared to lead change by taking risks, inspiring employees and fostering a shared ambition, these remain important factors. Change takes place at all levels during a digital transformation. The pillars behind the transformation are the compelling vision of leadership, the development of strategies, the promotion of a culture change and the alignment of talent and resources within the organization. A successful digital transformation can lead to the transformation of the organization's culture. In order to keep up with competitors, a leader must have digital knowledge, which means technology awareness and that ability to analyze quickly, to be aware of the impact of technological change, and then use them to best position the organization. The digital transformation process applies and evolves based on each organization's specific strategy to plan ahead of time the steps that aim to sustain and improve business performance. According to McKinsey's 2018 Article, "transformations are hard, and digital transformations are even harder." The key to success lies in reviewing processes, operations and customer relationships. A strategy doesn't just focus on changing the way it works, it focuses on what the organization will do more or less to help the client make the difference. Predictive modeling, understanding what the customer wants through experimentation, and using a framework based on real, verifiable and testable data are new digital transformation models to create a competitive advantage. Organizations with this level of innovation and flexibility they reach economic competitiveness through digitalisation.

In line with reality, it is important for us and for organizations that digital transformation takes into account all the parameters necessary for success, depending on strategy, roadmap, objectives, stakeholders, context, etc. It is also important not to look at digital transformation from a purely technological or purely marketing perspective or from any other perspective. ci In a globalizing world, digitalization is paramount because it eliminates certain human errors and thanks to artificial intelligence contributes to more efficient management and entails benefits.

SECURITY

The concept of security is delicate, one that everyone takes seriously, especially in a globalized world after the attacks of September 11, 2001. Security has been a lifelong concern for human communities. In fact, the need to ensure a constructive life, of material and spiritual progress, against external hostilities, arose with the existence of man, who, once they ensure their food and shelter, he also took care of his security. There is no single definition of this concept, because it is quite broad and encompasses several meanings, depending on the political context. However, it goes without saying that security is the idea of being or feeling safe from threats or dangers. Security is defined in several ways. We have selected the following definitions:

- Lack of war;[2]
- The ability of a country to successfully promote its national interests; (Penelope

[2] Bellany, Ian. *Towards a Theory of International Security*. Political Studies, Vol. 29, No. 1, March 1981, 102.

Hartland-Thunberg, 1985)

- Ensure future well-being;[3]
- Maintain a lifestyle acceptable to citizens, but consistent with the legitimate needs and desires of others;
- In any objective sense, it measures the existence of a threat to existing values, while in a subjective sense it measures the fear that those values will be attacked;[4]
- A sense of trust and tranquility which he gives to someone the absence of any danger;[5]
- Feeling of staying away from any danger;

Another definition we find in the paper Religion and security in 21st century Europe – Glossary of terms, where the concept of security is presented by a group of authors and "refers to the specific measures taken by a person, a group of people, the state, the coalition, either alone, or in consultation with other actors to ensure that its existence, integrity and essential interests are not threatened"[6].

Security is a political concept that has evolved over time. The Copenhagen School of Security studies has its origins in international relations and has developed an important study in the field of security, and the founder of this school of academic thought is the theorist Barry Buzan. This school places a special emphasis on the social aspects of security. Buzan's approach is interesting because it looks at security from a micro to macro perspective. It should be noted that before Buzan, there was a gap in the literature on the concept of security. Buzan set out to fill that void and worked on security research. In his article, *New Patterns of Global Security in the Twenty-First Century*, the theorist Buzan addresses five security-based sectors and moves toward a broader understanding. These are: Military, political, economic, societal and environmental. Each of these concepts cannot address the security issue in a separate perspective because they are linked, complex and connected to each other, forming a network of information[7].

According to the literature, "military security refers to the two-level interaction of States' offensive and defensive armed capabilities and States' perceptions of each other's intentions. Political security refers to the organizational stability of States, systems of government, and ideologies they confer legitimacy. Economic security refers to access to the resources, finances and markets needed to sustain acceptable levels of well-being and state power. Societal security refers to sustainability, under acceptable evolutionary conditions, by preserving group identity, language, culture, and religious and cultural customs. Last but not least, environmental security is about maintaining the local and planetary biosphere as an essential support system upon which all other human enterprises depend".[8]

---

[3] Martin, Laurence, *National Security in an Insecure Age*, Naval War College Review: Vol. 35, No. 5, 1982, article 3.
[4] Wolfers, Arnold, *National Security as an Ambiguous Symbol*, *Political Science Quarterly*, Editura Academy of Political Science Vol.67, No.4, Dec.1952, 485.
[5] Dexonline, avalilable at: adress https://dexonline.ro/definitie/securitate (07.04.2022).
[6] Buță Viorel; Emil Ion; Mihai Ștefan Dinu (coord.), *Religie și securitate în Europa secolului XXI– Glosar de termeni*, (Ed. Universității de Apărare „Carol I ", București), 2007, 99.
[7] Barry Buzan, *New Patterns of Global Security in the Twenty-First Century*, Editura Blackwell (Royal Institute of International Affairs), Vol. 67, No.3, Jul.1991, 433.
[8] Buzan, Waeve, Wilde, *Security: A new framework for analysis*, (Editura Lynne Rienner Pub., 1998), 8.

DIGITAL TRANSFORMATION (differences between digital transformation, digitization and digitalization)

Based on our analysis made on the concept of security, we will talk and try to continue during this research, to integrate security in the area of the digital age. In order to be able to study security in the field we have proposed to address, we need to first define the notion of digital transformation. Digital transformation is a rather ambiguous and vague concept, it has a lot of different meanings for different people, and at the moment it is useful for us to define it and discover what exactly that term means. Before choosing some definitions from the related bibliography, we will try to make our own contribution to the definition of this notion. In its simplest terms, we believe that digital transformation means changing the way we operate a business in which we work through the new organizational culture and through a better customer experience, changing the way we live and the way we do business.

According to the literature of specility, we have managed to extract some definitions characteristic of the field of digital transformation, and these are:

- According to Mazzone, "Digital transformation is the deliberate and continuous digital evolution of a company, business model, idea process or methodology, both strategically and tactically";[9]
- According to PwC, "Digital transformation describes the fundamental transformation of the entire business world by creating new internet-based technologies with a fundamental impact on society as a whole";[10]
- According to Boueé and Schaible, "we understand digital transformation as a consistent network of all sectors of the economy and the adaptation of players to the new realities of the digital economy. Decisions in network systems include data exchange and analysis, calculation and evaluation of options, as well as initiating actions and introducing consequences";[11]
- According to Deloitte Digital, "Digital transformation is becoming a digital enterprise — an organization that uses technology to continuously evolve all aspects of its business models (what it offers, how it interacts with customers, and how it works).";[12]
- According to Gartner, "Digital transformation can refer to anything from it modernization (e.g. cloud computing) to digital optimization, to the invention of new digital business models. The term is widely used in public sector organizations to refer to modest initiatives such as online service delivery";[13]

We see that the five definitions lead in a common direction, namely digital transformation is a broad process that embraces the entire organization. This transformation involves all processes and employees and is based on a different strategic vision of how the organization itself should act and react with a radical change in the mindset of employees.

The concept of digital transformation also plays a key role in defining three pillars. The first pillar is customer experience because today's consumers have more options than in the past. This means that the stakes are high for companies, not only to offer innovative

[9] Daniel R. A. Schallmo and Christopher A. Williams, *Digital Transformation Now!* Guiding the Successful Digitalization of Your Business Model, (Editura Springer, 2018), 10.
[10] Daniel R. A. Schallmo and Christopher A. Williams, *Digital Transformation Now!*..., 10.
[11] Daniel R. A. Schallmo and Christopher A. Williams, *Digital Transformation Now!*..., 10.
[12] Deloitte Digital, *Digital-Transformation: A PRIMER,* 2.
[13] Definition of Digital Transformation - *Gartner Information Technology Glossary*, Gartner, avalilable at: adress https://www.gartner.com/en/information-technology/glossary/digital-transformation, (06.04.2022).

products or services, but also meaningful interactions and experiences to delight customers and inspire brand loyalty. Let's just think about how many packaged food options we have these days. Our choice can be directly related to the company's digital transformation, whether it's easy-to-use applications, seamless transactions, excellent customer service or fast delivery. The second pillar is process-based, customer-focused organizations don't transform to add technology for their own sake. They do this because they support processes that truly benefit those they serve. Last but not least, the third pillar is technology. We are talking about using technology to improve a product or service, and at the same time, this digital transformation process creates an agile infrastructure that is needed to adapt to the demands of consumers. Organizations that master customer-centered change prioritize the quality of their technological experience, which means it's an enterprise-wide investment decision.

Digital transformation can easily be confused with two other concepts, namely the concept of digitalization and the concept of digitization. Even if at the first meeting with these terms give us the impression that it is one and the same and that it sounds similar, in theory they are not the same. Even some companies sometimes end up mixing both terms. Next, we will explore the differences between digital transformation, digitalization and digitization. According to the Gartner it Glossary, "digitization is the process of moving from analogue to digital form"[14]. In other words, it is really the process of converting information from a physical format to a dgital one. To be more clear, we will give some examples, such as: Home, scanning old family photos and saving them on your computer or mobile phone; in our office, converting all our paper documents into digital documents by scanning; convert our old videos or from the tapes into mp3 digital files.

Going forward, the digitalization process is all taken into account by the Gartner IT Glossary and assumes "using digital technology to change a business model and provide new revenue generation opportunities; it is the process of moving to a digital business"[15]. By consulting the literature we try to deepen by examples: the local taxi business has been digitized using a mobile app – instead of calling a certain phone number, we can use the app to call a taxi and we can also track its movement and pay, also, through the app, which means that the entire process has been digitized. Other examples include: instead of going to the cinema to watch movies, we can now watch movies using Netflix or Amazon Prime services; nowadays, we no longer buy audio tapes to listen to music, but use a streaming service like Spotify.

Well, the difference between these two terms that seem similar is that: digitization is the conversion of existing information or physical objects to a digital format, compared to digitalization which is a complete transformation of a business or a process, it is more of a holistic and systemic approach, so that its operations are carried out using digital technologies, in this sense we are talking about food delivery applications instead of the traditional way of making an order. We digitize information, digitalise the processes and roles that make up a business's operations and digitally transform the business and its strategy. Digital transformation encompasses both digitalization and digitization. It is not the process of converting a company's files from paper format to digital format. Digital transformation is the amalgamation of several initiatives, projects and processes to bring an

[14] Definition of Digitization - *Gartner Information Technology Glossary,* avalilable at, https://www.gartner.com/en/information-technology/glossary/digitization, (07.04.2022).
[15] Definition of Digitalization - *Gartner Information Technology Glossary*, avalilable at https://www.gartner.com/en/information-technology/glossary/digitalization, (08.04.2022).

organization from an early state of digital competence to a mature state with true digital capability.

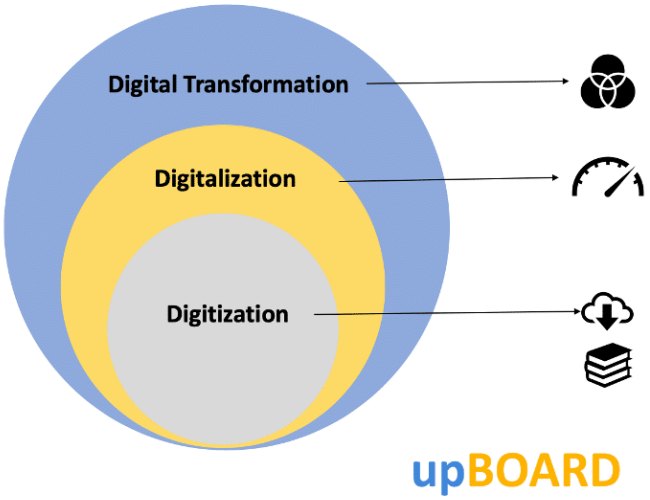

Figure 1. The process of digital transformation
Source: https://praxie.com/digital-organization-business-process-transformation-through-digitization/

SECURITY STRATEGIES

Next we will focus on security strategies and what they imply. In the section on security we defined and saw what the concept of security means, but we did not discuss it in the context of the digital era and digital transformation. In a digital world disrupted by known or lesser-known threats, adopting an anticipated "ready for anything" view of security is important. Large and small businesses need to consider cyber security if they want to stay protected from cybercrime. Information security faces unprecedented challenges and extraordinary opportunities. Advanced attacks are becoming more sophisticated and more frequent, testing the limits of existing capabilities. The effort of companies to digitize aggravates the problem and significantly increases the volume of sensitive and vulnerable organizational data to attack. As such, organizations need strategic plans for most of their activities. From the analysis of the specialty literature we have identified three definitions of security strategy. For example, the security strategy can be defined as:

- „the art of deciding how best to use the appropriate technologies and security measures for defensive information and implementing and applying them in a coordinated way to the information infrastructure of the defense organization against internal and external threats, providing confidentiality, integrity and availability at the expense of the least effort and cost to be effective"[16] according to Park şi Ruighaver;
- „the model or plan that integrates the organization's major security objectives, policies and action sequences into a cohesive whole"[17] according to Beebe şi Rao;
- „a plan to mitigate information security risks while respecting legal, statutory,

[16] Sangseo Park and Tobias Ruighaver, *Strategic Approach to Information Security in Organizations*, publicat în *International Conference on Information Science and Security (ICISS 2008)*, 10-12 Ian. 2008, Editura IEEE, 27.
[17] Nicole L. Beebe and V. Srinivasan Rao, *Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process*, Publicare: Communications of the Association for Information Systems: Vol.26, Art. 17, 31 Mar. 2010, 330.

contractual and internally developed requirements. Typical steps to building a strategy include defining control objectives, identifying and evaluating approaches to achieving objectives, selecting controls, setting benchmarks and metrics, and preparing implementation and testing plans"[18].

Looking at these definitions, we come to the conclusion that a strategic plan defines the need for action, the impact of specific actions and the underlying factors. The security strategy of any organization begins with an in-depth analysis of its business. As a result, a security strategy is an important document detailing the many steps an organization needs to identify, remedy and manage risks in a timely manner. Initial assessment, planning, implementation and constant monitoring are detailed processes in the development of a security strategy. Moreover, an operative strategy must be comprehensive, dynamic and resistant to any type of threat.

Cybersecurity expert and CEO Joseph Steinberg says that "cybersecurity is important for companies of all sizes" and "business leaders recognize the need to adapt accordingly and expand their cybersecurity strategies in step with the company's developments in personnel, processes and technologies".[19] According to two other authors, Jon Kerner and Henry Bell, they believe that by operationalizing the security strategy through a set of risks-based plans and actions, a bridge of cybersecurity and physical security projects and programs is created. "The business plan is the most powerful tool to ensure that the entire risk-based operating model is aligned with the organization"[20].

SECURITY CULTURE

Security culture is a concept consisting of two terms, which come from a different environment of activity. In order to fully understand this concept, it is necessary to define separately security, culture, and implicitly the merging of terms. In the first part of this work we defined and analyzed what the concept of security implies and how important it is, but we have not defined until now the notion of "culture" that is closely related to security, we will see why.

An analysis of the literature has shown that there is no accepted practical definition of culture. Several authors have defined culture as follows: Becker and Geer claim that it represents a "set of common understandings, expressed in language"[21], Kroeber and Kluckhoh point out that the idea of culture means "patterns transmitted by values, ideas and other symbolic systems that shape behavior"[22], Louis says that "it is usually used to refer to a common system of values, norms, and symbols, the term culture conveys an entire image, an

[18] Gary R. Lomprey , *Critical Elements of an Information Security Management Strategy*, University of Oregon Applied Information Management Program, July 2008, 18.
[19] Security Intelligence, *Your Security Strategy Should Scale and Evolve Alongside Your Business*, 2019, avalilable at: adress https://securityintelligence.com/articles/your-security-strategy-should-scale-and-evolve-alongside-your-business/, (10.04.2022).
[20] ScottMadden, *The Security Operating Model*, 27 Mai 2021, accessible online at adress https://www.scottmadden.com/insight/security-operating-model-strategic-approach-building-secure-organization/, (10.04.2022).
[21] Howard Becker and Blanche Geer, Human Organization, *Participant Observation and Interviewing: A Comparison*, Vol.16, No.3, 1 Sept. 1957, 29.
[22] Kroeber, A.I., and Kluckhohn, C., *Culture: A critical review of concepts*, Vol. 47, No.1, (1952), Editura Museum, Cambridge, Massachusetts, U.S.A., 34-48.

integrated set of dimensions or characteristics"[23]. The United Nations educational, Scientific and cultural Organization (UNESCO) defines culture as "a collection of distinctive spiritual, material, intellectual and emotional traits of society or a social group, encompassing not only art and literature, but also lifestyles, ways of living, systems of values, traditions and beliefs"[24]. If we extract the essence of these given definitions, we notice common elements.

Thus, starting from these theoretical aspects, the security culture can be interpreted as a model of basic assumptions, values, norms, rules, symbols and beliefs that influence the perception of challenges, opportunities and/or threats, and also influence the way of thinking about what security involves, the behavior and activities of active social actors, individual or collective[25]. As well, the security culture is closely related to security awareness, yet these two concepts are at odds, why do I say that? By security awareness we mean risk knowledge, while the security culture encompasses more knowledge as a starting point. At national level, in the glossary proposed by the National Defense Strategy Guide of The Country for the period 2015-2019, we identify a first definition, where the security culture represents "the totality of values, norms, attitudes or actions that determine the understanding and assimilation at the level of the society of the concept of security and those derived (national security, international security, collective security, insecurity, security policy, etc.)"[26].

In this context, by reporting security culture to private organizations, we can affirm that developing and maintaining an effective security culture is an essential part of a security regime and helps mitigate a range of threats that can cause physical, reputational or financial harm to an organization.

Achieving a proper security culture will help develop a security-conscious workforce and promote safe behavior among employees. Many organizations want to incorporate an effective security culture based on collective responsibility, where security is the strong point of all those who are part of an organization.

DIGITAL SECURITY CULTURE

The key to an effective security culture is trust, and that trust manifests itself with how leaders can create a culture of security in their organizations. Because so far in this paper we have focused on digital transformation, the security culture in the digital age involves classifying data that allows organizations to protect and share information with confidence. The term "digital security" refers to "the resources used to protect our online identity, data and other assets. These tools include web services, antivirus software, smartphone SIM cards, biometric elements, and secure personal devices. In other words, digital security is the process used to protect our online identity"27.

When we say digital security culture in organizations, we are actually referring to the culture of cyber security. The European Union Agency for Network and Information Security

---

[23] Meryl Reis Louis, *A Cultural Perspective on Organizations: The Need for and Consequences of Viewing Organizations as Culture-Bearing Milieux*, Editura Human Systems Management, Vol 2, No.4, 1 Dec. 1981, 249.

[24] UNESCO Institute for Statistics, *The 2009 Unesco Framework for Cultural Statistics (FCS)*, 2009, p. 9.

[25] Juliusz Piwowarski, Security Dimensions. International & National Studies, *Three Pillars of Security Culture*, No. 22, 2017, 21.

[26] Ghidul Strategiei Naţionale de Apărare a Ţării pentru perioada 2015-2019, *Glosarul pricipalelor concepte şi termeni cu care operează SNAP*, 17 Dec. 2015, Bucureşti, avalilable at: https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019, 7.

[27] Just Ask Thales EN, *What Is Digital Security?*, 17 Jul. 2015, avalilable at https://justaskthales.com/en/what-is-digital-security/, (30.04.2022).

(ENISA) emphasizes the following: "The cybersecurity culture of organizations refers to knowledge, beliefs, perceptions, attitudes, assumptions, etc. people's norms and values about cybersecurity and how they manifest themselves in behavior with information technologies"[28]. The growing number of cyber threats to organizations is increasing and has increased with the onset of the COVID-19 pandemic crisis. With the digital transformation, there is a growing need for companies to focus on cybersecurity, not only to mitigate ever-evolving threats, but also to unlock the growth that digital trust enables. Organizations must consider building resistance based on adopting a security mindset/culture in terms of technological knowledge. Cybersecurity culture isn't just about physical barriers to entry, it's more than that. In fact, it represents a mindset of all the people in the organization who work every day to protect the business.

Firstly, the digital security culture helps protect the most important asset of the business: Its data. An organization's data is hard to replace because most companies spend years and countless resources to collect and create the organization's data assets. Neglecting the cybersecurity culture and data loss could send organizations into insolvency. Thus, greater attention should be paid to data protection and cyber security at all levels. Our review of the literature confirms that in order to develop a cybersecurity culture, organizations should not be limited to the Security Education Training and Awareness (SETA) approach alone[29], but to investing heavily in implementing transformative changes to develop a cybersecurity culture. (ENISA, 2017; AlHogail 2015; Alshaikh et.al 2018). Secondly, the fundamental element for forming an effective cybersecurity culture is the empowerment and training of employees in the field of cybersecurity because it is everyone's responsibility.

Therefore, in a dynamic, uncertain context in which the digital environment has become essential for growth and prosperity, well-being and inclusion, digital security risks should be considered and organizations need to be more agile about learning.

CYBER-SECURITY IN ORGANIZATIONS (evolution, risks and vulnerabilities)

For every organization, both private and government, data/information security is a top priority. Bringing up the concept of "cyber security" we will be able to reflect on it in the following lines. Broadly speaking, Proofpoint considers the definition of the term and it is outlined as follows: "cyber security encompasses the technology, services, strategies, practices, policies designed to secure people, data and infrastructure from a wide range of cyber attacks"[30]. But in a narrow sense, at the organization level, cybersecurity means more than technology, it means that in the cybersecurity strategy the heart must be the people/employees, because they are the ones who manage the emails, data and cloud applications that directly influence the security of the organization. Data or information leaks from organizations have been recorded most of the time by employees. According to

[28] European Union Agency for Network and Information Security, *Cyber Security Culture in Organisations,* Editura: Publications Office, 2017, Luxemburg, avalilable at https://data.europa.eu/doi/10.2824/10543, (03.05.2022), 7.

[29] It is "a program designed to help organizations mitigate the number of security breaches caused by human error. This is done by informing people about information security policies and by being able to apply them during their daily activities to help prevent security incidents" IT Living Lab, *Security Education Training and Awareness (SETA)*, avalilable at https://livlab.org/seta/, (03.05.2022).

[30] Proofpoint, *What Is Cybersecurity? - Network Security Meaning | Proofpoint US*, 26.02 2021, avalilable at adress https://www.proofpoint.com/us/threat-reference/cybersecurity-network-security, (03.05.2022).

one report, 85% of errors were caused by people, and 61% were caused by credentials[31]. This means that anyone in any organization, regardless of role or seniority, can allow an attack to complete without the person or employee having any negative intentions.

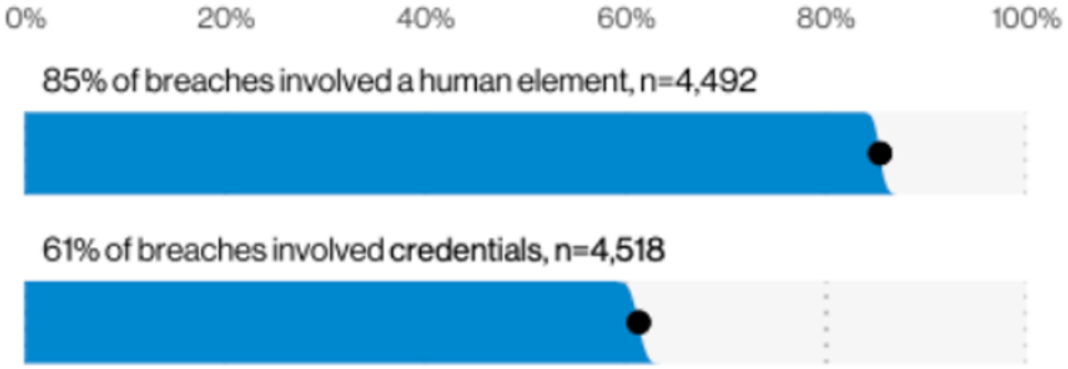

Figure 2. Verizon 2021 data breach report
Source: Data Breach Investigations Report 2021, p.7

A successful cyber attack on an organization's systems poses a serious risk that could suffer serious damage and financial losses. Risk is the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. Any event that could result in the compromise of organizational assets for profit or personal interest. If the organization is not vulnerable, then there is no risk. We can say that risk is the product of vulnerability and implicitly of threat. Let's take the following examples: The employee is a threat, access to social networks in the office illustrates vulnerability, and sharing confidential information is a risk to the organization; the virus is a threat, outdated antivirus installed on the system is a vulnerability, and the loss of data obviously will be a risk; the lack of adequate firewalls is a threat, the easy penetration of intruders into networks and network assets are a vulnerability, and the theft of important data will be considered a risk.

The Global Risks Report provides an example in the context of digital systems dependency: "The digitalization of physical supply chains creates new vulnerabilities, as those supply chains rely on technology providers and other third parties, who are also exposed to similar, potentially contagious threats"[32].

This acceleration of digital transformation and digitalisation, which is becoming more important, creates doors to risks, vulnerabilities and threats, while a cyber resilience strategy must be one of the priorities of organizations to counter these errors, as it will considerably reduce risks, financial impact and reputational damage. Risk management is fundamental to the emergence of cyber resilience, and the current COVID-19 pandemic has put the importance of digital assets at the forefront through several key steps involved. We consider a four-step approach to achieving and building a cyber resilience strategy:

1. Resilience plan to maintain it resilience and prevent unauthorized access by cyber attackers;
2. Conducting a risk analysis based on Activity Impact Analysis (BIA) which can

[31] Data-Breach-Investigations-Report, 2021, avalilable at https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx, (03.05.2022), 7.
[32] The Global Risks Report, 2022, 17th edition, editura World Economic Forum, 47.

facilitate the identification of the most likely internal and external cyber threats to the capacity of an organization. Conducting SWOT analysis to identify weaknesses such as insecure network periemter that could increase the risk of a cyber attack;

3. Identification and detection is the third element of a cyber resilience program. Continuous monitoring of the network and information systems can detect cyber security anomalies and potential incidents before they make their presence felt;
4. Evaluate the process of continuously improving the organization's security measures and adapting to the changing threat landscape.[33]

HOW THE DIGITAL TRANSFORMATION PROCESS IS APPLIED AND EVOLVING WITHIN PRIVATE ORGANIZATIONS

We used as a basis a questionnaire applied to a sample of 8 private organizations, which were randomly chosen from Cluj-Napoca and this questionnaire takes into account the applicability and evolution of the digital transformation process by following the level of digitalization, security and the existence of digital strategies.

The questionnaire starts with two questions identifying respondents, with which we tracked the age segment of the leaders of each organization and the number of employees. The predominant age is between 40-50 years, followed by the age range of 30-40 years, and the fewest respondents are in the age range 23-30 years and 50-60 years.

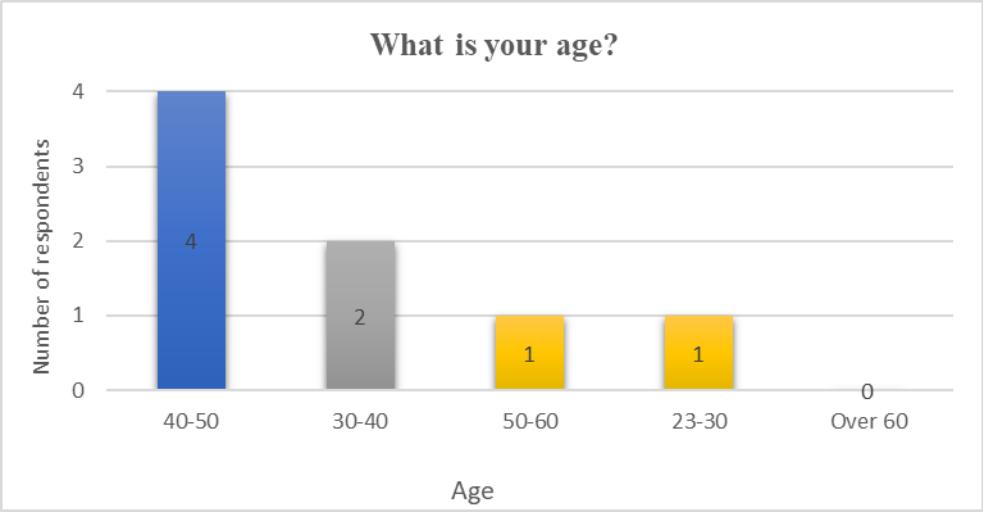

Figure 3. Age category of respondents
Source: Produced by the author based on the results collected from the questionnaire

The number of employees preponderant is greather than 100, this means that 4 of the 8 organizations surveyed are large enterprises, and the remaining 4 are part of the category of small and medium-sized enterprises with a number of employees less than 20 or between 20 and 100.

[33] Issquared, *What Is a Cyber Resilience Strategy and How Is It Implemented?*, 10. 03. 2021, avalilable at: adress https://www.issquaredinc.com/insights/resources/blogs/what-is-a-cyber-resilience-strategy-and-how-%20to-implement-it, (05.05.2022).

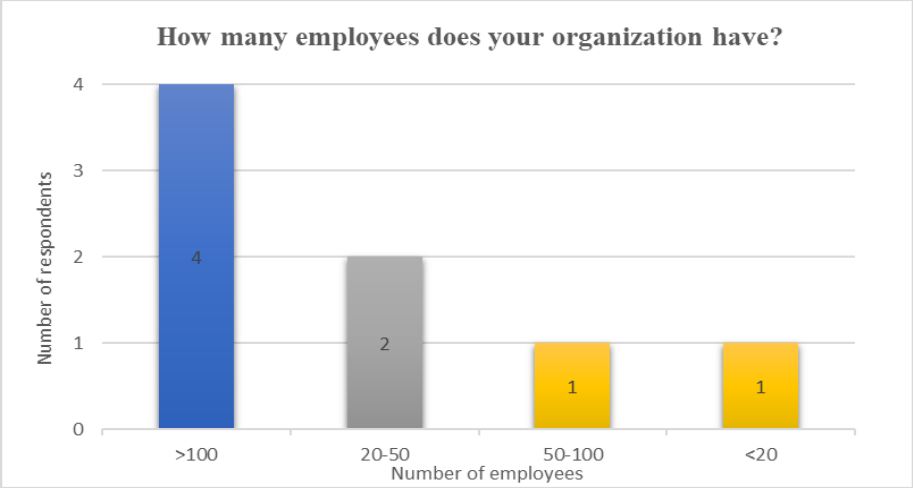

Figure 4. The number of employees in an organization
Source: Produced by the author based on the results collected from the questionnaire

We believe that the success of digital transformation depends on how leaders use digital technology to grow their organization, regardless of age. The literature studied has often revealed that the challenges that typically slow down digital transformation are not based on technology, but on people and organizational issues.[34].

That is why this statement is validated by the answers to question 7. Responsibilities and roles for digital transformation are partially defined by 75% of respondents and very well defined by 25% of respondents, which means that digital transformation cannot be achieved just by delegating responsibility to a single subordinate. For digital transformation to succeed, the entire leadership team must embrace every role in digital change. By focusing on these roles and responsibilities within each organization, they can contribute to a seamless digital transformation.

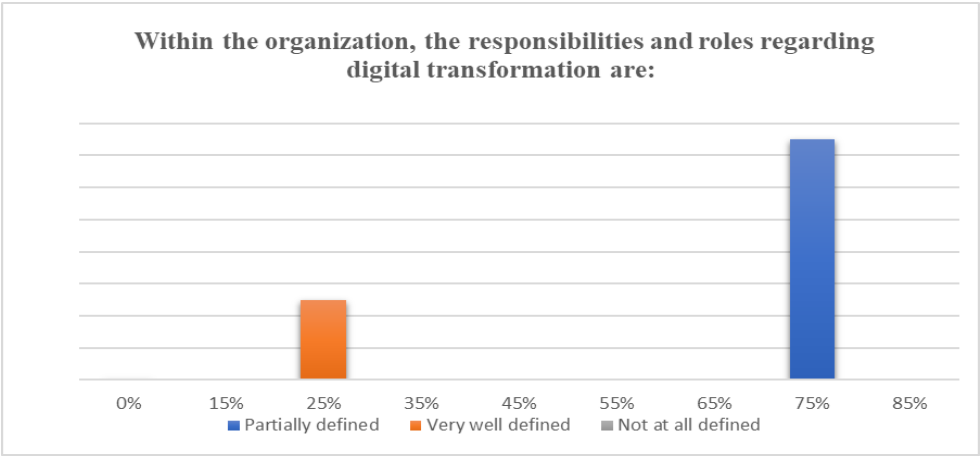

Figure 5. Distribution of responsibilities in an organization on digital transformation
Source: Produced by the author based on the results collected from the questionnaire

[34] Nepf - Make Organization Change Happen, *The Critical Role of Leadership in Accelerating Digital Transformation*, 25 Iun. 2018, avalilable at: https://www.nepf.co/the-critical-role-of-leadership-in-accelerating-digital-transformation/, (03.06.2022).

By looking at the answers to questions about digital transformation, we have come to a conclusion that private organizations are familiar with the concept of digital transformation and have heard about it, resulting in 100%, as it is not a new notion. Question 4: "How would you define this concept of digital transformation?" each of the respondents made their own contribution in defining and vision about what the digital environment means.

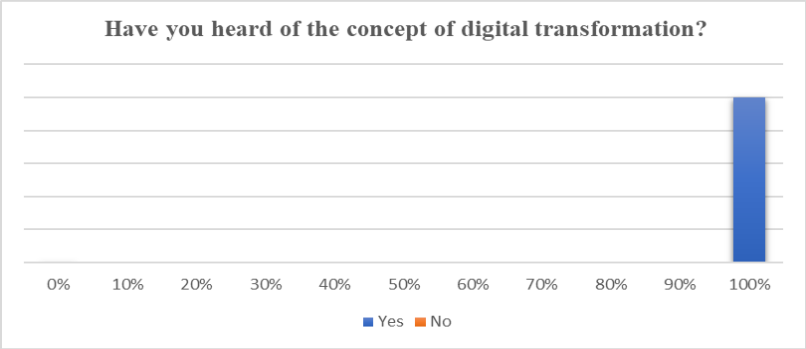

Figure 6. The concept of digital transformation
Source: Produced by the author based on the results collected from the questionnaire

Respondent	How would you define this concept of digital transformation?
1	Using new technologies to support employees and the organization;
2	Technological processes;
3	Information and communication technology;
4	The process by which departments and processes are carried out with the help of new technologies;
5	Introduction of digital processes. Databases accessible by everyone. Software for different processes;
6	Efficiency through digitalization;
7	Adapting the processes within the company to the new technologies;
8	Implementation of digital technologies by the company to optimize work processes and services;

Table 1. List of respondents who defined the concept of digital transformation
Source: Produced by the author based on the results collected from the questionnaire

The following questions were formulated to see to what extent organizations agree with the statements below:

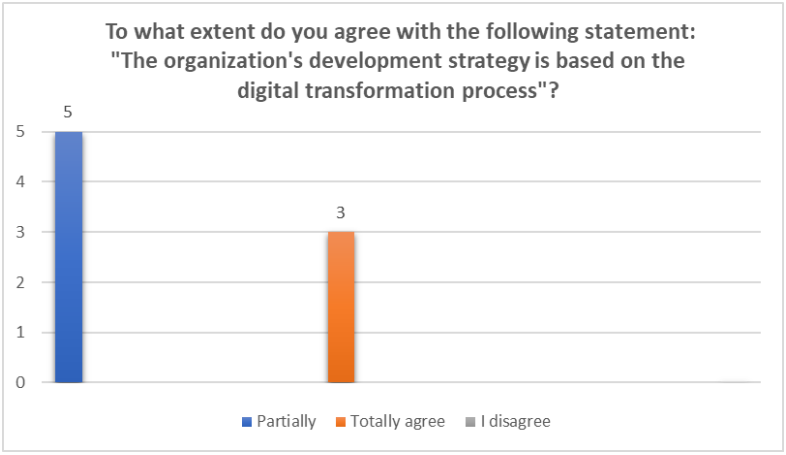

Figure 7. To what extent do respondents agree with the statement
Source: Produced by the author based on the results collected from the questionnaire

Five out of 8 respondents agree in part and 3 out of 8 agree that the organization's development strategy is based on the digital transformation process. The speed at which the world is moving is increasing, we live in a world where globalization and technology are closely intertwined. In an era where the fourth industrial revolution, as it is called by the literature, is increasingly making its presence felt, it is imperatively necessary that the organization's development strategy is based on the digital transformation process in order to be able to operate in optimal parameters. The term "development" itself involves an effort that focuses on improving an organization's capacity by aligning strategy and all structures.[35] So, in order to have performance, the development strategy involves a continuous, long-term process.

The digital age often involves getting new revenue streams, prioritizing consistent customer satisfaction measures, and building high-speed, equipped business models. At a more fundamental level, the "digital march" is essentially the latest way of conceptualizing trade, as many have called it.

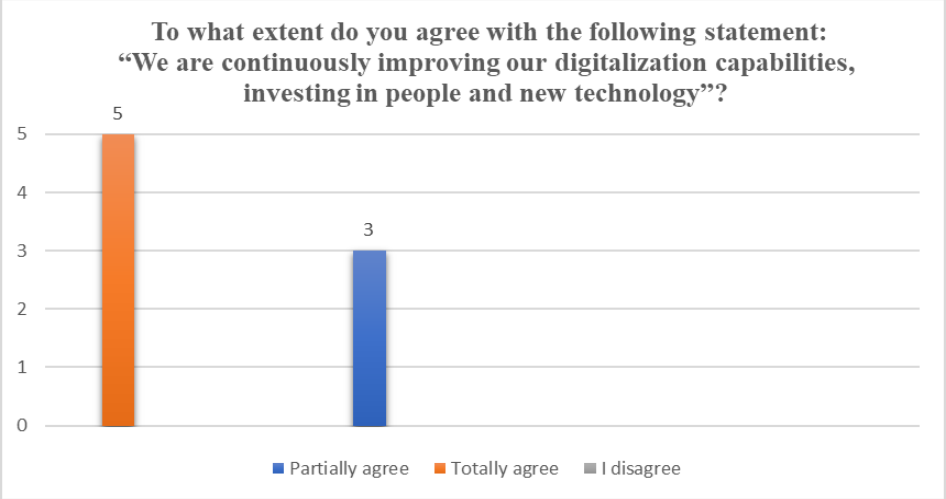

Figure 8. To what extent do respondents agree with the statement
Source: Produced by the author based on the results collected from the questionnaire

Depending on the technologies and business opportunities, leaders are driven to rethink and continually improve their approach to the market because the evolution of digital quality involves technology, strategy and people. Therefore, the results confirm that 5 out of 8 respondents are totally agree by the above statement and 3 out of 8 respondents are partially agree.

Next, we chose to leave the area of everything that involves the concept of digital transformation and what it means to change in itself the development strategy and the capabilities in terms of digitalization, asking a set of questions that are somewhat more sensitive. They have been put with a focus on security and in particular cyber security, which is a main pillar when such a transformation takes place in the digital context. The questions concern the management team of each organization surveyed, whether it is interested in risks/vulnerabilities and whether it complies with security best practices.

Only 2 out of 8 organizations are not interested in what the organizational security culture means, the remaining 6 according to the survey are aware of security policies and

[35] ATD, *What Is Organization Development | The 5 Phases of OD Strategies,* avalilable at: https://www.td.org/talent-development-glossary-terms/what-is-organization-development, (03.06.2022).

implicitly cyber security, which denotes a positive aspect. Given the new threats in the digital landscape, cyber risks deserve the same attention as other types of risks. Thus, an organizational security culture requires compliance with security regulations by educating employees and developing awareness.

By implementing good cybersecurity practices in the workplace, not only will a security culture develop over time, but the organization will also be better protected from cyber threats.

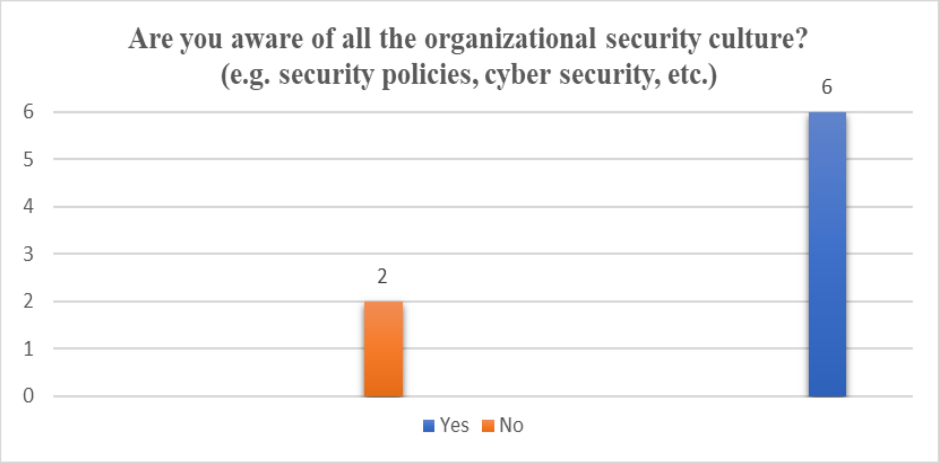

Figure 9. Awareness of organizational security culture
Source: Produced by the author based on the results collected from the questionnaire

The following question was asked to see if respondents understand weaknesses through cybersecurity assessments and audits. Of the 8 organizations, 5 of the respondents currently do not have a cybersecurity assessment or audit, unfortunately only 3 of them are aware of vulnerabilities and risks in the cyber environment.

Cybersecurity assessment covers areas such as vulnerability scanning, risk analysis, network access controls, and so on. On the other hand, cyber auditing focuses only on it systems used to store or process company data.[36]

Figure 10. Holding a cybersecurity assessment or audit
Source: Produced by the author based on the results collected from the questionnaire

[36] *ReadWrite*, *Overcoming Cybersecurity Assessment and Audit Confusion*, 2022, avalilable at: https://readwrite.com/overcoming-cybersecurity-assessment-and-audit-confusion/, (03.06.2022).

Questions 10 and 11 refer in particular to threats and vulnerabilities that may disrupt the organization's security.

At one point, in this paper we discussed in the section on risks and vulnerabilities, that employees with legitimate access rights are the most common cause of cyber breaches or attacks. The root cause may be a human error due to lack of skills to use new technologies, or an attack, as hackers often search for "sensitive doors," such as people inside the organization who are trustworthy and could be vulnerable. As a result, 5 of the 8 organizations surveyed believe that employees may pose a threat to the security of the organization.

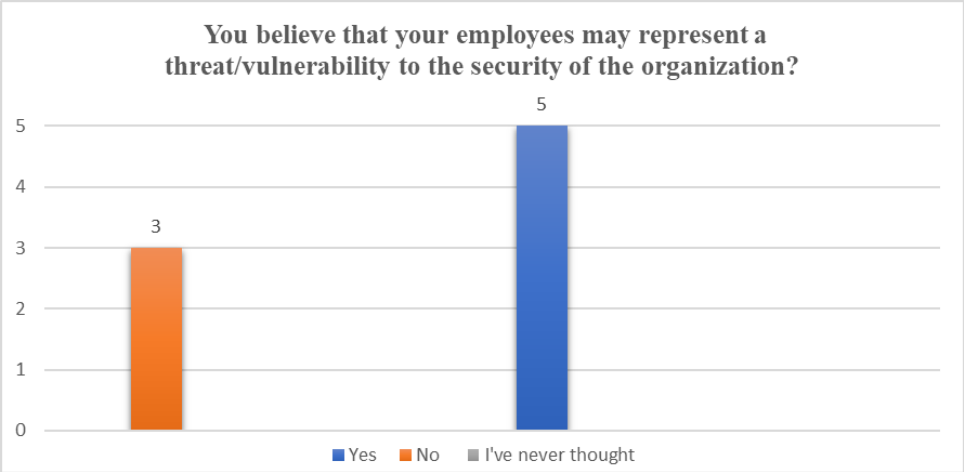

Figure 11. Employees and threats to the security of the organization
Source: Produced by the author based on the results collected from the questionnaire

To question 11 only one respondent has never considered and never thought that new technologies could pose a threat to the security of the organization, but the other 7 take into account the fact that new technologies and the way they are used entail a number of serious challenges that can disrupt security.

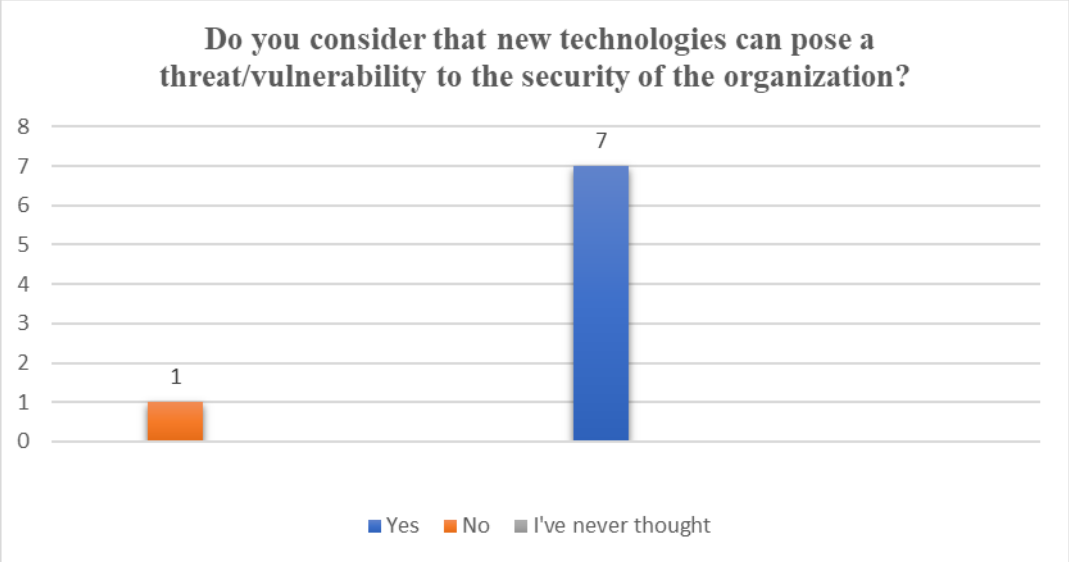

Figure 12. New technologies and threats to the security of the organization
Source: Produced by the author based on the results collected from the questionnaire

However, when talking about threats we also need to take into account external factors, not just internal ones, because if staff access to the premises is not secure, anyone or any unauthorized person could enter and cause damage to the organization.

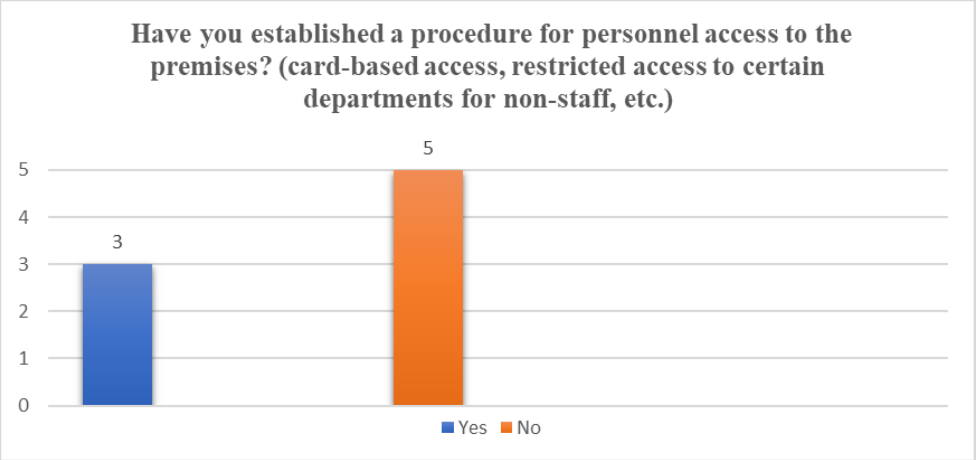

Figure 13. Procedures regarding personnel access to the premises
Source: Produced by the author based on the results collected from the questionnaire

Unfortunately, only 5 out of 8 respondents did not establish a procedure for staff access to the premises and only 3 of them established this procedure. Every business should provide a suitable working environment for authorized staff and a safe environment for both customer and property information.

Because we've been talking about sensitive information, most companies keep data in files, such as names and credit cards or other account data, through which customers or employees are identified. In order to perform certain business functions, this information serves to fulfill orders. Also, if all this sensitive information falls into the hands of cybercriminals, it can result in identity theft or similar damage. As such, question 13 was deliberately formulated with reference to how information is transferred between departments and what methods are used by respondents.

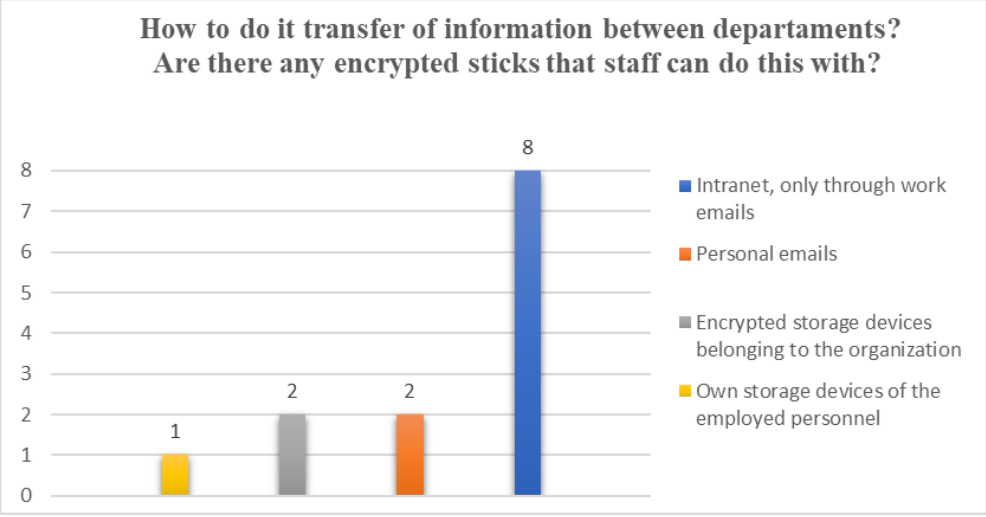

Figure 14. Methods of transfer of information between departments
Source: Produced by the author based on the results collected from the questionnaire

The highest percentage of answers to this question went to the transfer of information through internet , only through work emails. All 8 organizations use this method, but in

addition to that, they have implemented other methods. Two respondents also use personal emails, two others also benefit from encrypted storage devices belonging to the organization, while one respondent also uses own storage devicesof the employed personnel. However, regular emails are not a secure method for sending sensitive data, the best practice would be to encrypt the transfer, which contains information that could be used by fraudsters.

Simultaneously with protecting the transfer of information, the electronic equipment with which employees operate must also be somehow preserved safely. The results obtained in question 14 are affirmative with a total of 87,5% answers and 12,5% negative.

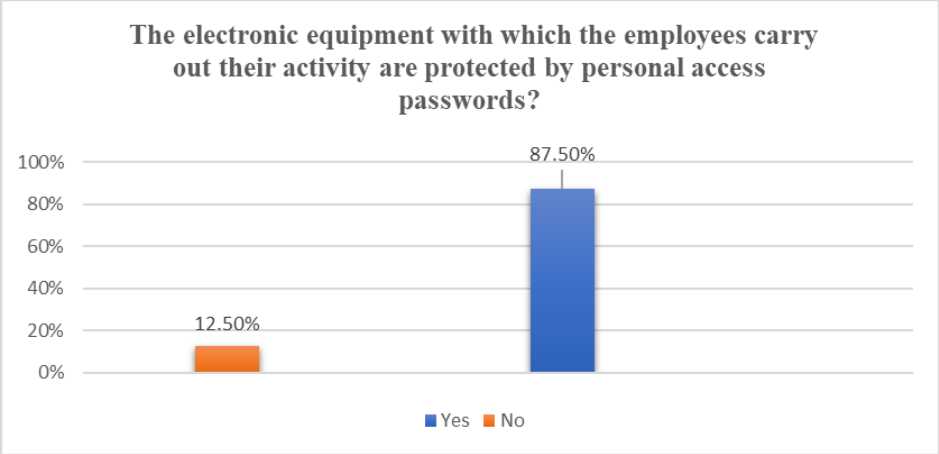

Figure 15. Protection of electronic equipment
Source: Produced by the author based on the results collected from the questionnaire

IT experts recommend that employees use strong passwords. The longer the password, the lower the risk. Simple passwords are easily guessed by, for example, the common words in the dictionary.

Unfortunately, almost every organization will suffer a system attack at some point, but if a well-executed cyber incident response procedure is implemented, it can minimize the impact of the data breach. Following the survey, we found that the vast majority of organizations surveyed are still unprepared to respond appropriately to cybersecurity incidents. 62,5% of respondents indicating that they do not have a procedure to respond to cyber security incidents, 25% of them have the procedure under implementation and only 12,5% have applied this cyber accident response plan.

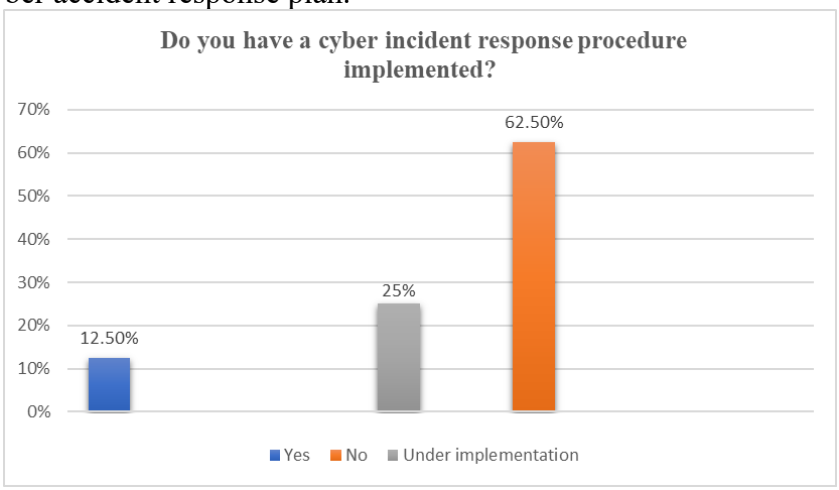

Figure 16. The procedure for responding to cyber incidents
Source: Produced by the author based on the results collected from the questionnaire

The questionnaire concludes with an open-ended question asking respondents to exemplify what they consider to be the biggest risks to the organization, from the perspective of the digitalization/ digital transformation process. As shown in the table below, only two respondents believe that new technologies do not generate risks, and the others identified some risks as follows.

Respondent	What do you think is the biggest risk to the organization, from the perspective of digitalization process/ digital transformation ?
1	Vulnerability of equipment/ IT infrastructure
2	Staff reluctance to change, lack of/ weak digital competence;
3	There are no risks;
4	New technologies should reduce risks, not generate them;
5	Non-adaptation of personnel to new technologies, data theft, industrial espionage;
6	Lack of interoperability and lack of qualified personnel;
7	Wrong implementation of processes. Misunderstanding of key employees in the implementation of digital processes and tools;
8	Vulnerable equipment/ misuse of equipment;

Table 2. List of respondents who exemplified the risks to the organization from the perspective of digital transformation
Source: Produced by the author based on the results collected from the questionnaire

CONCLUSIONS

The 21st century is often called the digital age, or according to Deloitte, it is also called the fourth industrial revolution that transforms economies and jobs. Various technologies, especially digital, use a combination of data analysis, artificial intelligence and cognitive technologies to create digital businesses that are not only interconnected but also fully capable of making informed decisions.[37] Digitization and digitalization have reached a whole new level, leading to unprecedented possibilities to design and invent new products and services. The two terms are the most important and perhaps the least understood factors. Understanding the implications of digitalization is the key to understanding the paradigm shift in innovation. The question is: How to innovate?

First of all, we've seen what digital transformation means theoretically, which is an umbrella concept for the other two notions of digitization and digitalization, and that there are many methods and tools that provide an answer to this question simply because organizations now have more options to innovate digitally than in the past. New tools such as easy-to-use applications, seamless transactions, excellent customer service or fast delivery. Obviously, with the emergence of new tools, a security strategy is needed, a step-

[37] Deloitte Romania, *A patra revoluție industrială este aici*, avalilable at: https://www2.deloitte.com/ro/ro/pages/technology-media-and-telecommunications/articles/the-fourth-industrial-revolution-is-here.html, (03.06.2022).

by-step document that is based on a holistic risk assessment. Also, regardless of whether we are talking about private or public organizations, a strategy requires clearly defined roles and responsibilities of the members of the organization. A more stringent approach to security can better align departments within an organization.

Second, the culture of security refers to the cumulation of values, shared by everyone in an organization, that drives people to think and how to approach security. We mentioned in the section on digital security culture, the main risk to an organization, where the Verizon 2021 report showed that human error is the direct and/or indirect cause of most security incidents, including through wrong, intentional or unintended behavior, indicating approximately a percentage of 85% of organizations' data breaches. These incidents are caused by human deficiencies, respectively the poor skills of employees in terms of information security. Literally, the lack of a security culture gives rise to risks and vulnerabilities that can cause huge financial losses and damage to business reputation.

Last but not least, after analyzing the results obtained from the distribution of the questionnaire, organizations heard and understood what the concept of digital transformation is, defining it as “the use of new technologies to support employees and the organization”. They believe that new technologies and employees may represent threats/vulnerabilities to the security of the organization, but there are few who have a cybersecurity assessment or audit or do not have a well-established plan for responding to cyber incidents.

REFERENCES

1. **Bellany, Ian**. "Towards a Theory of International Security." *Political Studies* 29, no. 1 (March 1981).
2. **Becker, Howard, and Blanche Geer**. "Participant Observation and Interviewing: A Comparison." *Human Organization* 16, no. 3 (September 1, 1957).
3. **Beebe, Nicole L., and V. Srinivasan Rao**. "Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process." *Communications of the Association for Information Systems* 26 (2010).
4. **Buță Viorel; Emil Ion; Mihai Ştefan Dinu** (coord.), *Religie și securitate în Europa secolului XXI– Glosar de termeni*, Ed. Universității de Apărare „Carol I ", București, 2007.
5. **Buzan, Barry, Ole Waever, and Jaap de Wilde**. *Security: A New Framework for Analysis*. Nachdr. Boulder, Colo.: Rienner, 1998.
6. **Buzan, Barry**. "New Patterns of Global Security in the Twenty-First Century." *International Affairs* 67, no. 3 (July 1991).
7. Data-Breach-Investigations-Report, 2021, avalilable at https://www.verizon.com/business/resources/reports/2021-data-breach-investigationsreport.pdfx
8. Deloitte Digital, *Digital-Transformation: A PRIMER*.
9. Deloitte Romania. "A patra revoluție industrială este aici.", avalilable at https://www2.deloitte.com/ro/ro/pages/technology-media-and telecommunications/articles/the-fourth-industrial-revolution-is-here.html.
10. "Dexonline.", avalilable at https://dexonline.ro/definitie/securitate.
11. European Union Agency for Network and Information Security. *Cyber Security Culture in Organisations.* LU: Publications Office, 2017. avalilable at https://data.europa.eu/doi/10.2824/10543.
12. Gartner. "Definition of Digital Transformation - Gartner Information Technology Glossary." avalilable at https://www.gartner.com/en/informationtechnology/glossary/digital-transformation.
13. Gartner. "Definition of Digitalization - Gartner Information Technology Glossary.", avalilable at https://www.gartner.com/en/informationtechnology/glossary/digitalization.
14. Gartner. "Definition of Digitization - Gartner Information Technology Glossary.", avalilable at https://www.gartner.com/en/informationtechnology/glossary/digitization.
15. **Gary R. Lomprey** , *Critical Elements of an Information Security Management Strategy*, University of Oregon Applied Information Management Program, July 2008,
16. "Ghid_SNApT_2015-2019_AP.Pdf.", avalilable at https://www.presidency.ro/files/userfiles/Ghid_SNApT_2015-2019_AP.pdf.
17. Just Ask Thales EN. "What Is Digital Security?,", avalilable at https://justaskthales.com/en/what-is-digital-security/.
18. **Kroeber, A.I., and Kluckhohn**, C., *Culture: A critical review of concepts*, Vol. 47, No.1, (1952), Editura Museum, Cambridge, Massachusetts, U.S.A.
19. **Louis, Meryl Reis**. "A Cultural Perspective on Organizations: The Need for and Consequences of Viewing Organizations as Culture-Bearing Milieux." *Human Systems Management* 2, no. 4 (December 1, 1981).
20. **Martin, Laurence**. "National Security in an Insecure Age" 35, no. 5 (1982).
21. Nepf - make organization change happen. "The Critical Role of Leadership in Accelerating Digital Transformation," June 25, 2018, avalilable at https://www.nepf.co/the-critical-role-of-leadership-in-accelerating-digitaltransformation/.
22. **Park, Sangseo, and Tobias Ruighaver**. "Strategic Approach to Information Security in Organizations." In *2008 International Conference on Information Science and Security (ICISS 2008)*, 26–31. Korea: IEEE, 2008.
23. **Pessoa Jos, and Lydia Deloumeaux**. *The 2009 Unesco Framework for Cultural Statistics (FCS).*, 2009.
24. **Piwowarski, Juliusz**. "Three Pillars of Security Culture." Apeiron, 2015.
25. Proofpoint. "What Is Cybersecurity? - Network Security Meaning | Proofpoint US," February 26, 2021, avalilable at https://www.proofpoint.com/us/threatreference/cybersecurity-network-security.
26. ReadWrite. "Overcoming Cybersecurity Assessment and Audit Confusion," January 19, 2022, avalilable at https://readwrite.com/overcoming-cybersecurityassessment-and-audit-confusion/.
27. **Schallmo, Daniel R. A., and Christopher A. Williams**. *Digital Transformation Now!* SpringerBriefs in Business. Cham: Springer International Publishing, 2018.

28. **ScottMadden**. "The Security Operating Model," May 27, 2021, avalilable at https://www.scottmadden.com/insight/security-operating-model-strategicapproach-building-secure-organization/.
29. Security Intelligence. "Your Security Strategy Should Scale and Evolve Alongside Your Business," December 20, 2019, avalilable at https://securityintelligence.com/articles/your-security-strategy-should-scale-andevolve-alongside-your-business/.
30. **The Global Risks Report**, 2022, 17th edition, editura World Economic Forum.
31. **Wolfers, Arnold**. 'National Security' as an Ambiguous Symbol." *Political Science Quarterly* 67, no. 4 (December 1952).
32. "What Is a Cyber Resilience Strategy and How Is It Implemented?", avalilable at https://www.issquaredinc.com/insights/resources/blogs/what-is-a-cyberresilience-strategy-and-how-%20to-implement-it.
33. "What Is Organization Development | The 5 Phases of OD Strategies | ATD.", avalilable at https://www.td.org/talent-development-glossary-terms/whatis-organization-development.