Digital Transformation Impact on Organization Management and Several Necessary Protective Actions

Doina BANCIU[1]*, Adrian Victor VEVERA[2], Ion POPA[1,3]

[1] Academy of Romanian Scientists, Ilfov 3 Street, District 5, 030167, Bucharest, Romania
doina.banciu@aosr.ro *(*Corresponding author*)*

[2] National Institute for Research & Development in Informatics - ICI Bucharest,
8-10 Maresal Averescu Avenue, District 1, 011455, Bucharest, Romania
victor.vevera@ici.ro

[3] The Bucharest University of Economic Studies, 2-10 Căderea Bastiliei Street,
District 1, 010615, Bucharest, Romania
ion.popa@man.ase.ro

Abstract: The paper presents the impact of the digital transformation on organizations. It outlines the specific details of management functions and protective actions with particular emphasis on information security. The management function is analyzed thought digital transformation pillars and the primary activities that managers perform in order to achieve organizational goals. The key management functions (foresight, planning, organizing, leading, and controlling) are interrelated and interdependent, and effective management requires a balanced approach to all including management of cybersecurity procedures. The paper underlines the main function of cybersecurity management in connection with fundamental management function. The paper also briefly describes the main cybersecurity procedures.

Keywords: Cybersecurity management, Data collection management, Digital transformation, Proactive actions.

1. Introduction

Nowadays, digital transformation is imperative for all businesses. Due to the variety of digital technologies that have been developed over time, which allowed for constant communication between objects and people as well as new methods of creating and processing data, the central paradigm of the digital transformation has emerged (Schneider & Kokshagina, 2020). Tang (2021) defines digital transformation as a type of business transformation that is driven by emerging technologies. According to González-Varona et al. (2021) digital transformation is a multifaceted phenomenon driven by technology that has an impact on society, politics, and economy and it causes market disruptions that call for strategic responses from businesses to stay competitive. Moreover, Vial (2019) discovers that the term "digital transformation" describes a process that aims to enhance an entity by bringing about major changes in its characteristics through a combination of information, computer, communication, and networking technologies.

In the most general approach, digital transformation refers to the introduction of digital technologies into all areas of a business, leading to major changes in the way the organization operates and delivers value to customers. Thus, the processes developed in digitally transformed organizations are based on technological support that, in addition to the facilities offered, can also create unpleasant problems that must be controlled and avoided. In this context, in the cybersecurity system, technology must be protected through various tools, procedures and measures that organizations must establish adequately.

In this context, the purpose of this paper is to present the impact of digital transformation on organizations, highlighting the specific details of management functions and cybersecurity requirements.

The present paper is structured in such a way as to address, on the one hand, the management functions in the context of digital transformation, and on the other hand, the focus is on the key areas of digital transformation, such as customers, competition, data, innovation, security. At the same time, the cybersecurity in task management is addressed in the paper, its particularities being highlighted.

The paper is organized as follows. Section 2 describes the main management functions in the digital environment and analyses the approaches of different authors, concerning the role of management in the digital context. Also, in this section, the main actions concerning cyber security protection, in the case of companies, is identified. The following section, Section 3, is dedicated to the most important components of digital transformation (customers, competitors, data, innovation, security) which are analysed in line with the tasks management (foresight, planning,

https://doi.org/10.24846/v32i1y202305

organizing, controlling, leading) and with the cyber security requirements and goals. Also, this section presents the data collection involved in the digital transformation and underlines that data collection about customers is the care of the entire digital process. The last section, Section 4, consists in providing the conclusions which present the main aspects that have to be taking into consideration in cyber security management process.

2. Management Functions in the Context of Digital Transformation

Digital transformation (or DT) refers to the use of digital technologies to fundamentally change how organizations operate and deliver value to their customers. Moreover, digital transformation is a phenomenon that impacts every aspect of human society, as noted by Kaplan et al. (2004). It compels companies and industries to undertake significant organizational changes and make critical adaptations to their business strategies in order to remain viable and successful (Porfírio et al., 2021).

The following section will focus on the key characteristics of digital transformation and management functions. This analysis considers the current context, which places greater emphasis on the impact of the pandemic on organizations. Before outlining these specific details, it is important to provide brief definitions of management functions to ensure a better understanding of the present research. Therefore, the management function refers to the primary activities that managers perform in order to achieve organizational goals (Fayol & Coubrough, 1930). The key management functions are: foresight, planning, organizing, leading, and controlling (Wood & Wood, 2002). These management functions are interrelated, and interdependent, and effective management requires a balanced approach to all.

Within the studies from the specialized literature, researchers do not agree that the first management function, which is organizational foresight, is a crucial element for achieving business success (Mahmoud et al., 2016). Despite this, organizational managers often overlook the importance of corporate foresight, leading to challenges in competitiveness (AlMujaini et al., 2021). Without effective organizational foresight, organizations may struggle to adapt to constantly evolving business environments and respond appropriately to external changes. As a result, according to Mahmoud et al. (2016), organizations are often lacking in innovation and experience stagnant growth.

Planning allows organizations not only to react to changes in their environment but also making their own changes, with impact on their environment (Popa et al., 2019). In the context of digital transformation, organizations must be able to adapt to rapidly changing business environments and technological advances (Schwertner, 2017). Forecasting can help organizations anticipate potential challenges and opportunities and make informed decisions about how to allocate resources to achieve their goals. Furthermore, effective forecasting in a digital context requires access to real-time data, advanced analytics tools, and expertise in emerging technologies (ElMadany et al., 2022). Using these tools and methods, organizations can make more accurate predictions about customer behavior, market trends, and industry developments. This, in turn, enables organizations to develop more effective strategies for innovation, growth, and competitiveness in the digital age (Caputo et al., 2021).

In terms of planning, according to Matt et al. (2015), digital transformation can help organizations gather and analyze data more effectively to make better-informed decisions. In the organizing function, digital transformation can help organizations streamline processes, automate repetitive tasks, and improve collaboration (Li, 2020). For example, cloud-based software tools can facilitate real-time collaboration and communication between team members regardless of their location.

The leading function of management can be enhanced through digital transformation, allowing managers to effectively engage with employees and customers through new digital channels such as Zoom, Teams, and more (Henderikx & Stoffers, 2022). With the increasing number of organizations that undergo digital transformation, it is becoming evident that the leading challenges extend beyond top management to all levels of management (Petry, 2018). Managing and guiding these technology-driven transformations requires new perspectives on leading (Henderikx & Stoffers, 2022). Once digital transformation is initiated, the role of the manager is to provide support for the ongoing process of digitalization

and to lead and manage the newly emerging digital organization (Klein, 2020).

In the controlling function, digital transformation can help organizations in real-time monitoring and measurement of their performance. Digital dashboards can track and analyze key performance indicators (KPIs), providing managers with current information about their organization's performance (Lanzolla et al., 2020).

Overall, digital transformation is a critical element of modern management practice, and organizations that are able to successfully leverage digital technologies will be better positioned to compete and succeed in today's fast-paced business environment (Zaki, 2019). The digital transformation of a company has to have a strategic approach and thus properly take into consideration the risk management, security and good project management of digital transformation.

Beside the general rules concerning the management of company, the digital transformation process has to have a strategic approach and it takes into consideration the digital risk management and cybersecurity protection. According to Li & Liu (2021), cybersecurity includes measures to protect information, data, and networks against internal or external threats.

The digital transformation impacts all key management functions, including foresight, planning, organizing, leading, and controlling (Wood & Wood, 2002). These management functions are interrelated and interdependent, and effective management requires a balanced approach to all. According to task management theory, each task has to be improved with specific procedures in line with cybersecurity protection.

In order to make a company more resilient one needs robust cybersecurity strategies that include the following principal goals:

- Determination of the areas to invest – technology, human resources, software, etc.
- Definition of what an organization considers to be threats, what the likely responses will be and the identification of the weaknesses.
- Identification of areas in the businesses that are reliant on third parties (the major risk areas for cybersecurity is third-party).
- Information and documentation on how it would recognize a security breach.

The investment in security tools and technology could protect but not necessarily prevent an attack. It is very important to invest in users' education and awareness to enable them to monitor, early detect and respond quickly to a breach. Every business and organization's infrastructure must take cybersecurity seriously because a business or organization that focuses on cybersecurity has a greater chance of success as it can better defend its customers' and employees' personal information from outside threats (Li & Liu, 2021).

Having a strong incident management plan, the company can prevent, control, detect, identify breach and build a cybersecurity system in line with its need. According to Oriola et al. (2021) incident handling and response services that aid in incident prevention are part of security incident management. The incident handling services comprise incident detection and reporting, correlation, categorization, prioritizing, assignment of events, and mitigation planning procedures (Oriola et al., 2021). The incident reaction entails the steps taken to stop or lessen an occurrence, coordinate and distribute information, and put follow-up plans into place (Oriola et al., 2021).

From the managerial point of view, these touch the foresight and planning/function task Figure 1 presents the management tasks for cyberattacks prevention.

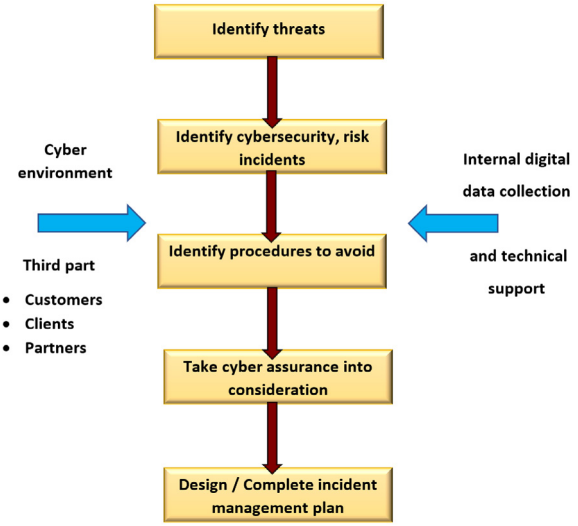

Figure 1. Management task – foresight and planning

The most frequent critical components of effective incident management touch the following aspects:

- Training the users to be able to identify a potential attack and know whom to inform.
- Having in place tools and technology to identify and prevent malware.
- Regular in place monitoring over systems and infrastructure.
- Control each task involved in security.
- Verify awareness of staff company.

It is very useful to implement a formal tested process for dealing with incidents and the way to prevent potential issues or get a response to solve it as quickly as possible.

3. Domains of Digital Transformation: Customers, Competition, Data, Innovation, Security

As Tata Mendez says: *"Digital Transformation is not only the production of content or services, but must be internal. It is a transversal work, nobody should have the crown, because they are all digital delegates. We need people who care about these issues and budgets that feed them"* (Defelipe, 2019).

The continuous introduction of new digital technologies to the market has motivated organizations to transform their businesses digitally. As a result, digital transformation has become a top management priority of significant strategic importance (Feroz et al., 2021). According to Rogers (2016), digital transformation has the potential to impact various domains of an organization, including customer experience, operations, data from the business model (competition and innovation level), and the value of an organization. Additionally, David Rogers (2016) argued that digital transformation is more than just technology. It is about rethinking the entire business model and it starts with understanding the customer. At the end of the day, digital transformation is a management issue, a management activity which should transform the organization into a digital one, matching the management functions with the digital requirements.

From the customer's perspective, digital transformation means providing a seamless, integrated experience across all touchpoints and channels, both online and offline. It means understanding the customer's needs and desires (Bosch & Olsson, 2021) and using data and analytics to personalize the experience (Rogers, 2016). According to Rogers (2016), organizations that are successful in digital transformation are those that place the customer at the center of their strategy and use digital technologies to enhance the customer's experience.

Organizations are striving to improve their product performance and customer experience by integrating new features and functionalities through the continuous digitization of their operations. As a result, there is a significant change in the way value is created, revenue is generated, and customer relationships and experiences are managed (Bosch & Olsson, 2021).

Also, it should be noted that digital transformation is enabling companies to gather vast amounts of data on their customers and their behaviors, which can be used to develop new business models and revenue streams (Rogers, 2016). This means that companies that are able to leverage their data effectively are likely to gain a significant competitive advantage over those that cannot (Stalmachova et al., 2022). Therefore, competition plays a significant role, since the digital landscape is constantly changing, and companies that fail to adapt and innovate run the risk of falling behind (Saarikko et al., 2020).

Additionally, according to Rogers (2016), it is important for organizations to recognize that their biggest competitors may not always be external but could come from within their own supply chain. This is particularly relevant in the context of digital transformation, as suppliers are increasingly able to use digital channels to reach customers directly. This creates a potential threat to the traditional relationship between organizations and their suppliers, as suppliers may be able to offer lower prices or other advantages to customers through direct access.

As it was presented above, all processes developed into digitally transformed company are based on technological support. This support offers facilities, but also a lot of unpleasant issues which have to be controlled and avoided. In cybersecurity system, the technology is protected though different tools, procedures and measures. Best practices seem to be a mix of well-defined techniques, software, and strategies:

- Keeping firewalls, operating systems, and virus engines up-to-date.

- Check the users' password and their rights.
- Passwords protecting the Wi-Fi.
- Take into consideration data scrubbing.
- Implement ITC general controls in depth.
- Formalize the incident management plan.
- Take into consideration cyber insurance.
- Check physical site controls.
- Review controls against social engineering generally.
- Conduct penetration testing regularly.

The components presented are divided among management functions, each of them being a characteristic for one specific, management function. Figure 2 illustrates the linking between the tasks and management functions: organizing and controlling. These tasks are strongly linked and a short breach into one can destroy the security of entire system.

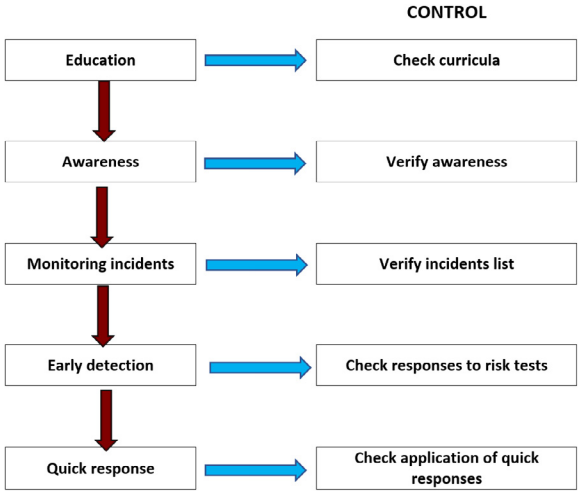

Figure 2. Management task – organizing and controlling

It is necessary to underline that there are many legal regulations (legal framework) on this domain, at national and international level. The cybersecurity system has respected this regulation and transformed it in security procedures accordingly. The most significant example is the EU's General Data Protection Regulation (GDPR). GDPR came into force in May 2018, and it is identified as the main factor in companies taking the first steps in cybersecurity. A special attention has to be paid to the private data about the clients/customers. The GDPR regulation has to be respected in a strict manner (Banciu et al., 2021). It demonstrated that the legal framework could have a strong influence on cyber protection. The providers of artificial intelligence (AI) software and the managers of AI systems can take example from this regulatory compliance point of view.

GDPR represents a model for companies helping them to better understanding the level of control they want to implement across the various business units in the cybersecurity domains. The model could be also adapted for protecting the business from data loss, unauthorized access, destruction of both financial and sensitive data collections also.

Figure 3 shows the linking among leading and control functions of management and tasks in cybersecurity control.

The same approach has to be applied in the public administration bodies. According to some authors' opinion, the control function of management is not enough developed in case of cyber security protection (Banciu et al., 2020).

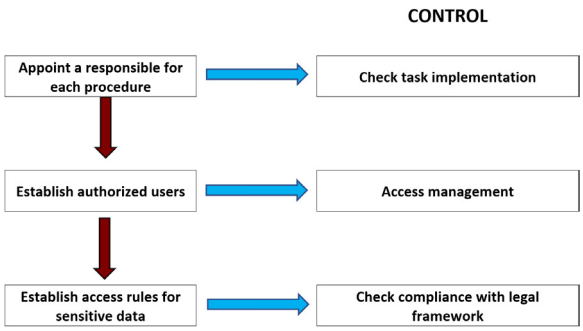

Figure 3. Management task – leading

The key issue in the digital transformation process of companies is represented by data. According to the modern approach in ICT domain and the European strategy for digitalization till 2030 (European Union, 2022), the most common support for data and software is the cloud system. The data protection in the cloud system requires specific rules and procedure.

The modern cloud architecture can accommodate thousands of data repositories and hundreds of collectors and applications that access the data. The companies are not taken care of the data security in the cloud system. This task is the task of cloud service providers. If the cloud is implemented into companies, as own ICT resource, the management must apply procedures similar to the ones that have already been presented in Figures 1-3. It has to be mentioned that the cloud represents the strongest protection for data collections (data bases, repositories) given by the software system.

The main data collection of the digitally transformed companies is presented in Figure 4. Data are linked each other through specific procedures so that the decision-makers have a strong support and a complex view of the companies in real-time and any time.

Figure 4. Data collection involved in digital transformation process

The components of security are taken care of by the cloud platforms for their managed database. The most usual components are:

- Database Management: the cloud provider is responsible for keeping each database solution up to date.
- Logging: cloud providers offer telemetry for both sides - network and database access.
- Access Controls: cloud providers taking over all the physical access protections and, in addition, help with basic security like access controls. If an organization has a central repository of identities and authorizations, it is the company's responsibility to link them into the cloud provider's systems.

A part of these functions is taken by DBaaS (also known as managed database service). It is offered by cloud platform and allows users to access and also to use a cloud database (IBM, 2023). Besides, the management has to apply the critical security controls (including detection and response) so as to protect data and comply with regulatory demands, if the case.

In order to secure and audit unstructured data in a cloud file repository the customer of the cloud service needs to deploy additional controls:

- Data discovery and classification. It is important and even required for most privacy regulations to discover all instances and files with sensitive information and classify them for their content.
- Access management. One example of best practice for each organization is applying for granular access, integrated with corporate policies and access management solutions;
- Enforcing policy. Based on those access controls, to prevent abuse from authorized users, the number of queries, or the amount of data to be downloaded can be limited;
- Anomaly detection alongside policy enforcement is the first line of defense for breach detection or improper usage discovery;
- Encryption. A cloud customer should have more control over encryption algorithms and key management.

Mayhew et al. (2016) state that organizational decision-making has been focused on big data, business analytics, and "smart" environments, as organizations try to find ways to derive valuable insights from data and improve their performance. Every department in a company relies on data as a vital component as it provides valuable insights and generates new value for the organization. With the advent of digital technologies, data have become more accessible and easier to collect, analyze, and interpret. This has enabled companies to make data-driven decisions and optimize their operations in real time (Rogers, 2016). Having access to database and repository of cloud the companies have to have a very closed dialog with the cloud providers in order to fit their internal regulation and procedure accordingly. This touches the organizing and leading management function in connection with control procedures.

The last domains of digital transformation are innovation and value which are deeply intertwined (Roger, 2016). The adoption of digital technologies has enabled organizations to approach innovation in a new way, one that emphasizes continuous learning and the creation of new value. By leveraging digital tools and platforms, companies can foster a culture of innovation that is built on experimentation, collaboration, and rapid iteration (Appio et al., 2021). The security of innovation becomes crucial for the company. The innovations are based on knowledge and data which are stored in a digital form. The results are also often available in a digital form. Innovation and value are key outcomes of digital transformation, and companies that are able to effectively harness the power of digital technologies can gain a significant competitive

advantage in today's rapidly evolving marketplace (Nambisan et al., 2019). For this reason, the procedures for security protection of innovative data and products are the responsibility of management, even if there are many sophisticated automated procedures given by software system. Without innovation, organizations risk falling behind their competitors and missing out on the many benefits that digital transformation can bring.

4. Conclusion

According to the most relevant works in the digital transformation domain, the whole process depends on managerial skills and performances and managerial understanding. Besides, the digital transformation operates with huge data collection both inside and outside companies.

Most of this data is sensitive because it could offer confidential information about the companies. This issue could provide useful information to the competitors, which can have a negative influence on the company's efficiency, losing some competitive advantages. Thus, cybersecurity must be well implemented by performing management tasks, in line with management functions.

Cybersecurity management must consider the following aspects:

- data collection and their classification according to their importance within the company;
- the access rights of users inside and outside the company;
- ensuring software/hardware investments dedicated to security;
- collaboration with cloud or external ICT providers, in order to fit the security procedures;
- to ensure staff training and awareness;
- to put the right people in charge of running each type of security procedure;
- to design a clear risk management plan, in case of incidents;
- collaboration with national and international bodies responsible for/regarding cybersecurity;
- involving companies' top management in decision making, concerning cybersecurity.

The result of the cooperation between the cybersecurity management and the general management of the company results in a digital transformation that can become a successful one or can compromise the entire business activity.

REFERENCES

AlMujaini, H., Hilmi, M., Abudaqa, A., & Alzahmi, R. (2021) Corporate foresight organizational learning and performance: The moderating role of digital transformation and the mediating role of innovation in SMEs. *International Journal of Data and Network Science*. 5(4), 703-712. doi: 10.5267/j.ijdns.2021.7.011.

Appio, F. P., Frattini, F., Petruzzelli, A. M. & Neirotti, P. (2021) Digital transformation and innovation management: A synthesis of existing research and an agenda for future studies. *Journal of Product Innovation Management.* 38(1), 4-20. doi: 10.1111/jpim.12562.

Banciu, D., Fodorean, D. & Cirnu, C. E. (2021) Cyber Security and Human Rights Considering the Metaverse. *Journal for Freedom of Conscience [Jurnalul Libertății de Conștiință]*. 9(2), 648-654.

Banciu, D., Rădoi, M. & Belloiu, S. (2020) Information Security Awareness in Romanian Public Administration: An Exploratory Case Study. *Studies in Informatics and Control*. 29(1), 121-129. doi: 10.24846/v29i1y202012.

Bosch, J. & Olsson, H. H. (2021) Digital for real: A multi-case study on the digital transformation of companies in the embedded systems domain. *Journal of Software: Evolution and Process.* 33(5), e2333. doi: 10.1002/smr.2333.

Caputo, A., Pizzi, S., Pellegrini, M. M. & Dabić, M. (2021) Digitalization and business models: Where are we going? A science map of the field. *Journal of Business Research.* 123, 489-501. doi: 10.1016/j.jbusres.2020.09.053.

Defelipe, S. (24 October, 2019) Libraries are not obsolete, this is how their Digital Transformation advances. *Impacto TIC.* https://impactotic.co/en/the-digital-transformation-of-libraries/ [Accessed 20th February 2023].

ElMadany, H., Alfonse, M., & Aref, M. (2022) Forecasting in Enterprise Resource Planning (ERP) Systems: A Survey. In: Magdi, D. A., Helmy, Y. K., Mamdouh, M., Joshi, A. (eds.) *Digital Transformation Technology. Lecture Notes in Networks and Systems*. (volume 224) Singapore, Springer Nature. doi: 10.1007/978-981-16-2275-5_24.

European Union. (2022) *Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030*. https://eur-lex.europa.eu/eli/dec/2022/2481/oj [Accessed 20th February 2023].

Fayol, H. & Coubrough, J. A. (1930) *Industrial and general administration*. London, Sir I. Pitman & Sons, Ltd.

Feroz, A. K., Zo, H. & Chiravuri, A. (2021) Digital Transformation and Environmental Sustainability: A Review and Research Agenda. *Sustainability*. 13(3), 1530. doi: 10.3390/su13031530.

González-Varona, J. M., López-Paredes, A., Poza, D. & Acebes, F. (2021) Building and development of an organizational competence for digital transformation in SMEs. *Journal of Industrial Engineering and Management*. 14(1), 15-24. doi: 10.3926/jiem.3279.

Henderikx, M. & Stoffers, J. (2022) An exploratory literature study into digital transformation and leadership: Toward future-proof middle managers. *Sustainability*. 14(2), 687. doi: 10.3390/su14020687.

IBM. (2023) *What is Database-as-a-Service (DBaaS)?*. https://www.ibm.com/topics/dbaas [Accessed 20th February 2023].

Kaplan, B., Truex, D. P., Wastell, D., Wood-Harper, A. T. & DeGross, J. I. (eds.). (2004) *Information Systems Research: Relevant Theory and Informed Practice*. Boston, Kluwer, Academic Publisher.

Klein, M. (2020). Leadership characteristics in the era of digital transformation. *Business and Management Studies: An International Journal*. 8(1), 883-902. doi: 10.15295/bmij.v8i1.1441.

Lanzolla, G., Lorenz, A., Miron-Spektor, E., Schilling, M., Solinas, G. & Tucci, C. L. (2020) Digital Transformation: What is new if anything? Emerging patterns and management research. *Academy of Management Discoveries.* 6(3), 341-350. doi: 10.5465/amd.2018.0103.

Li, F. (2020) Leading digital transformation: three emerging approaches for managing the transition. *International Journal of Operations & Production Management.* 40(6), 809-817. doi: 10.1108/IJOPM-04-2020-0202.

Li, Y. & Liu, Q. (2021) A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 7(8), 8176-8186. doi: 10.1016/j.egyr.2021.08.126.

Mahmoud, M. A., Blankson, C., Owusu-Frimpong, N., Nwankwo, S. & Trang, T. P. (2016) Market orientation, learning orientation and business performance: The Mediating Role of innovation. *International Journal of Bank Marketing.* 34(5), 623-648. doi: 10.1108/IJBM-04-2015-0057.

Matt, C., Hess, T. & Benlian, A. (2015) Digital transformation strategies. *Business & Information Systems Engineering.* 57, 339-343. doi: 10.1007/s12599-015-0401-5.

Mayhew, H., Saleh, T. & Williams, S. (2016) Making data analytics work for you – instead of the other way around. *McKinsey Quarterly.* 4, 29-41.

Nambisan, S., Wright, M. & Feldman, M. (2019) The digital transformation of innovation and entrepreneurship: Progress, challenges, and key themes. *Research Policy.* 48(8), 103773. doi: 10.1016/j.respol.2019.03.018.

Oriola, O., Adeyemo, A. B., Papadaki, M. & Kotzé, E. (2021) A collaborative approach for national cybersecurity incident management. *Information & Computer Security*. 29(3), 457-484. doi: 10.1108/ICS-02-2020-0027.

Petry, T. (2018) Digital leadership. In: North, K., Maier, R. & Haas, O. (eds.) *Knowledge Management in Digital Change*. Switzerland, Springer: Cham, pp. 209-218.

Popa, Ș. C., Simion, C. P., Ștefan, S. C. & Albu, C. F. (2019) Strategy: A Big Challenge for a Small Business. Evidences from North-East Romanian SMEs. *Economic Computation and Economic Cybernetics Studies and Research.* 53(3), 169-186. doi: 10.24818/18423264/53.3.19.10.

Porfírio, J. A., Carrilho, T., Felício, J. A. & Jardim, J. (2021) Leadership characteristics and digital transformation. *Journal of Business Research*. 124(C), 610-619. doi: 10.1016/j.jbusres.2020.10.058.

Rogers, D. L. (2016) *The Digital Transformation Playbook: Rethink Your Business for the Digital Age*. New York, USA, Columbia University Press.

Saarikko, T., Westergren, U. H. & Blomquist, T. (2020) Digital Transformation: Five recommendations for the digitally conscious firm. *Business Horizons*. 63(6), 825-839. doi: 10.1016/j.bushor.2020.07.005.

Schneider, S. & Kokshagina, O. (2020) Digital transformation: What we have learned (thus far) and what is next. *Creativity and Innovation Management*. 30(2), 384-411. doi: 10.1111/caim.12414.

Schwertner, K. (2017) Digital transformation of business. *Trakia Journal of Sciences*. 15(1), 388-393. doi: 10.15547/tjs.2017.s.01.065.

Stalmachova, K., Chinoracky, R. & Strenitzerova, M. (2022) Changes in Business Models Caused by Digital Transformation and the COVID-19 Pandemic and Possibilities of Their Measurement – Case Study. *Sustainability*. 14(1), 127. doi: 10.3390/su14010127.

Tang, D. (2021) What is digital transformation?. *EDPAC.* 64(1), 9-13. doi: 10.1080/07366981.2020.1847813.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems.* 28(2), 118-144. doi: 10.1016/j.jsis.2019.01.003.

Wood, J. C. & Wood, M. C. (eds.). (2002) *Henri Fayol: Critical Evaluations in Business and Management.* (2nd volume) London & New York, Taylor & Francis.

Zaki, M. (2019) Digital transformation: harnessing digital technologies for the next generation of services. *Journal of Services Marketing*. 33(4), 429-435. doi: 10.1108/JSM-01-2019-0034.