European Research Studies Journal
Volume XXV, Issue 4, 2022

pp. 215-223

The Impact of Dynamic Capabilities and Competences of Employees on the Digital Security of Small and Medium-Sized Enterprises

Submitted 06/11/22, 1st revision 23/11/22, 2nd revision 20/12/22, accepted 30/12/22

Wiesław Danielak[1]

Abstract:

Purpose: *The aim of the article is to show the impact of the dynamic capabilities and competences of employees as a mechanism that generates the digital security of the enterprise.*
Design/methodology/approach: *The methods used in the study include literature analysis as well as the selection and synthesis of secondary and primary empirical source materials. A proprietary questionnaire was used to obtain the primary data. 107 managers and employees of small and medium-sized enterprises in Poland participated in the survey. The obtained data was subjected to statistical analysis and conclusions from the research were developed. The study is theoretical and empirical in nature.*
Findings: *The study revealed the main effects of digital technology on the digital security of the enterprise. Competences and dynamic capabilities of employees play a key role in managing the company's digital security. Research shows that employees have a diverse range of competencies and dynamic capabilities in the field of digital security. They are able to recognize, react and assimilate information related to threats to varying degrees. Also take the initiative in the event of threats.*
Practical implications: *Those enterprises that have greater competencies and dynamic capabilities of employees more often take actions for safety. The low level of digital competence of employees increases their uncertainty in solving problems with digital technologies.*
Originality/Value: *This study identifies the main effects of digital technology on the digital security of the enterprise. The results of the study can provide knowledge to managers and employees about the impact of the competencies and dynamic capabilities of employees on managing the digital security of the enterprise.*

Keywords: *Dynamic capabilities, digital competences of employees, digital security of the enterprise.*

JEL Classification: *D22, D81, D83, M54.*

Paper Type: *Research study.*

[1]*Professor, Institute of Management and Quality Sciences, Department of Strategic Management and Marketing, University of Zielona Góra, Poland,*
ORCID 0000-0002-7319-6847, e-mail: w.danielak@wez.uz.zgora.pl;

1. Introduction

Modern technologies have a key impact on the long-term development of the enterprise as well as markets and industries. Digitization has become a strategic tool for the continuous development of companies around the world (Sehlin, Truedsson, and Cronemyr, 2019).

Due to the fact that with the development of modern technologies, the danger of cyberattacks increases, managers and employees should have competences and dynamic capabilities to recognize, react and counteract threats. Effective management of digital security requires cooperation between managers, specialists and employees using modern technologies.

The aim of the article is to show the impact of the dynamic capabilities and competences of employees as a mechanism that generates digital security for small and medium-sized enterprises.

2. The Impact of Digital Transformation on Business

As a result of changes in the environment, the approach of entrepreneurs and managers to the implementation of solutions related to digital transformation has been changed. Digital transformation is about the acquisition of technology and the absorption of digital knowledge to enrich and increase the value creation opportunities for the customer and company stakeholders (Schiuma *et al.*, 2022).

Digital transformation accelerated during the COVID-19 pandemic, where many enterprises had to increase their digital capabilities to ensure business continuity. Suddenly it turned out that it is necessary to run own business more digitally, sell online, communicate and work remotely. Employees had to acquire digital and IT skills in a short time to perform tasks in the conditions of the pandemic.

Under the influence of digital transformation, the way of managing the enterprise has changed. The ability to use digital technologies to communicate, manage relationships with customers, suppliers, employees and other stakeholders has gained in importance.

Digital technologies influence the diversification of products and new technological competences (Neirotti, Raguseo, and Paolucci, 2018). New technologies, which are more and more widely used, change the rules of market competition, lead to building new business models and change the ways of generating and delivering value to customers. According to research by Krstić *et al.* (2022), digital business transformation is a prerequisite for the survival of organizations and they must adapt to changes at the pace at which new technologies emerge.

The Internet has a huge impact on the pace and dynamics of competition, lifestyles, customer relationships and technological innovation (Lányi, Hornyák, and Kruzslicz, 2021). The digital technology adopted by the organization increases the ability to positively respond to customer needs, improves customer-side activities, helps increase sales and efficiency by reducing costs (Foroudi *et al.*, 2017). Internet solutions support the improvement of the quality and speed of transactions and communication (Li *et al.*, 2018; Olvera-Lobo and Casrillo-Rodriguez, 2018).

3. The Use of Digital Technologies in the Activities of Enterprises in Poland

According to the data of the Central Statistical Office, there are 2.26 million enterprises in Poland. The overwhelming majority are small and medium-sized enterprises (99.8%). Micro-enterprises dominate (97.0%), small enterprises account for 2.2% and medium-sized enterprises – 0.6%, and large enterprises – only 0.2%. They run services (52.9%), trade (21.6%), construction (15.4%) and industry (10.0%). The share of enterprises in creating the GDP product is 72.3%.

In Poland, in 2017-2021, as many as 98.5% of enterprises had access to broadband Internet. 71.4% of enterprises had their own website. As many as 78.3% of enterprises equip employees with mobile devices (applications for smartphones and tablets) enabling mobile access to the Internet.

In the group of small and medium-sized enterprises, 52% use digital technologies. In the European Union, the average is 60%. In 2020, the percentage of enterprises conducting electronic sales was 17.9%. Online sales were most often conducted by large enterprises (44%), rather than medium-sized enterprises (22%) and small enterprises (16%).

In 2021, almost every second enterprise used social media (45.6%). They were most popular in the group of large companies (77.7%), then medium-sized (57.9%) and small (42.0%). In 2021, 28.7% of Polish enterprises used paid cloud computing services. Mainly large (69.7%) than small enterprises (24.4%). The most common purchases were e-mail (22.6%), office software (18.3%), enterprise file storage (11.8%) and financial software (8.6%).

In 2021, 18.7% of enterprises used Internet of Things devices or systems. Digital technologies were most often used in logistics (11.5%), to secure premises (11.3%), to control machines and vehicles (6%) and to optimize energy consumption (4.8%). Only 2.9% of enterprises used Artificial Intelligence technologies.

According to research by Krstić, Rejman-Petrović, Nedeljković, and Mimović, (2022), there is relatively low efficiency of using digital potential in business. Therefore, there is a need for a better understanding of the essence and goals of the digital business transformation process by employees and management in order to

create conditions for the efficient implementation and optimization of business digitization.

4. Threats Related to the Digital Security of the Enterprise

Digitization is one of the most dynamic changes nowadays. It gives new opportunities for improvement and development of enterprises and brings with it uncertainty and threats related to the digital security of enterprises. With the development of networks of information and communication systems, the number of attacks and external threats increases.

A cyber threat is any potential circumstance, event or activity that may cause damage, cause disruption or otherwise adversely affect the operation of networks and information systems and users (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, access: 18/11/2022).

The most popular threats in cyberspace include malicious software (malware), sending spam, blocking access to services, scanning the network, ports (scanning), sending fake e-mails and text messages usually with a malicious link, spoofing. Social engineering attacks are also dangerous, where scammers often send messages on behalf of banks or well-known companies and stores, thus counting on the credulity of customers. It is necessary to remember that such institutions never ask for confidential data by e-mail or SMS.

Activity in the digital world is associated with the need to use security measures against cyber threats. When using banking applications, shopping online or using social media, it is necessary to be careful and remember about the safety rules. Banks offer additional security in the form of customer behavioural profiles.

Enterprises are exposed to hacking into their systems, attempts to phishing data or infecting their devices with viruses. They must be aware that they will be exposed to attacks carried out using new methods such as, Phishing and Pharming, Ransomware, Juice Jacking, Clickjacking, Man in the middle or viruses and bots.

To guarantee the digital security of the organization, every employee should be involved in this process. Cybersecurity is the resistance of ICT systems to actions that violate the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data, or related services offered or available through these networks and IT systems (Czyżak, 2018, p. 106).

Cybersecurity management comes down primarily to making decisions in the area of applied security, monitoring security and responding to cyberattacks. Therefore, the right leadership style is essential for decision-making and the promotion and dissemination of digital culture throughout the organization (Schiuma *et al.*, 2022).

According to research conducted by kpmg.pl in June 2022, 89% of Polish enterprises monitor their security. 78% respond to cyberattacks, 47% test their infrastructure for cyberattacks and implement cyberthreat awareness programs (44%).

5. Using the Dynamic Capabilities and Competences of Employees in the Company's Digital Security

A manifestation of dynamic capabilities is the ability to quickly respond to changes in the environment. Dynamic capabilities include the ability to detect, integrate and transform opportunities and threats (Teece, 2007; Lu *et al.,* 2018). Dynamic capabilities refer to the development, implementation and protection of a combination of resources and competencies (Ellström *et al.,* 2022). They determine the company's ability to reconfigure internal and external resources and competencies in response to the rapidly changing environment (Teece, 2012).

Dynamic capabilities allow quickly responding to unfavourable phenomena in the environment. They allow reacting to technological changes and changing customer expectations. Dynamic capabilities provide a consistent approach to digital transformation due to the high impact of digital technologies on business (Warner and Wäger, 2019). The use of dynamic capabilities of employees should bring benefits from the skilful management of resources and competencies at the disposal of the company as well as resources and competencies existing in the environment.

Both the company's strategy and goals must be flexible and adapt to new opportunities (Ellström *et al.,* 2022). Companies often sense opportunities but then fail to take advantage of them for a variety of reasons, such as lack of commitment, risk aversion, or financial considerations (Teece, 2007). To overcome such shortcomings, companies need to refine policies and procedures, strengthen their leadership, and refine their strategies to understand, capture, and evaluate potential business opportunities (Teece, 2007).

Companies lack knowledge about Industry 4.0 technologies, so they should support actions to improve qualifications to enable employees to use the potential of new technologies (Pirola, Cimini, and Pinto, 2020). It is important to improve the competence of employees in terms of acquiring new skills and knowledge about the programs, applications and tools necessary to perform digital tasks. Enterprises should strengthen the IT competences of employees. With many services now moving online, the need for cybersecurity and data protection training has increased.

6. The Description of Test Results

The survey was conducted in December 2022 in Poland. 107 respondents were surveyed, who are responsible for issues related to digitization in their companies.

They were managers, specialists and employees. 57 small and 50 medium-sized enterprises participated in the research. Due to the sector of activity, service enterprises dominated, followed by production and trade enterprises. They were active in the construction, energy, real estate, municipal services, automotive, media and communication, as well as logistics and transport sectors.

The aim of the study was to identify the factors ensuring the digital security of the enterprise. Most of the respondents admitted that securing IT data in the company was important (79.5% of answers yes and 20.4% rather yes). IT resources in the company are well protected (69% of medium-sized and 49% of small companies).

Threats resulting from cybercrime are monitored more often in medium-sized companies (74% of medium-sized and 43% of small companies). In most cases, companies employ IT specialists who care about digital security (71% of medium-sized and 39% of small companies). Medium-sized companies use the services of external entities specialized in this field more often than small ones.

Competences and dynamic capabilities of IT specialists and properly trained employees play a key role in managing the company's digital security. The respondents admitted that each of the employees took care of cybersecurity, and 12% stated that they did not know who took care of cybersecurity in the company.

Most of the respondents admitted that there was a cyberattack in their company in the last 3 years (68% of medium-sized and 59% of small companies). However, those surveyed were unable to determine whether this was a damaging incident. Only 18% of respondents indicated that they had not experienced a cyberattack.

Most of the respondents admitted that they knew who to notify in the event of a cyberattack. Only 11% did not have such knowledge. Typically, employees keep their superiors informed of cyberattacks on an ongoing basis.

When asked if employees experienced a cyberattack while working remotely, the vast majority indicated that they had not experienced such incidents. Over 30% of respondents in medium-sized and 46% in small businesses have experienced mobile phone hacking. The respondents indicated that they most often received text messages urging them to provide logins and passwords to bank accounts, make payments for a courier package and a request to complete or update customer data.

Data backups are used for security purposes in the enterprise. The majority of respondents (82%) admitted that backups were used. Only 9% of respondents indicated that they were not used, and 5% had no knowledge. The majority of respondents admitted that they did not use logging and alerting systems for security purposes (58% of medium-sized and 79% of small companies). About 12% of respondents have never heard of such systems, and according to 5% there is no such need.

In the surveyed enterprises, disk and device encryption is not used too often for security purposes. Only 15% of medium-sized companies use encryption. There was a large discrepancy among the respondents as to their knowledge about the frequency of updated antivirus software. The question I do not know when the update is made was answered by as many as 29% of medium-sized and 65% of small companies surveyed.

The majority of respondents admitted that they used 91% antivirus protection in the enterprise. This is the basic form of protection against cyberattacks. As many as 72% of respondents from medium-sized companies admitted that they used cloud computing. In small companies, 49% do not see such a need, and 12% have no knowledge.

Respondents were asked to indicate the reasons for the lack of an appropriate approach to cybersecurity issues in the enterprise. According to them, the biggest challenge is the cost of implementation – 42%, followed by the lack of time to implement procedures – 39%. Equally important are the insufficient financial resources (21%) and the lack of staff with the necessary knowledge (12%). Only 4% said digital threats were not a significant risk to their business. None of the respondents showed low awareness of this issue.

7. Summary

Enterprises in Poland are increasingly implementing modern technologies, which increases their innovativeness and gives them greater development opportunities. Entrepreneurs and managers are aware of many risks associated with the use of digital technologies. Cybersecurity is one of the biggest challenges facing enterprises today.

The competencies and dynamic capabilities of employees play a key role in managing the digital security of the enterprise. Employees have a diverse range of competencies and dynamic capabilities in the field of digital security. They are able to recognize, react and assimilate information related to threats to varying degrees. Also take the initiative in the event of threats. Those enterprises that have greater competencies and dynamic capabilities of employees more often take actions for safety.

The low level of digital competence of employees increases their uncertainty in solving problems with digital technologies. Therefore, it is expected that improving the digital competences of employees will contribute to the development of work processes and increase the sense of security.

The most important task is to raise employees' awareness of the company's cyber security through appropriate training. Improving the dynamic capabilities of employees to adapt to changes in the environment and develop their digital

competences can reduce the perception of uncertainty in the digital security of enterprises. Enterprises must ensure the development of digital competences of employees and educate them about new cyber threats emerging in communication and everyday work.

References:

Czyżak, M. 2018. Bezpieczeństwo w Cyberprzestrzeni. Urząd Komunikacji Elektronicznej Polska. Teka Kom. Praw. OL PAN. T. XI, 2018, 2, 101–120.

Ellström, D., Holtström, J., Berg, E., Josefsson, C. 2022. Dynamic capabilities for digital transformation. Journal of Strategy and Management, 15(2), 272-286. https://doi.org/10.1108/JSMA-04-2021-0089.

Foroudi, P., Gupta, S., Nazarian, A., Duda, M. 2017. Digital technology and marketing management capability: achieving growth in SMEs. Qualitative Market Research, 20(2), 230-246. https://doi.org/10.1108/QMR-01-2017-0014.

Krstić, A., Rejman-Petrović, D., Nedeljković, I., Mimović, P. 2022. Efficiency of the use of information and communication technologies as a determinant of the digital business transformation process. Benchmarking: An International Journal. https://doi.org/10.1108/BIJ-07-2022-0439.

Lányi, B., Hornyák, M., Kruzslicz, F. 2021. The effect of online activity on SMEs' competitiveness. Competitiveness Review, 31(3), 477-496. https://doi.org/10.1108/CR-01-2020-0022.

Li, L., Su, F., Zhang, W., Mao, J.Y. 2018. Digital transformation by SME entrepreneurs: a capability perspective. Information Systems Journal, 28(6), 1129-1157.

Lu, Qicheng, Liang, Linlin, Jia, Fei, 2018. How Strategic Learning Impacts Organizational Innovation: Based on a Dynamic Capability Perspective. Journal of Management World, 34(9), 109-129.

Monitor transformacji cyfrowej biznesu, czerwiec 2022, Monitor-Transformacji-Cyfrowej-Biznesu-2022.pdf.

Neirotti, P., Raguseo, E., Paolucci, E. 2018. How SMEs develop ICT-based capabilities in response to their environment: Past evidence and implications for the uptake of the new ICT paradigm. Journal of Enterprise Information Management, 31(1), 10-37. https://doi.org/10.1108/JEIM-09-2016-0158.

Olvera-Lobo, M.D., Castillo-Rodríguez, C. 2018. Dissemination of Spanish SME information through web 2.0 tools. Journal of Transnational Management, 23(4). https://doi.org/10.1080/15475778.2018.1509422.

Pirola, F., Cimini, C., Pinto, R. 2020. Digital readiness assessment of Italian SMEs: a case-study research. Journal of Manufacturing Technology Management, 31(5), 1045-1083. https://doi.org/10.1108/JMTM-09-2018-0305.

Raport Głównego Urzędu Statystycznego. Społeczeństwo informacyjne w Polsce w 2021 r, GUS Warszawa 2021. Poland.

Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce w 2022 roku. Polska Agencja Rozwoju Przedsiębiorczości. Warszawa 2022, Raport-o-stanie-sektora-maych-i-rednich-przedsibiorstw_13_10_2022.pdf.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019.

Sehlin, D., Truedsson, M., Cronemyr, P. 2019. A conceptual cooperative model designed for processes, digitalisation and innovation. International Journal of Quality and Service Sciences, 11(4), 504-522. https://doi.org/10.1108/IJQSS-02-2019-0028.

Schiuma, G., Schettini, E., Santarsiero, F., Carlucci, D. 2022. The transformative leadership compass: six competencies for digital transformation entrepreneurship. International Journal of Entrepreneurial Behavior & Research, 28(5), 1273-1291. https://doi.org/10.1108/IJEBR-01-2021-0087.

Teece, D.J. 2007. Explicating dynamic capabilities: the nature and micro-foundations of (sustainable) enterprise performance. Strategic Management Journal, 28(13), 1319-1350.

Teece, D.J. 2012. Dynamic capabilities: routines versus entrepreneurial action. Journal of Management Studies, 49(8), 1395-1401.

Warner, K.S.R., Wäger, M. 2019. Building dynamic capabilities for digital transformation: an ongoing process of strategic renewal. Long Range Planning, 52(3), 326-349.