European Research Studies Journal
Volume XXVI, Issue 4, 2023

pp. 160-172

Cyber Security of Remote Work in Poland and the EU - Selected Aspects

Submitted 25/10/23, 1st revision 10/11/23, 2nd revision 06/12/23, accepted 30/12/23

Piotr Ładny[1], Piotr Gutowski[2]

Abstract:

Purpose: *The purpose of the article is to present cyber security issues in the context of the development of remote work in the European Union and Poland , as well as to identify the cyber security challenges facing individual countries, their institutions and business entities.*
Design/Methodology/Approach: *The article analyzes the changes that have occurred in the area of remote work in recent years and assesses the impact that these changes have caused in the level of cyber security of entities and employees using IT solutions to perform their duties remotely. The research method adopted by the authors was a survey method conducted via the Internet (Computer-Assisted Web Interview) on a representative group of 1,108 Poles aged 18-65 and secondary research, based on an analysis of the literature, research results and reports on cyber security and remote working.*
Findings: *As the number of people performing their work remotely using information technology continues to grow, including especially in the wake of the Covid 19 pandemic, the number of cyber threats to infrastructure and data belonging to companies and institutions has increased. The research shows that one of the key elements influencing the level of cyber security in the context of remote work is the digital competencies related to this area among employees performing their duties in a virtual work environment. EU countries have taken a number of measures to reduce and close the competence gap that exists in the market with regard to cyber security issues. Unfortunately, one can notice a significant difference in the scope of these activities between Poland and other EU countries. Therefore, Poland should take more active measures to create a comprehensive system of acquiring and developing digital competencies related to protection against digital threats among people already in the workforce, as well as among children and young people. The construction of educational programs and training in the field of cyber security is necessary not only in the context of the following development of remote work, but is also a prerequisite for the safe development of the digital economy.*
Practical implications: *The critical conclusions presented in the article are a starting point for further research, relating to the competence gap in cyber security in the context of changes related to the digitization of the economy and the labor market, which will allow the development of a set of measures that will be necessary to increase the cyber security of companies, institutions and the economy as a whole in Poland.*

[1]*Dr., Institute of Spatial Management and Socio-Economic Geography, University of Szczecin, Poland, piotr.ladny@usz.edu.pl;*
[2]*Dr., inz. Institute of Management, University of Szczecin, Poland, piotr.gutowski@usz.edu.pl;*

Originality/Value: *The authors pointed to the ongoing changes in the labor market, including an increase in the number of employees performing their duties remotely, and the associated cyber security problems. The analysis of the problem points to insufficient competence in cyber security among employees and those entering the labor market and the low effectiveness of educational programs to date, as well as the need for a stronger inclusion in the Polish cyber security system of active measures aimed at raising the level of digital competence, including competence in the area of digital security and digital resilience as key to the further development of the digital economy and modern forms of employment. The conclusions formulated in this article are a contribution to the discussion on building a comprehensive cyber security system in Poland.*

Keywords: *Cybersecurity, remote work, Internet.*

JEL codes: *J24, L86, M15.*

Paper type: *Research article.*

1. Introduction

The modern world, rushing towards increasing digitization and use of technology, presents not only new opportunities but also challenges. The development of remote work, which has gained particular momentum in the wake of the COVID-19 pandemic, is one of the effects of this trend.

Remote work is becoming one of the elements creating conditions for the development of the digital economy. New technologies and regulations enabling remote work, foster innovation, work flexibility, strengthen the roles of e-commerce, online services and remote teams.

It should be noted that not only the pandemic but also the transformations taking place in modern economies, including the growing role of technology in defining new business models, the increasing interdependence and networking of the global economy and individual companies, the increasing role of women in business and the economy, as well as generational changes and the resulting expectations of employees create demand for this form of work organization.

However, as employees use a variety of platforms and tools to perform their professional duties remotely, cyber security threats are also on the rise.

Today's digital threats are becoming more sophisticated and diverse, and attacks are becoming more sophisticated, targeted and complex. Cyber criminals are using advanced techniques, including artificial intelligence, machine learning or social engineering, making cyber attacks more difficult to prevent and detect.

In a remote work environment when employees connect from remote, often unsecured locations, making additional use of equipment and infrastructure that is outside the organization's control, digital competencies become the foundation for creating a secure online environment, especially competencies related to identifying threats and countering their effects. Knowledge of how to identify and avoid potential threats, the proper use of digital tools and the ability to respond to incidents are the key elements that make up an effective system of protection against cyber attacks.

New regulations being introduced at the EU level and in individual member states are creating conditions and facilitating the introduction of flexible forms of employment including remote working solutions, but in order to take advantage of these facilitations, the protection of information, data and virtual systems must become a priority, and one of the main means to achieve this goal should be the development of digital competencies including, in particular, competencies related to cyber security for employees and those entering the labor market.

Aware employees, equipped with the skills to identify threats, take appropriate action and use cyber security tools, are the first line of defense against cyber attacks, contributing to maintaining the integrity and confidentiality of data in the era of the digital economy.

2. The Rise of Cyber Threats Associated with Remote Work

The idea of remote work, also referred to as telecommuting, is a concept that has been around for a long time. Its roots can be traced back to the 1950s, but it wasn't until the development of information and communication technologies and personal computers in the early 1970s that the conditions were created for putting the idea into practice (Hill *et al.*, 1996).

Variety of telework terms are found in the scientific literature: teleworking, home-based work, working from home, home-based telework, homeworking, telecommuting, virtual office, virtual work, e-work, flexiplace, flexible work (Brinzea and Secara, 2017; Nakrošiene *et al.*, 2019).

In Europe, the term telework was defined as a “form of organizing and/or performing work, using information technology, in the context of an employment contract/relationship, where work, which could also be performed at the employers' premises, is carried out away from those premises on a regular basis” (European Framework Agreement on Telework, 2002).

In Poland, the concepts of remote work were not regulated until 2007 in which the concept and regulations of telework were introduced into the Labor Code for the first time. According to the accepted definition, remote work meant the regular performance of work duties outside the company's premises, using electronic

communication means, and the transmission of the results of this work in a specific form.

In 2023, the legislation was amended and the term telework was replaced by the term remote work, defining more adequately to the changes that have occurred in the labor market the definition of the concept of remote work and the legitimacy of its provision.

According to the adopted definition, remote work is work performed in whole or in part at the place indicated by the employee and agreed with the employer in each case, including at the address of the employee's residence, in particular using means of direct communication at a distance.

Technological developments over the past 20 years especially in the field of Internet communication and online collaboration tools have helped create the conditions for the development of remote work. This is the basis for the development of the modern economy (Drab-Kurowska, 2010).

Companies, realizing the benefits of this form of employment, increasingly offered remote work as an option for their employees, allowing them to expand their employee recruitment reach, improve their work-life balance and reduce the costs associated with maintaining traditional offices (Budziewicz-Guźlecka and Drab-Kurowska, 2017).

Up until 2020, however, the growth was slow and mainly involved people using this form sporadically or occasionally. In 2019, about 5.4% of all employed people in the EU-27 usually worked from home, a percentage that has remained rather constant since 2009. However, over the same period, the share of those employed from home at least sometimes increased from 5.2% in 2009 to 9% in 2019.

Remote work has surged in 2020 due to the development of the covid pandemic. During the first semester of 2020, working from home has become the customary mode for millions of workers in the EU and around the world (Sostero et al., 2020). Estimates indicate that in parts of the EU countries, more than 40% of the employed population has started teleworking full-time in 2020 (Eurofound, 2020).

The Labour force survey (LFS) of EU countries shows that in 2020 the number of employed people working from home usually increased by more than 120% compared to 2019 (from 5.4% to 12%. The number of people who worked from home usually or sometimes increased from 14.4% to 20.6%. In the following years, the share of employed people who worked from home usually or sometimes was 24% of those employed in 2021 and 22.4% in 2022 (Lfsa_ehomp, 2022).

In Poland prior to the pandemic, the share of employed people working remotely in 2019 was about 4.6%, lower than the EU average, but the introduction of solutions

to prevent the epidemic from developing has caused the number of people working from home to rise sharply, as in other European countries.

Labor market data shows that in Q1 2020 the share of people working remotely rose to 11% of the workforce and in Q1 2021 the percentage was 14.2% (Wpływ epidemii COVID-19 ..., 2023).

The rise in popularity of remote work has triggered a number of changes in the labor market. In addition to the benefits for employees and employers, there have also been challenges, much of which have been technological in nature and related to the widespread use of tools and platforms that enable remote work and ensuring the security of data and infrastructure (Budziewicz-Guźlecka, Czaplewski, and Drab-Kurowska, 2018).

For many years now, there has been a clear trend related to the increase in cyber threats and cyber incidents. The problem has been further amplified by the Covid pandemic and the associated increase in the number of employees performing their duties remotely often from their homes and other locations unprepared to ensure adequate levels of security

As remote working was very often forced by the growing number of infected people and dynamically introduced restrictions on movement and social contacts, a number of entities implemented solutions in this regard without adequate hardware and human resources and based on hastily created procedures.

In practice, this has meant that the growing number of people working with private infrastructure and the devices working in it, often also without comprehensive training, have become targets for cybercriminals exploiting vulnerabilities and weaknesses. As reports summarizing cybersecurity incidents indicate, there is clearly a large and growing adaptability of cybercriminals.

They are reaching out more skillfully to both the latest technologies and psychological and sociological observations, which translates into increasingly sophisticated attacks , taking advantage of, among other things, gaps in system security, unauthorized access, leaks of confidential information and human vulnerabilities (ESET Threat Report, 2023).

It is not only large companies and organizations that are becoming targets of cyberattacks, but increasingly small and medium-sized businesses as well. According to Verizon's 2022 Data Breach Investigations Report, 43% of cyberattacks today target small businesses rather than large enterprises (Data Breach Report, 2022).

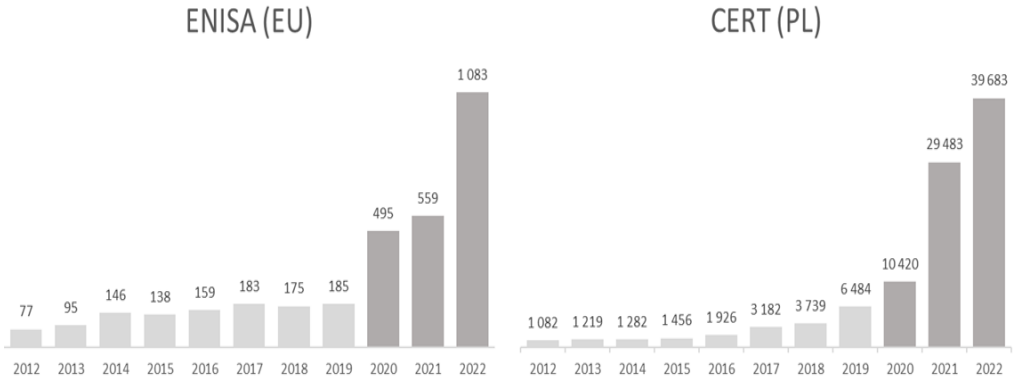
According to an EU study published in May 2022, 28% of European SMEs were victims of cybercrime in 2021 (SMEs and Cybercrime, 2022), and Checkpoint

estimates that the number of cyberattacks on corporate networks increased by 50% in 2021 compared to 2020 (Check Point Report, 2022). The European Union Agency for Cybersecurity (ENISA) estimates that the cost of dealing with a security incident in the EU is typically between €213,000 and €300,000 (ENISA Threat Landscape, 2022).

The number of reported cybersecurity incidents by European critical service providers shows that 2020 saw a significant increase. 495 incidents were reported to ENISA, a more than 167% increase compared to 2019. Further increases were registered in the following years - by 12.9% in 2021 and 93.6% in 2022 (CIRAS, 2023).

An increase in IT threats and incidents is also observed in Poland. Reports from CERT Poland - Poland's first computer incident response team, which has been part of the national cyber security system since 2018 - show that the number of reported incidents has increased significantly in 2020 and beyond (Krajobraz bezpieczeństwa polskiego internetu, 2023). The number of incidents handled between 2012 and 2022 by ENISA and CERT Poland is shown in Figure 1.

Figure 1. *Number of incidents handled by ENISA and CERT Poland in 2012-2022*



Note: ** ENISA only records reports from critical service providers, CERT Poland handles incidents reported by all Internet users in Poland.*
Source*: Own study based on data from ENISA and CERT Poland.*

The increase in cyber threats observed worldwide, including in EU countries, concerns not only the number, vectors and means of attacks or areas affected by the threats, but also their impact on users and economic systems. Cyber Security Ventures, a cyber security research center, estimated that the costs generated in this way for the global economy in 2021, reached US$6 trillion, compared to around US$3 trillion just 10 years ago.

By 2026, total spending on securing networks and services is expected to be as high as $16.8 billion (Cybercrime To Cost ..., 2023). According to another report

compiled by analyst firm Techanvio, spending on digital security will rise to $23.34 billion by 2026, with the increase in worker mobility and the growth of remote work cited among the reasons for such growth (Technavio, 2022).

3. Digital Competence in Cybersecurity as a Prerequisite for the Operation and Development of Remote Work

After the pandemic, the number of people working remotely has decreased, but in most countries it remains significantly higher than before the pandemic (Demetriades *et al.,* 2023). Regulations on this form of employment being introduced at the European Union level and in individual member states (including Poland) indicate that telework and ICT-based mobile work have become part of a package of new working conditions that are an integral part of the digital economy.

It should be assumed that in post-pandemic conditions, remote work will remain an important part of the labor market while adapting to new conditions and changing its nature. The most important areas in which changes should be expected are: the introduction of a hybrid work model that combines remote work with office work, the development of IT infrastructure and online collaboration tools, increased employer support for mental health care, online training and work-life balance programs for employees, and an increased focus on data security and protection from cyber attacks in connection with work done remotely (Demetriades *et al.,* 2023) (Sostero *et al.,* 2020).

Referring to the issues of cyber-security and cyber-resilience of organizations, the importance of which was emphasized in the context of the development of telework in EU regulations even before the pandemic (ETUC *et al.,* 2006), special attention should be paid to the need to develop digital competencies of employees, which are crucial for successful functioning in a virtual work environment (Budziewicz-Guźlecka, 2013; 2019).

The combination of developed technological tools, proper cybersecurity practices and digital competence is the foundation for the success and stability of remote work. This problem affects not only professionals employed in IT departments but also employees working in areas other than IT, due to the growing number of attacks that exploit employee vulnerabilities and social engineering, thus bypassing safeguards built in at the hardware or software level.

An example is the results of a study assessing the impact of user knowledge and behavior on phishing threats. This research showed that there is a relationship between the knowledge and the behavior of end-users in the aspect of utilizing anti-phishing solutions (Wang, 2013).

ESET's survey of 1,200 European and North American SMEs found that among the top 5 factors amplifying the risk of cyber attacks, 43% of percent of respondents

cited employees' lack of knowledge about cyber security, and 32% further hybrid or remote working. Only 48% of SMEs claimed to be moderately/very confident in their cyber resilience.

Among Polish SMEs, only 10% of respondents indicated such an assessment (Toward the Cutting Edge, 2022). A report published by cyber security firm Clavister found that Organizations are not yet confident in their abilities to support hybrid working, only around a third of companies felt they already had comprehensive security coverage to support hybrid working (A New Era of European Cyber Defence, 2023).

The problem appears to be becoming a global issue. A report published by Firme Fortinet shows that worldwide, 84% of organizations suffered one or more breaches that they could attribute to a lack of cybersecurity skills and/or awareness. A key factor is that organizations struggle to find and retain certified cybersecurity people (Fortinet, 2023).

The growing number of incidents is accompanied by an increased sense of threat felt by both employees and employers. A survey commissioned by the European Commission at the end of 2019 shows that the vast majority of respondents (76% on average) perceived a growing risk of becoming a victim of cybercrime (in Poland - 72%), but despite the growing awareness and sense of threat among respondents, the belief in having sufficient competence to protect against threats is falling.

Only 59% of Europeans believe that they have sufficient knowledge and skills to protect themselves from this type of crime. in Poland, such a belief is expressed by 53% (Eurobarometer Survey, 2020).

A survey conducted by the authors of the article on a representative sample of Poles in 2023 shows that about 54% of Poles rate their knowledge and skills in defense against cyber threats insufficiently (none at all - 11%, very poorly - 11% and poorly - 32%).

At the same time, the survey shows that educational activities in the field of cyber security are insufficient. Of all respondents, 95% indicated that they get information on cyber security by visiting news portals and social media, Only 15% by attending training at work and 6% by attending classes at school and college. At the same time, 10% responded that they are not interested in cyber security issues

It is worth noting that the survey indicates a significant weakness of the Polish education system in the field of cyber security because among the participants of training conducted by employers, as many as 76% rated it poorly or very poorly. In the case of classes conducted during education, the percentage of those rating them poorly or very poorly was even higher, at 81% for classes in elementary and secondary schools and 82% for classes in higher education.

The existence of a significant competency gap is confirmed by the results of a survey conducted by the Internet Standards, Security and Safety Coalition (IS3C) working group in 65 countries around the world, including Europe. Among industry and business representatives, 44% rated the cybersecurity competency of graduates they hire as low or very low (Zmniejszanie luki ..., 2022).

Lack of sufficient knowledge in the field of cyber security is part of a broader phenomenon occurring in Poland - a low level of broadly understood digital competence. Taking into account the overall digital competence at both the basic and advanced levels, i.e. two of several elements on the basis of which the Digital Economy and Digital Society Index (DESI) is created, it can be seen that Poland is among the 4 worst EU countries ahead of only Italy, Bulgaria and Romania (The Digital Economy and Society Index, 2022).

4. Discussion

It is often pointed out that the reason for the current problems of inadequate levels of competence among non-IT employees has been the reduction of cybersecurity support activities to technical security of systems and devices (Cybersecurity Culture Guidelines, 2019). Failure to consider the human factor in this area has reduced the level of the organization's ability to prevent and protect against attacks especially when employees are taken en masse outside the protected infrastructure, e.g., to home networks.

The increase in demand for employees with competencies in the area of cybersecurity including not only IT professionals, but also employees who use digital technologies on a daily basis, has caused many countries, international organizations and employers to start recognizing the need to improve cyber security competencies. Also, geopolitics and international conflicts are causing an increase in awareness related to cybersecurity and the long-term consequences of risks.

Today, more and more cyber security initiatives are being launched at the international and national levels. However, it should be noted that the security system that is being created has so far focused on selected areas, such as the protection of critical infrastructure or the fight against terrorism, Cyber security regulations have mainly concerned large market players and public institutions.

Much less emphasis has been placed on solutions to enhance the security of citizens, small and medium-sized businesses, or employees outside of IT departments. An example of action at the international level is that of the EU, which allocated significant resources to support digital transformation and support digitization processes during the Covid 19 pandemic, with €127 billion allocated for digital reforms, increasing resilience and closing digital skills gaps, including those related to cyber security. These activities included the development of, among others:

- The Digital Education Action Plan (2021-2027) - is a call for greater cooperation at European level on digital education to address the challenges and opportunities of the COVID-19 pandemic, and to present opportunities for the education and training community (teachers, students), policy makers, academia and researchers on national, EU and international levels.
- The EU's Cybersecurity Strategy for the Digital Decade - aims to build resilience to cyber threats and ensure that citizens and businesses reap the benefits of trustworthy digital technologies, including through activities related to raising competence and reducing cyber skills gaps among the workforce.

Another example of creating a comprehensive framework for the cybersecurity education process can be found in the European program Digital Europe (DIGITAL) and a 3-year project underway in Finland from September 2022 under the auspices of the Ministry of Transport and Communications and Aalto University, which aims to develop an educational package to support cybersecurity education in EU member states.

Much worse is the introduction of systemic solutions to eliminate the competence gap in cyber security in Poland. Although in 2021 Poland was among the 3 EU countries with the highest percentage of enterprises that registered cyber security incidents (the percentage of enterprises in Poland was 29.7%, while the EU average was 22.2% (22% of EU Enterprises Had ICT Security Incidents, 2023), and the necessity of cyber security education already at the elementary school level is now emphasized as a key element, Poland lacks a harmonized system for building citizens' competence in this area.

Education programs currently do not specify the scope of knowledge that should be imparted at various stages of education, as well as methods for validating this knowledge. A report by the Polish Supreme Audit Office (Najwyższa Izba Kontroli – NIK) assessed training and education activities regarding the prevention and protection against computer crimes as insufficient and ineffective (*Działania Państwa w zakresie …*,2022).

In February 2023, the Council of Ministers adopted a resolution to establish a program for the development of digital competence, for which more than PLN 2.8 billion has been allocated. The goal of the program, which will be implemented until 2030, is to raise the level of digital competence in society, and to develop digital education. Although the goal of this program is not in doubt, the detailed provisions are criticized by specialists as inconsistent and incomplete (Opinia Na Temat PRKC, 2023).

5. Conclusion

Remote work has become an integral part of the global labor market, and its popularity has grown significantly in recent years, further accelerated by the

COVID-19 pandemic. Many companies are implementing hybrid models, combining remote work with in-office work, which increases flexibility and employee comfort levels. However, the rapid growth of this work model brings significant challenges, especially in the context of cyber security.

The rise of remote practices means greater exposure of organizations to cybercrime threats. Companies are facing an increasing number of attacks, phishing, ransomware and other forms of malware that can lead to data leaks and other serious information security consequences.

Unfortunately, Poland still faces the challenge of bridging the competence gap in the field of cyber security, especially in the context of the dynamic development of remote work. The lack of sufficient action and investment in education, training and employee awareness poses a challenge to effectively safeguard against cyber threats.

In order to meet these challenges, it is necessary to increase investment in the development of cyber security competencies and alignment with international standards and practices. Improving this area will allow more effective protection of data and infrastructure from cyber threats associated with remote work, which is key to securing the stability and security of modern organizations and creating conditions for the growth of the popularity of remote work.

The development of educational activities in relation to those already working and those yet to enter the labor market is key to ensuring the digital security of institutions, companies and the economy as a whole. These issues are the starting point for further research, including an analysis of the current state and opportunities in the labor market and the digital competence of remote workers, which will allow the development of a set of actions that will be necessary to raise the cyber security of companies and institutions in the context of changes in the labor market.

References:

2022 Data Breach Investigations Report. 2022. Available at: https://www.verizon.com/business/resources/reports/dbir/.

22% of EU enterprises had ICT security incidents. 2023. Eurostat News. Available at: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1.

A New Era of European Cyber Defence – looking ahead to 2023. 2023. Clavister. Available at: https://www.clavister.com/blog-post/a-new-era-of-european-cyber-defence-looking-ahead-to-2023/.

Brinzea, V.M., Secara, C.G. 2017. The Telework, A Flexible Way To Work In A Changing Workplace. Scientific Bulletin - Economic Sciences, 16(3), 104-112.

Budziewicz-Guźlecka, A. 2013. Wiedza i kapitał ludzki czynnikiem rozwoju przemysłów kreatywnych. Przemysł kreatywny–Ekonomia na styku kultury i biznesu, 84-99.

Budziewicz-Guźlecka, A. 2019. Oddziaływanie polityki społeczno-gospodarczej na zmiany polskiego rynku usług telekomunikacyjnych. Wydawnictwo Naukowe Uniwersytetu Szczecińskiego.

Budziewicz-Guźlecka, A., Drab-Kurowska, A. 2017. The analysis of selected issues pertaining to e-administration in Poland in the context of smart city. Nord. Balt. J. Inf. Commun. Technol, 17-32.

Budziewicz-Guźlecka, A., Czaplewski, M., Drab-Kurowska, A. 2018. Integracja sektorowa wybranych europejskich rynków pocztowych i telekomunikacyjnych w warunkach globalizacji. Wydawnictwo edu-Libri.

Check Point Software's 2022 Security Report. 2022. Available at: https://pages.checkpoint.com/cyber-security-report-2022.

CIRAS Incident reporting. 2023. CIRAS. Available at: https://ciras.enisa.europa.eu/ciras-consolidated-reporting.

Cybercrime To Cost The World 8 Trillion Annually In 2023. 2023. Cybercrime Magazine. Available at: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/.

Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. 2019. Report/Study, ENISA. Available at: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity.

Demetriades, S., Cabrita, J., Eiffe, F.F. 2023. The future of telework and hybrid work. Eurofound, https://doi.org/10.2806/234429.

Drab-Kurowska, A. 2010. Poziom technologi informatycznych w przedsiębiorstwach województwa zachodniopomorskiego. Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług, (57 E-gospodarka w Polsce. Stan obecny i perspektywy rozwoju. Cz. I), 153-160.

Działania Państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości. (KPB.430.010.2022). 2022. Najwyższa Izba Kontroli. Available at: https://www.nik.gov.pl/plik/id,27206,vp,30013.pdf.

ENISA Threat Landscape 2022. 2022. Report/Study. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

ESET Threat Report H1 2023. 2023. Available at: https://www.eset.com/us/business/resource-center/reports/eset-threat-report-h1-2023/.

ETUC, UNICE-UEAPME, & CEEP. 2006. Implementation of the European Framework Agreement on Telework—Report by the European social partners: Adopted by the Social Dialogue Committee on 28 June 2006. Available at: https://resourcecentre.etuc.org/sites/default/files/2019-09/Telework%202006_Final%20Joint%20Implementation%20Report%20-%20EN.pdf.

European framework agreement on telework. 2002. Available at: https://resourcecentre.etuc.org/sites/default/files/2020-09/Telework%202002_Framework%20Agreement%20-%20EN.pdf

Europeans' attitudes towards cyber security (cybercrime)—Eurobarometer survey. 2020. Available at: https://europa.eu/eurobarometer/surveys/detail/2249.

Eurostat lfsa_ehomp. 2022. Available at: https://ec.europa.eu/eurostat/data/database?node_code=lfsa_ehomp.

Fortinet 2023 Global Cyber Skills Gap Report. 2023. Fortinet Blog. Available at: https://www.fortinet.com/blog/industry-trends/skills-gap-report-untap-talent.

Hill, E.J., Hawkins, A.J., Miller, B.C. 1996. Work and Family in the Virtual Office: Perceived Influences of Mobile Telework. Family Relations, 45(3), 293-301. https://doi.org/10.2307/585501.

The Digital Economy and Society Index (DESI). 2022. Available at: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022.

Internet security market by solution and geography—Forecast and Analysis 2022-2026. 2022. Available at: https://www.technavio.com/report/internet-security-market-industry-analysis.

Krajobraz bezpieczeństwa polskiego internetu w 2022 roku. 2023. Available at: https://cert.pl/uploads/docs/Raport_CP_2022.pdf.

Nakrošiene, A., Buciuniene, I., Goštautaitė, B. 2019. Working from home: Characteristics and outcomes of telework. International Journal of Manpower. https://doi.org/10.1108/IJM-07-2017-0172.

Opinia na temat „Programu Rozwoju Kompetencji Cyfrowych do roku 2030". 2023. Sektorowa Rada ds. Komptetencji. Telekomunikacja i Cyberbezpieczeństwo. Available at: https://srtcb.radasektorowa.pl/publikacje-raporty/badania-i-analizy/369-opinia-dot-programu-rozwoju-kompetencji-cyfrowych-do-roku-2030.

Regulations to address work–life balance in digital flexible working arrangements. 2020. Publications Office. https://doi.org/10.2806/03528.

SMEs and Cybercrime—Eurobarometer survey. 2022. Available at: https://europa.eu/eurobarometer/surveys/detail/2280.

Sostero, M., Milasi, S., Fernandez-Macias, E., Hurley, J., Bisello, M. 2020. The potential for teleworking in Europe and the risk of a new digital divide. RIETI. Available at: https://www.rieti.go.jp/en/special/p_a_w/162.html.

Toward the cutting edge: SMBs contemplating enterprise security. 2022. Available at: https://www.welivesecurity.com/2022/11/10/toward-cutting-edge-smbs-contemplating-enterprise-security/.

Wang, P.A. 2013. Assessment of cybersecurity knowledge and Behavior, an anti-phishing scenario. CIMP 2013 the Eighth international Conference on Internet Monitoring and protection, Rome, Italy. Available at: http://www.thinkmind.org/articles/icimp_2013_1_10_30003.pdf.

Wpływ epidemii COVID-19 na wybrane elementy rynku pracy w Polsce. 2023. Available at: https://stat.gov.pl/obszary-tematyczne/rynek-pracy/popyt-na-prace/wplyw-epidemii-covid-19-na-wybrane-elementy-rynku-pracy-w-polsce-w-czwartym-kwartale-2022-roku,4,12.html.

Zmniejszanie luki pomiędzy potrzebami branży cyberbezpieczeństwa a umiejętnościami absolwentów szkół wyższych. 2022. Available at: https://www.nask.pl/download/30/4662/RaportzbadankoalicjiIS3C-lukamiedzypotrzebamibiznesuakompetencjamiabsolwentowszk.pdf.