



Major Risks and Consequences of Corporate Sector Digitalization

Elnur Mekhdiev^{a,*} , Elizaveta Sokolova^b , Igbal Guliev^c ,
Parvana Mammadova^d 

a. Center for Analysis, Risk Management and Internal Control in Digital Space, Financial University under the Government of the Russian Federation, Moscow, Russia.

b. Department of State and Municipal Administration, Financial University under the Government of the Russian Federation, Moscow, Russia.

c. International Institute of Energy Policy and Diplomacy, MGIMO University, Moscow, Russia.

d. Department of Industrial Economics and Management, Azerbaijan Technical University, Baku, Azerbaijan Republic.

* Corresponding Author, E-mail: e.mekhdiev@gmail.com

Article Info

Article Type: Research Article

Article History:

Received: 28 March 2021

Received in revised form: 12 June 2021

Accepted: 26 July 2021

Published online: 01 July 2023

Keywords:

Digitalization,

Risks,

Consequences,

Smes,

Corporate Sector,

Social Risks.

JEL Classification:

G32, M10, O16, D81.

ABSTRACT

Nowadays, digitalization and its risks are in the focus of the researchers' and the corporate sector's attention, as they represent a new economic and technological frontier. It is extremely important for the corporate sector to formulate approaches to identifying the digitalization risks and financing sources to reduce them. The other important issue is the question on whether the modern society can survive the shocks of the digital era, and stay free – the authors forecast where will the process of total digitalization (in corporate sector first of all) lead the modern society. This research is dedicated to this spectrum of tasks. The main article's focus is to identify the digitalization's generalized risks and to formulate the enterprise's primary steps, which are effective in the transition to a digital business model. At the same time, the other important result is the estimation of the social and public effect of digitalization and formulation of the ways of declining the emerging risks. Within the research, the main results are the proof that the digitalization risks and benefits are the different degrees of the same results; the identification and systematization of the digitalization basic risks for the corporate sector and the development of universal basic steps to start the enterprise's business model transforming in the context of digitalization.

Cite this article: Mekhdiev, E., Sokolova, E., Guliev, I., & Mammadova, P. (2023). Major Risks and Consequences of Corporate Sector Digitalization. *Iranian Economic Review*, 27(2), 561-582. DOI: <https://doi.org/10.22059/ier.2021.83910>



©Author(s).

Publisher: University of Tehran Press.

DOI: <https://doi.org/10.22059/ier.2021.83910>

1. Introduction

In the whole, digitalization is seen as a complex process, which includes a number of incompletely defined components; each component represents a separate area of research. Today, there is no single digitalization definition; there is no also a single approach to the risks and benefits which are brought by digitalization. One of the key problems which form such effect consists in digitalization is a process involving all economic actors. Within this research, the focus will be on the corporate sector.

Digitalization concerns both large enterprises and small and medium-sized businesses (SMEs), because today digital enterprise is one of the company's competitiveness' elements in the whole (Digitalization and Corporate Strategy, 2018). A separate element of the digitalization research is the risks, which it brings to the companies' activities. This approach allows identifying sectors of the economy and population's social life, in which changes are necessary to mitigate the digitalization negative effects.

The other important issue discussed is the future of the digital sector. Today the scope of penetration of digital technologies in our everyday life is growing fast. The aim of big corporations' today changes – they seek gaining information about customers in addition to profits. This leads to the significant risks for both corporate sector and for people (Yuval Noah Harari, 2018). In this regard, the estimation of these risks and methods of their compensation is a very significant task.

Within the article, the authors set the goal to develop a new attitude towards risks for corporate sector in the digital era, and to highlight digital economy's advantages; these advantages use will allow companies to compensate for the increasing costs for covering risks. The research has a wide gap and aims at any company, which seeks its path in the digitalizing world. In order to narrow the research gap, the major recommendations and research will be conducted based on data

for bigger companies. The problem the authors seek to solve is the absence of balance between the need for data and the ability to protect it. The authors seek to find balance between the new technologies, providing risks for people and the conservative attitude, which limits the possibilities for tight interaction with digital sphere, but allows preserving personal data.

2. Literature Review

Corporate sector is the pioneer of digitalization in economy – it is the first to try to cut down the risks through the introduction of digital technologies and innovations. Hence, it's the first to encounter the risks digitalization bears. The interesting work focuses on the interconnection of digitalization and business models, proving that digital society provides specific business models, which should exist in nearly any company (Rachinger et al. 2019). The works on the risks in the digital era are numerous (Saptarshi Ganguly et al., 2017), for instance, depict the current situation and offer solutions for the corporate sector in order to cut down the risks. Another article (Navindu Harishchandra, 2019) researches concrete aspects of digitalization, namely goodwill, and the idea of brand image through digital media interpretation is very important for the digital risks estimation, but this works offer a wider approach to the digital risks. All the mentioned articles are aimed primarily on the big companies, while (Khanboubi and Boulmakoul, 2018) offers a broader approach and analyses the needed changes in the risk management as the sphere of economy. The second approach is closer to the one, used in this article. The other important is the OECD report (OECD, 2018), which provides a comprehensive analysis of the risks of digitalization in the global economy. The practical aspect is covered in (Päivi Parviainen et al., 2017), and it comprises the ideas of the risk management transformation and new risks arising, so it provides a firm basis for this paper.

The data-enabled growth is depicted in, (Ritter, et al. 2020), where the authors prove, that a company today has no option but to go digital. Moreover, the current situation with the COVID-2019 pandemic has influenced the digitalization pace, the rapid growth of it is proved in (Mandviwalla and Flanagan, 2021), moreover, big companies tend to go digital slower than the small ones. The digital responses of the SMEs to crisis are depicted in (Guo et al., 2020), but none of the mentioned articles concentrates on risks of digitalization process. The other article (Härmand, 2021) lacks the same moment, but proposes an important conclusion: the companies can transfer nearly all business processes in the digital sphere.

Taking all the mentioned into account, the contribution of this paper comprises from the new approach to assessing the effectiveness of the spending on cybersecurity and risk management, which has not been mentioned in the previous works. In addition to that, the paper provides a basis for the further research in the sphere of digital risks, especially in the direction of SMEs in the cyber risks environment.

3. Methodology

Within the article, the definition of the digitalization term seems to be a significant issue, gives four term's definitions from various sources, the authors are inclined to believe that the most accurate definition is "the digitalization is the process by which companies reorganize their work methods and strategies to obtain greater benefits thanks to the implementation of new technologies". It includes both household and technical process' components, while the other definitions highlight only one side.

To assess the corporate sector's risks, the authors turn to well-known companies, taking part in evaluating of the corporate sector's activities: Deloitte, Ernst and Young, McKinsey. Reports' analysis of these companies allows us to create generally accepted approaches to the risks of digitalization. Then, the authors assess the possibility of

the digitalization risks avoiding: the closed information space creation by the company and statistical estimation of the largest social networks use show that company's isolation is impossible in the digital age. The authors then conduct a similar analysis for SMEs. The analysis result is the identification of a risks compact system for enterprises from digitalization, which includes the most relevant risks, and the digitalization benefits, arising from these risks.

The authors also evaluate the companies' willingness to fight with the identified risks and to invest in information protection; to realize this estimate the authors compare growth rates of the cybersecurity costs and the growth in the number of enterprises in OECD countries. The OECD countries' sample is the most representative, as it includes both developed and developing countries. Taking into account the identified trends, the authors develop a system of recommendations for the company's softest transition to a digital development model.

The authors use autoregressive models and Excel functions in order to forecast the general trend of the development of ICT sector. The authors suggest using the following index for the estimation of the sufficiency of the spending on the cybersecurity:

$$Index = \left(\frac{\Delta Spendings}{\Delta ICTGrowth} + \frac{\Delta Spendings}{\Delta Cybersecurity breakages} + \frac{\Delta ICTShare}{\Delta ICTGrowth} \right) / 3$$

where Spendings – spending on cybersecurity, ICTGrowth – trade in ICT services in dollars, ICTShare – share of ICT trade of total trade in services, Cybersecurity breakages – harm done by the cybercrimes. This index will allow to estimate whether the economic agents append enough on cybersecurity and whether they spend effectively. If the value of the index is higher than 1, the spending is sufficient and efficient, if it equals to 1, or is near this value, every component is estimated by itself: the first fraction stands for sufficiency, the second for efficiency, the third for the correction of sufficiency (during the

calculation of sufficiency it's necessary to divide the first fraction on the third fraction) – if the result of the fraction is higher than 1, the component is sufficient/efficient, vice-versa is true too.

4. The Risks Digitalization Bears for The Corporate Sector

Digitalization and its risks are described in detail in numerous reports by international rating agencies and organizations (UNCTAD, 2019). In fact, we are talking about the transforming process of the companies' business model to ensure the fastest possible interaction with the client and to receive the largest possible amount of information about the client and his preferences. The paradigm of the manufacturer's main questions is changing, we mean such questions as what, for whom, when (Rachinger et al., 2019), as the digitalization and new high production automation technologies (which is, in fact, digitalization's part) allow to produce goods in a short time and deliver them to the client almost anywhere.

Changing in the business model causes a change in the enterprise's risk system. Deloitte identifies ten main areas of risks (Managing Risk in Digital Transformation, 2018); this reflects the company's approach completeness. But today the main risks are still the risks to personal data and the risks of gaining unauthorized access to company information. Thus, risks connected with the product and information are the most noticeable (technological risks are in some ways futuristic today; there are no any companies which have transferred their goods production and distribution to a digitalization level when it can change the production or sales chain, in order to cause financial harm to the company) (OECD, 2018). In a situation when information becomes the main risk source, it is necessary to take measures to protect it in open space or in isolation. Taking into account, the statistics of information use by customers and new ways of its spread through social networks, isolation does not look like a good enough option for the enterprise (Figure 1).

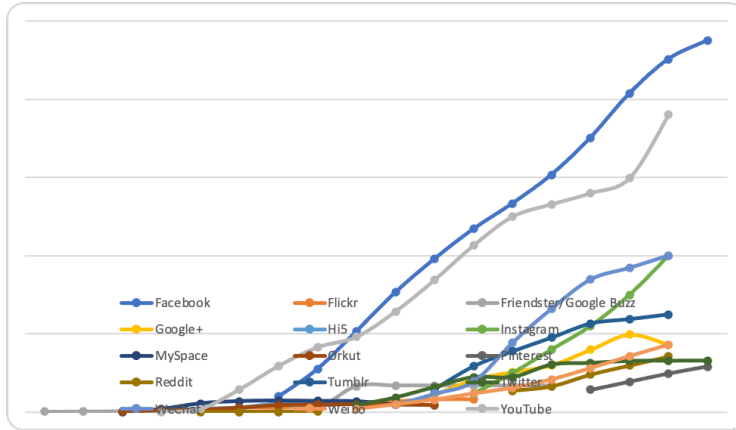


Figure 1. The Number of Social Networks Users

Source: Roser (2015) and outworldindata

Figure 1 demonstrates the possibilities, provided by social networks in the sphere of information spread. The new impertive for MNCs is gaining access to information on their customers, especially with the rise of Big Data technologies. Still, the other important issue is the safety of this information. As we have mentioned earlier, the more data companies gain, the more backdoors there are for the theft of it. In this regard, enterprises have to look for ways and measures to protect the information in an open space; often these measures are not effective even with large companies. Such measures are not affordable for SMEs as more than 51% of SMEs do not even take measures to protect information, although 41% of information attacks are carried out specifically for SMEs (Grand, 2018). Thus, the main risks which can be identified in digitalization for the corporate sector are the following:

- 1- Information and its derivatives protection
- 2- Inflated digitalization costs with unobvious benefits in the short term
- 3- The complexity of the enterprise's business model transformation, as a result, a number of its functioning risks appears

4- Lack of ready solutions for marketing products in a digital society.

All foregoing leads that many enterprises, situated in the most developed countries, regard to the digitalization with caution and in some cases, negatively (Elding and Morris, 2018). However, the positive digitalization effects come from its own flaws:

1- There is faster information spread between potential customers, as a result, the company receives significant competitive advantages and a wider customer base

2- There are more effective financial control system and a greater number of financial instruments for raising capital both in the short and long term

3- Reducing production and transaction costs, reducing labour costs and raising capital

4- The ability to develop an individual approach to each client due to the extensive data availability on its activities and interests in the public domain (LBBW, 2019).

In fact, the digitalization risks are lapped over by its advantages, and this process can be described as a zero-sum game, where the risk for one is a benefit for the other. In the conditions of the digitalization, we are talking about a consumer market redistribution and a production model change, we mean, a change in global value chains and the emergence of weakly protected corporate assets, which looks like a new frontier in the economy in the whole because it affects economic relations in the complex (Ivančić, 2019).

Nowadays, it is necessary to notice that the cost-effectiveness of risk reduction in the cybersecurity field is quite low (de Bruijn and Janssen, 2017; Jang-Jaccard and Nepal, 2014). Information, presented in Table 1, is very necessary within the article's research.

Table 1. Comparison of the Cybersecurity Spending's Growth Rate and the Growth of The Enterprises' Number

	2017	2018	2019
Spending on cybersecurity, billions \$US	101,5	114,2	124,1

	2017	2018	2019
Enterprises number growth (%)	6,42	17,15	24,42
Spending on cybersecurity growth (%)	16,10	12,41	8,73
Cybercrime damage (in million \$US)	1418,7	2710	3500

Source: OECD (2021); Moore and Keen (2018); Clement (2020).

As the calculations' results, presented in Table 1, show the growth in the number of companies in OECD countries (which is obey the general growth dynamics) exceeds the expenses growth for cybersecurity; consequently, in the context of constant cyber threats increase, the protection level against them lowers.

In this context, it is necessary to highlight another digitalization risk, we mean, the invisibility and underestimation of the threats, which is being created by the digitalization, especially from the corporate sector, which sees additional costs for itself in the risk control system.

At the same time, significant profits of the ICT sector leads to the inflow of investments and growth of number of companies, introducing services in digital sphere (Henry-Nickie et al., 2019).

5. The Risks of Corporate Sector Digitalization for The Society

The other important issue, that should be revealed in this article is the issue of global information space and emerging information economy (Razvan, 2020). This leads to the growth of number of e-commerce enterprises and the growth of data flow between the customers and companies. Data vulnerability as a risk for corporate sector has been discussed earlier – the major consequence for the corporate sector is the loss of profit and goodwill (as it happened with Facebook, for instance (Davey Winder, 2019). But the security of the clients is rarely discussed in this regard (Kuru and Bayraktar, 2017).

The client in case of the loss of data or the misuse of it can lose much more – in addition to financial losses, he/she bears the risks of private life breakage, as in case of iCloud leaks, or the loss of intellectual property, characteristic to the more developed economies (Park et al., 2019). Earlier we mentioned that big corporations and MNCs do their best to protect their customer data, although for the

reasons of further commercial use and preservation of goodwill. SMEs don't have such a potential, but their share on the market of e-commerce is high (Lekhanya, 2016). Figure 2 demonstrates the growth of volume of international trade in ICT services.

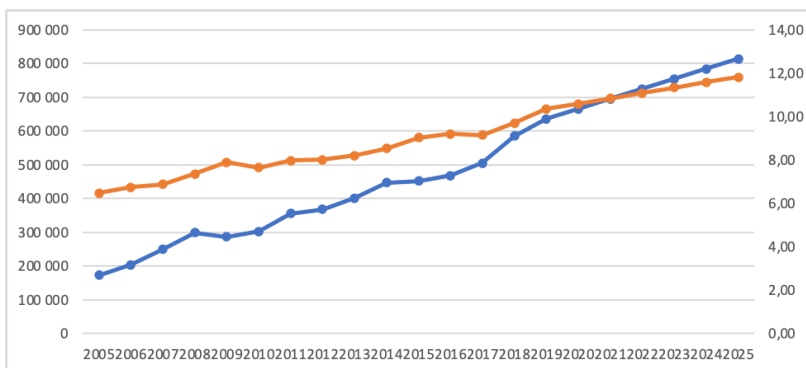


Figure 2. The Volume of Trade in ICT Services and Its Forecast

Source: UNCTAD (2019).

The graph shows, that in 2020 11% of trade is conducted via Internet, which requires authorization and can be used as an instrument of gaining personal data and information on customer behavior. In 2025, the corporate sector will have access to the personal data of every 8-th person in the world, including card number, name and surname, telephone number and address. It makes people vulnerable to the breakages of data, which is obvious, but it provides new risk – the possibility of manipulation.

Companies, which have access to the vast volume of personal data can develop mechanisms, allowing them to predict customer behavior and to cut the costs of promotion and make it more effective (Puri and Mohan, 2020; Lee and Cho, 2020). Despite the fact, that this is a big advantage for the MNCs, such as Google, for instance, it is a significant risk for people, leading to the loss of freedom of choice and change in market behavior. The easy manipulation with the behavior of people in the world of Big Data can bring risks to

corporations too – in case their competitors steal their data (or the data of their clients).

As a result, modern state of digitalization allows putting forward several serious risks for society:

1-Risk for personal data – it does not matter whether the data is transferred or stored by a corporation or person

2-Risk for personal life and freedom – the contemporary society is based on liberal values and respect to private life. In case algorithms of Big Data are able to calculate the behavior of a person, there will be no personal life as it will be available to the owners of such algorithms. As a result, the choice a person makes will be highly predictable too, changing the free market patterns. While the choice is predicted before it is made, the freedom is lost due to the owners pursue of information on such predictions for revenues.

3- Risk for corporate goodwill – when a company uses data of its customers for manipulating them, the social unrest and loss of reputation of the corporation should be expected.

While speaking of the loss of freedom, the question of who we can trust our personal data arises. The obvious answer – if we cannot trust corporations and SMEs, we can try trusting our data to the state, as a major regulator of the legislative system and the possessor of the rights protection mechanisms (legislative system, police, armed forces etc.). Nevertheless, the major issue about the state, that besides its interests in our personal data – for instance, during the elections for the manipulation with the results, it cannot protect our data significantly better than corporate sector (Rojszczak, 2020; Baik, 2020). It especially refers to the countries, where the influence of MNCs is high; moreover, the state is a corporation itself in some way, so it needs our data too.

The calculation of the proposed index of the sufficiency/efficiency of the spending on digital security is presented in Table 2.

Table 2. The Calculation of Sufficiency/Efficiency of Digital Security Spending Index

	2017	2018	2019
Index value	0,7862	0,5233	0,6933
Sufficiency/corrected	2,09/-	0,78/2,1	1,01/1,31
Efficiency	0,17	0,42	0,3
Correction of sufficiency	0,09	0,37	0,77

Source: Research finding.

The results of table 2 clearly demonstrate a tendency of the abundance of expenditures on the digital security, but their extreme inefficiency. As a result, the other important risk for the society arising from this data is the ineffective spending of taxes and revenues created from the purchases of people in the Internet. The other important issue about this problem is that at the current stage nobody knows how to fight cybercrime effectively (Wang, 2020).

There is no clear answer to the question of what to do with the risks of digitalization for the society. It's clear that every economic agent has its own interests and goals about personal data of the people. We cannot trust our personal data neither corporations, nor state, in the extreme case of digitalization (the penetration of it in our everyday lives) we can't trust even ourselves – it may occur that our electricity or gas provider monitors our supply/demand and calculates which devices we use in some period of time. For now we can only rely on the sudden solution of this problem. The only secure point in this regard is that we should control the distribution of our data by ourselves and have common responsibility for the breakages of personal data. In this case, the democratic solution of the problem is the most reasonable, as it allows to control every data transaction closely and commonly. The technology of distributed register can be of an assist in this case, but in its modern state it can't serve as a mighty instrument of control over personal data transactions.

6. Discussion

Based on the conducted research the authors consider necessary to form a bundle of recommendations, based on the comparison of the results of this study and similar works.

The findings of the article correlate with other similar studies, for instance, (Kwilinski, 2020) depicts the social influence of digitalization in EU, but at the same time, the issue, which are raised, are more of a long-run character, as in the nearest future the more substantial risks are of the data protection character.

In this regard, a closer look at the interconnection between the social risks and the economic consequences of the massive digitalization, presented in (Zemtsov et al., 2019) allows forming a significant recommendation for the any company, intending to introduce a digital model:

1- It is necessary to analyze the threats which may actually arise in the during the transition to a digital model. For example, if a company operates in the industrial sector, such threats may include job cuts, an increase in the recovery time of the production line in the equipment malfunction event, etc., but for the sales company, the main threat will be the loss of customer data confidentiality.

The interesting effect of the digitalization of companies lies in the sphere of data protection, and (Nabbosa, 2020) supports the findings of our research. The companies, even if they concentrate on the data protection are very vulnerable to cyber threats as they don't know exactly the character of such threat. The named source advises to introduce a systematic checklist, but we offer to extend this measure and to specify and characterise all the measures in the following way:

2- In accordance with the identified threats, it is necessary to begin data protection measures; among these measures, 2 groups can be distinguished: reducing the human factor risk and technological risks reducing. Within both groups, it is necessary to create a system of the

digitalization risks control by using the digitalization benefits. For example, the human factor can be levelled by a traffic control system, and the technological risks (hacking risks) reduction can be lowered, on the contrary, by hiring qualified personnel in the field of information protection and IT specialists.

The state regulation of data protection is a vital part of the digitalization in the world, as it's proved in (Sidorenko, Von Arx, 2020), digitalization should proceed only in case the country has a firmlegal basis for it, otherwise, the scenation of cybercrime spreading will arise. The same refers to the companies, the interesting fact is that companies can and should adopt to the conditions (Margiono, 2020), at least they can choose the pace of digitalization. In this regard, the other recommendation is formed:

3- Calculate the digitalization benefits and the reducing risks' costs: the second ones should be covered by the received benefits. If the digital transformation costs are higher than the benefits from it, it is necessary to reduce the business model transformation tempo and turn to a less comprehensive enterprise protection program at the technological level.

We haven't specifically studied influence of digitalization on marketing, but several works have made conclusions on the necessity of the changes in the approaches to marketing (Orazymbetova et al. 2020) for instance, sets a number of criteria, which should be fulfilled in order the company complies with the new digital conditions. The other research (Ayaydin and Gulerman, 2017) complies with the idea of the need for specification of needs of companies, when researching marketing issues. All in all, the major scientific discourse allows to give another recommendation:

4- Change the PR system, form a focus on the goods and company's services promotion through digital channels. At the same time, special attention should be paid to the formation of a company's goodwill, as it lies on the basis of its products' marketability in the digital age.

The data-driven economy is the contemporary reality and the companies should adopt to the conditions, proposed by the general track of the economic development. (Kubina et al., 2015) proves the necessity of digitalization in corporate sector and that the companies, which have adopted strategies in digital sphere are more successful, than those who didn't. In this regard, the last recommendation for the companies is the following:

5- Higher attention to the protection of the private data of the customers and at the same time collection of the data available.

Taking into account the proposed algorithm, for the corporate sector as a whole, it is necessary to rethink the approach to digital risks: the system "the threat model - investment in the fight against the threat – control" does not work in a digital space where control can be carried out only when the threat occurred. The development of a predictive system to fight against the digitalization's risks should come first in importance for companies, as without the ability to detect the threat source before or in the worst case at the same time as it arises, it is impossible to fight against cyber threats and reduce the digitalization risks.

The results of the paper comply with the existing scientific knowledge, still they make a wider impact on the risk management system of the companies, as the proposed steps are universal and allow to introduce the cyber risk management system (even an elementary one) in the SMEs, which hasn't been offered before.

7. Conclusion

Based on the obtained results and the place of these results in the scientific discussion framework, the authors come to the following conclusions.

Digitalization significantly changes the corporate sector's risk landscape and requires a new fight model against them, which is directed at preventing the emergence of a threat before it arises. To

form a unified approach to digitalization, a clear individual strategy for integrating into the digital environment is required from most sector's companies, or at least from all market makers.

In the whole, the digitalization risks are the reverse side of its advantages; that's why the fight against the risks of digitalization should be carried out in a clearly defined advantages' framework which it provides both financially and physically. Today, this proportion is not respected, as a result, the cyberattacks' number and success is growing. It is necessary to notice, cyberattacks are the main threats to information integrity, which is the main resource for a digital company.

For SMEs, the issue of fighting against cyber threats is also extremely important, but due to the high cost of effective methods in the fight against them, SMEs have to abandon cybersecurity for the sake of competitiveness. It is necessary to raise the question of the collective security system formation, as the cyber threats' prevention by a proactive system of measures to reduce the large companies' risks will reduce the threat to SMEs.

The rise of the question of collective security leads to the question of social risks of digitalization and the ways of counteracting them. In the contemporary conditions one can't trust his data anybody, and still he/she is not secure. This situation requires collective solution, based on democratic principles and transparency.

One of the ways to overcome these issues, includes several significant steps, including changes in PR, changes in consumers' private data management, new risk-management system and a systematic approach to risks in the concrete sector.

References

Ayaydin, F., & Gulerman, I. (2017). Effectiveness of Digital Public Relations Tools on Various Customer Segments. *Pressacademia*, 4(3), 259-270.

Baik, J. (2020). Data Privacy against Innovation or against Discrimination? The Case of the California Consumer Privacy Act (CCPA). *Telematics and Informatics*, 52, 1-10.

Bruijn, H., & de Janssen, M. (2017). Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies. *Government Information Quarterly*, 34(1), 1-7.

Clement, J. (2020). IC3: Total Damage Caused by Reported Cyber Crime 2001-2019. Retrieved from <https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us>

Digitalization & Corporate Strategy. (2018). M&BD Consulting. Retrieved from <https://www.mbdconsulting.ch/publications/digitalization-corporate-strategy>

Elding, C., & Morris, R. (2018). Digitalization and its Impact on the Economy: Insights from a Survey of Large Companies. *ECB Economic Bulletin*, 7/2018, 1-5.

Ganguly, S., Harreis, H., Margolis, B., & Rowshankis, K. (2017). Digital Risk: Transforming Risk Management for the 2020s. Retrieved from <https://www.mckinsey.com/business-functions/risk/our-insights/digital-risk-transforming-risk-management-for-the-2020>

Grand, A. (2018). Cybersecurity Statistics. Retrieved from <https://bestvpn.org/cybersecurity-statistics>

Guo, H., Yang, Z., Huang, R., & Guo, A. (2020). The Digitalization and Public Crisis Responses of Small and Medium Enterprises:

Implications from a COVID-19 Survey. *Frontiers of Business Research in China*, 14, 19-39.

Harari, Y. N. (2018). *21 Lessons for the 21st Century*. Spiegel & Grau: Jonathan Cape.

Harishchandra, N. (2019). Impact of Digitalization on Corporate Reputation. *Conference on Impact of Digitalization on Corporate Reputation*, Sri Lanka, 1-13.

Härmand, K. (2021). Digitalization before and after the Covid-19 crisis. *ERA Forum*, 22, 39–50.

Henry-Nickie, M., Frimpong, K., & Sun, H. (2019). Trends in the Information Technology Sector. Retrieved from <https://www.brookings.edu/research/trends-in-the-information-technology-sector/>

Ivančić, L., Bosilj, V., & Vukšić, M. S. (2019). Mastering the Digital Transformation Process: Business Practices and Lessons Learned. *Technology Innovation Management Review*, 9(2), 36-50.

Jang-Jaccard, J., & Nepal, S. (2014). A Survey of Emerging Threats in Cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993.

Khanboubi, F., & Boulmakoul, A. (2018). A Roadmap to Lead Risk Management in the Digital Era. *Conference: ASD 2018: Big Data & Applications 12th Edition of the Conference on Advances of Decisional Systems*, Marrakech, Morocco, 1-12.

Kubina, M., Varmus, M., & Kubinova, I. (2015). Use of Big Data for Competitive Advantage of Company. *Procedia Economics and*

Finance, 26, 561-565.

Kuru, D., & Bayraktar, S. (2017). The Effect of Cyber-Risk Insurance to Social Welfare. *Journal of Financial Crime*, 24(2), 329-346.

Kwilinski, A., Vyshnevskiy, O., & Dzwigol, H. (2020). Digitalization of the EU Economies and People at Risk of Poverty or Social Exclusion. *Journal of Risk Financial Management*, 13(7), 142-151.

LBBW. (2019). Key Terms of Digitalization and Industry 4.0. Retrieved from https://www.lbbw.de/articlepage/understanding-markets/key-terms-digitalization-industry-4-0_6vip5a4gw_e.html

Lee, H., & Cho, C.-H. (2020). Digital Advertising: Present and Future Prospects. *International Journal of Advertising*, 39(3), 332-341.

Lekhanya, L. M. (2016). E-commerce as an Instrument of Governing Smes' Marketing Strategy in an Emerging Economy. *Risk Governance and Control: Financial Markets and Institutions*, 6(4), 298-315.

Managing Risk in Digital Transformation. (2018). *Deloitte Touche Tohmatsu India LLP*. Retrieved from <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf>

Mandviwalla, M., & Flanagan, R. (2021). Small Business Digital Transformation in the Context of the Pandemic. *European Journal of Information Systems*, 30(4), 359-375.

Margiono, A. (2020). Digital Transformation: Setting the Pace. *Journal of Business Strategy*, 42(5), 1-15.

Moore, S., & Keen, E. (2018). Gartner Forecasts Worldwide

Information Security Spending to Exceed \$124 Billion in 2019. Retrieved from <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>

Nabbosa, V. L. (2020). Me too: Value Creation by Digitalization and Data Privacy. *Conference: ICEBT'20: 2020 the 4th International Conference on E-education, E-business and E-technology*, Retrieved from <https://doi.org/10.1145/3404649.3404650>

OECD. (2018). Financial Markets, Insurance and Private Pensions: Digitalization and Finance. Retrieved from <http://www.oecd.org/finance/Financial-markets-insurance-pensions-digitalisation-and-finance.pdf>

OECD. (2018). Implications of the Digital Transformation for the Business Sector. Retrieved from <http://www.oecd.org/sti/ind/digital-transformation-business-sector-summary.pdf>

OECD. (2021). Timely Indicators of Entrepreneurship (ISIC4). Retrieved from <http://www.oecd.org/sti/ind/digital-transformation-business-sector-summary.pdf>

Orazymbetova, A., Bekmurzayev, B., Kazykeshvova, A., Faizullina, S., & Kogabayeva, A. (2020). How to Effectively Build Marketing in the Digital Era Economies. *E3S Web of Conferences*, 159, 26-40.

Park, J., Cho, D., Lee, J., & Lee, B. (2019). The Economics of Cybercrime: The Role Of Broadband And Socioeconomic Status. *ACM Transactions on Management Information Systems*, 10(4), 1-15.

Parviainen, P., Tihinen, M., Kääriäinen, J., & Teppola, S. (2017). Tackling the Digitalization Challenge: How to Benefit from

Digitalization in Practice. *International Journal of Information Systems and Project Management*, 5(1), 63-77.

Puri, D., & Mohan, T. (2020). Behavioral Advertising With Big Data: A Consumer's Perspective. *International Journal on Emerging Technologies*, 11(3), 771-776.

Rachinger, M., Rauter, R., Müller, C., Vorraber, W., & Schirgi, E. (2019). Digitalization and Its Influence on Business Model Innovation. *Journal of Manufacturing Technology Management*, 30(8), 1143-1160.

Razvan, S. (2020). Several Contemporary Economy Features, Consequences of Internet Expansion and I.C.T. Innovations in the World. *Studies in Business and Economics*, 14(3), 175-181.

Ritter, T., & Pedersen, C. L. (2020). Digitization Capability and the Digitalization of Business Models in Business-To-Business Firms: Past, Present, and Future. *Industrial Marketing Management*, 86, 180-190.

Rojszczak, M. (2020). CLOUD Act Agreements from an EU Perspective. *Computer Law and Security Review*, 38, 1-14.

Roser, M., Ritchie, H., & Ortiz-Ospina, E. (2015). Internet. Retrieved from <https://ourworldindata.org/internet>

Sidorenko, E. L., & Von Arx, P. (2020). Transformation of Law in the Context of Digitalization: Defining the Correct Priorities. *Digital Law Journal*, 1(1), 24-32.

UNCTAD. (2019). Digital economy report 2019. Value Creation and Capture: Implications for Developing Countries [Online]. Retrieved from

https://unctad.org/system/files/official-document/der2019_overview_en.pdf

UNCTAD. (2019). International Trade in ICT Services, Value, Shares and Growth, Annual. Retrieved from <https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=158359>

Wang, X. (2020). Criminal Law Protection of Cybersecurity Considering AI-based Cybercrime. *2020 International Conference on Artificial Intelligence and Information Technology, ICAIIT 2020, Seoul, South, Journal of Physics: Conference Series, 1533(3)*, 120-135.

Winder, D. (2019). Unsecured Facebook Databases Leak Data of 419 Million Users. Retrieved from <https://www.forbes.com/sites/daveywinder/2019/09/05/facebook-security-snafu-exposes-419-million-user-phone-numbers/?sh=83dae891ab7f>

Zemtsov, S., Barinova, V., & Semenova, R. (2019). The Risks of Digitalization and the Adaptation of Regional Labor Markets in Russia. *Foresight and STI Governance, 13(2)*, 84–96.