Digitalization and cybersecurity in companies and supply chains: challenges and opportunities

Nazar Hlynskyy[1], Oksana Dovhun[1], Jolanta Pochopień[2]

[1]Lviv Polytechnic National University
Ukraine

[2]Bielsko-Biala University of Applied Sciences,
Poland

***Abstract*— The digitalization of the economy has many positive aspects, affects competitiveness and economic efficiency, but also creates challenges for companies and organizations. Business operates in a global environment and at the same time in countries with different progress levels of digital tools. This, in turn, affects the different levels of cybersecurity that companies can provide - depending on the level of development, field of activity, as well as on which market participants build the supply chains. The number of cyber attacks is growing in different countries, so learning new approaches, improving the legislative framework, and making management decisions to build cyber resilience are important. The authors have researched the laws and programs related to cybersecurity in force and what solutions are offered by scientists in this field. By surveying the businesses, it was found out what methods of cybersecurity are used by companies in Ukraine, what are the obstacles to implementation, and what consequences were observed after cyber attacks.**

Keywords— digitalization, cybersecurity, cyber resilience, cyberattacks on business, supply chains, SCM.

I. INTRODUCTION

In many countries of the world, the transition to a digital society is one of the priority tasks, which is confirmed by state strategies and programs for the development of the digital economy. For example, Denmark adopted its digital strategy back in 2000, Great Britain, Hong Kong, and New Zealand – in 2008. The European Union began implementing digital reforms in 2009. Ukraine approved a digital development strategy in 2018 (Myronova M., 2022). Over the past few decades, a powerful technological revolution has taken place in the field of computer and telecommunications use, which has led to fundamental changes, a significant acceleration of the speed of information transmission, and the development of companies. At the same time, rapid information progress has caused the problem of data security. However, as noted by Boyko V.D. (Boyko V.D. et al., 2022), from the perspective of a systemic approach, most cybersecurity problems arise due to the lag of the modern legislative framework from scientific and technological progress.

Countries targeted by the largest number of cyberattacks in the world: USA, Ukraine, South Korea, China. In 2023, Ukraine was the target of Europe's largest share of state-sponsored cyberattacks. Regarding initiatives at the level of different countries, the (Global Cybersecurity Index, 2024) aptly states: "For countries working to achieve cybersecurity meaningful connectivity, the GCI offers a clear picture of where they are and a roadmap of activities to make progress. Countries must, however, be willing to engage in the ongoing processes of enhancing cybersecurity and working to enhance the quality and impact of their activities.

During the war with Russia and the political conflict with its allies, increasing the number and variety of cyberattacks from outside is possible, especially in critical sectors of the economy. In 2022, the number of registered cyber incidents was 2,194, in 2023 – 2,544, in 2024 – 4,315 (69.8% more compared to 2023). The most popular types of cyberattacks are DDoS, Ransomware, and Phishing. The forecasted growth of the cybersecurity market is from 138 million USD in 2024 to 208 million USD in 2029. For comparison, the cybersecurity market in Poland is 800 million USD. The strengths of the market are the unique experience in countering cyberwar, which allows Ukraine to share information with international partners; growth of digitalization in the public and private sectors, which

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 29, No 1 (2025), pages 7
https://doi.org/10.19192/wsfip.sj1.2025.7
Received: January 2025., Accepted: March 2025,
Published: March 2025

stimulates demand for cybersecurity products and services; and international support. Market weaknesses: lack of systematic funding due to military risks and low awareness in the field of cybersecurity; fragmentation of market offers, in particular, lack of cooperation between startups, incomplete legal regulation (IT Ukraine Association, 2024).

In 1st place in terms of the number of cyber incidents in Ukraine – the government and local authorities, in 2nd – the security and defense sector, in 3rd - telecommunications and IT, 4th place is shared by the media and energy sectors, in 5th – logistics and transport.

The results of the survey "The State of European supply chains 2024" (Reuters Events) showed that digital supply chain transformation is a high priority for 48% of European organizations and a top priority for 27%. In particular, one of European firms' 3 top digital transformation investment priorities is enhancing cybersecurity measures to protect against data breaches and cyber-attacks. According to the Global Cybersecurity Index 2024, Ukraine is in the "Establishing" group (score of 55–85) with higher score in legal measures and technical measures but lower in organizational measures and capacity development. These indicate the need to increase the number of educational programs for target audience and implement digitalization and cybersecurity strategies by businesses and entrepreneurs (Global Cybersecurity Index, 2024). In logistics companies, many processes, including inventory management, routing, order processing, and supplier interaction, occur through digital platforms. This increases the area of potential attacks. The use of warehouse management systems (WMS), transport management systems (TMS), and ERP creates many access points for attackers.

Since there are problems of lack of a digital security strategy, lack of interaction, and increasing threats, it is advisable to investigate: 1) what laws and programs are in force in this area; 2) what scientific developments are there that can be used to ensure the cyber resilience of supply chains and business as a whole; 3) which companies experience cyberattacks and what actions are companies taking to increase cyber resilience, etc.

II. METHODS

In this study, we use the analysis method of scientific sources, analytical data, and statistical information on the topics of digitalization, cybersecurity, and cyber resilience in companies and supply chains. Primary data was collected through a survey of companies to identify the state of cybersecurity in business. A descriptive research method and a generalization method were also applied to record and structure the study's general conclusions.

III. LITERATURE REVIEW

Cybersecurity is about protecting against cyberattacks that target a company's corporate networks. As for cyber resilience, experts define it as a company's response after a cyberattack and how it will recover. Cyber resilience, in addition to security, includes a number of processes and tasks related to brand and information technology protection, such as backup and disaster recovery, etc. The article (Kostromina M.O., Garnatko L.O., 2022) states: "Cyber resilience is a concept that combines business continuity, information system security, and organizational resilience. That is, the concept describes the ability to continue to achieve planned results despite complex cyber events, such as cyberattacks, natural disasters, or economic downturns." In global terms, cyber resilience goes beyond technical considerations and focuses on developing an effective immune system for each digital sphere. Common elements of cyber resilience include governance, access rights, segmentation, ensuring data integrity and confidentiality, proactive response to cyber incidents, recovery, and coordinated protection.

In this study, we will focus on the cybersecurity of companies, particularly supply chains. In July 2021, the EU Agency for Cybersecurity (ENISA) published the report "Threat Landscape for Supply Chain Attacks" (NISS, 2022): 1. The study analyzed 24 attacks and made a general conclusion that even the most advanced cybersecurity systems are not enough to protect organizations in the conditions of the current wave of AchLP deployment. 2. The fact that the risk of an increase in the number of cyber-attacks is increasing is also evidenced by the Microsoft 2022 report. It is opinion, that the continuation of the Russian-Ukrainian war and its cyber component will lead to a "more likely use of highly reserved capabilities, such as zero-day vulnerabilities, attacks on OKI or supply-chain attacks".

Supply chain attacks are spreading around the world:

- cyberattacks are aimed at supply chains with the aim of disrupting the work of related companies. For example, attacks can disable transport infrastructure or cause delays in the delivery of goods (WEZOM, 2023);
- logistics companies operate with sensitive information, in particular, the loss or compromise of this data can lead to disruption of operations, financial losses, lawsuits, loss of customer trust, additional costs to eliminate the consequences, partial or complete shutdown of business (WEZOM, 2023). For example, over the past two years, 63% of IT organizations have been victims of attacks on software supply chains, which indicates the scale of the problem (PROIT, 2024).

SCA (English Supply Chain Attack) – an attack on the supply chain. The main idea of SCA is to gain access to a company's data and/or control over its information system through its counterparties. The attack can be directed at both buyers and suppliers of the company. Among the suppliers, software vendors should be especially highlighted since through them, hackers can gain access to version control of the program code, and therefore malicious software can be distributed in the form of a legitimate program, and there is no 100% way to protect against such threats.

There are different types of attacks on supply chains, but they can be grouped into two fundamentally different approaches: 1) Software, i.e. attacks aimed at the source code of the supplier's software. In this case, hackers introduce malicious code into

applications and updates of legitimate software; 2) Hardware, i.e., attacks directed at devices, particularly routers, webcams, and keyboards, to bypass standard authentication procedures and unauthorized remote access. One of the common types of attacks on supply chains is a backdoor (back door), i.e., gaining remote access to devices and data while remaining unnoticed (Galushko O., Seliverstova T., 2022).

According to the Organization for Economic Cooperation and Development (OECD), in 2024, Ukrainian companies have the following main problems (Business.diia, 2024):

- an increase in the number of cyberattacks. The number of cyberattacks has increased significantly since the beginning of Russia's full-scale invasion of Ukraine. The losses caused to Ukrainian enterprises by cybercrime in 2023 amounted to more than 1 billion UAH. (which is 96% more than in 2021 and 62.5% more than in 2022);
- dependence on outdated software;
- insufficient data protection. Ukrainian legislation does not separately regulate the procedure for notifying personal data subjects or law enforcement agencies about personal data security breaches;
- low level of awareness among small and medium-sized businesses. Small companies are particularly vulnerable, often have limited access to technology and resources;
- lack of human resources. Even if companies are aware of the risks, many experience a shortage of qualified personnel to maintain cybersecurity at the proper level;
- lack of cyber resilience. The lack of a comprehensive digital security strategy and insufficient interaction with government agencies and other stakeholders hamper protective measures.

In many countries around the world, there are draft laws, legal regulations on cybersecurity and programs that help combat cyber threats. In Ukraine, some of them are the following: 1) The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017, as amended), which defines the legal and organizational foundations for protecting the vital interests of citizens, society and the state in cyberspace, establishes obligations for cybersecurity entities, including businesses, to protect information systems and networks; 2) Cybersecurity Strategy of Ukraine (2021–2025) – defines the directions of cybersecurity development, including cooperation between the state and the private sector to counter cyber threats; 3) Business Cyber Diagnostics Program of 07/12/2024 – launched by the Ministry of Digital Transformation of Ukraine, this program provides 500 Ukrainian companies with free digital infrastructure diagnostics services to identify vulnerabilities and increase the level of cybersecurity; 4) Public-private partnership in the field of cybersecurity. In particular, the State Service for Special Communications, in accordance with the Order of the Cabinet of Ministers, should soon propose a draft law on public-private partnership in the field of cybersecurity; 5) 08/30/2024 The government approved the decision on the "Strategy for the Recovery, Sustainable Development and Digital Transformation of Small and Medium-Sized Enterprises (SMEs) for the Period Until 2027", and also approved the operational plan of measures for its implementation for 2024-2027.

The country that leads the cybersecurity market – the USA – has numerous laws and programs on cybersecurity and cyber resilience, including:

1) Cybersecurity Information Sharing Act (CISA, 2015) – a law that promotes the exchange of information about cyber threats between private companies and the government.
2) The Cybersecurity Enhancement Act (2014) – focuses on cybersecurity research and standardization.
3) Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA, 2022) – requires critical infrastructure to report cyber-attacks to CISA (CISA, 2025).
4) Programs to increase awareness of citizens and businesses about cyber threats: National Cybersecurity Awareness Program (NCAP) (CISA, 2025) and Cybersecurity Framework at the National Institute of Standards and Technology (NIST, 2025), etc.
5) The USAID grant program provided grants to startups, developers, and companies offering innovative cybersecurity solutions, aimed at strengthening national preparedness and protecting Ukraine's critical infrastructure. Ukraine also established cooperation with the Cybersecurity and Infrastructure Security Agency (CISA). On January 20, US President Donald Trump signed an executive order temporarily suspending all US foreign assistance programs for 90 days pending reviews, including USAID.

The European Union has the following programs and documents:

1) The EU Digital Single Market Strategy (2015).
2) The EU Digital Europe Program (2021–2027). The Commission has proposed a path to the Digital Decade. The Digital Compass indicates four cardinal points for this trajectory: digital skills, secure and efficient digital infrastructure, digital transformation of business, and digitalization of public services. In September 2022, Ukraine signed an agreement to participate in this program, which is aimed at developing advanced digital skills, implementing digital technologies in enterprises and building digital infrastructure. Also, within the framework of the Digital Europe program, grants are provided to support projects aimed at developing cooperation and implementing legislation in the field of cybersecurity (DIIA, 2025).
3) The EU4Digital initiative is aimed at extending the benefits of the EU's Digital Single Market to the Eastern Partnership countries, including Ukraine. The initiative supports the development of a digital economy and society, including cybersecurity aspects (EU4Digital, 2025).
4) In 2018, The European Parliament adopted a resolution "Fighting Cybercrime", which states that Russia and China, through state and non-state institutions, are planning and implementing cyberattacks on the critical infrastructure of EU member states. In December 2020, the European Commission presented a new EU cybersecurity strategy. Cybersecurity is identified as a key factor for

building a resilient digital Europe, as well as for achieving the goals of the EU's strategic autonomy, provided that the open digital economy of the European community is preserved (Fediyenko O.P., 2024).

5) On 12.03.2024, the European Parliament approved new cyber resilience standards for the protection of digital products in the EU – the Cyber Resilience Act (EU Cyber Resilience Act of 15.09.2022). The document aims to ensure the safety, resilience and proper information on the cybersecurity of products. MEPs also emphasized the increased role of the EU Agency for Cybersecurity (ENISA) in identifying and managing vulnerabilities and incidents, and approved educational and training programs to improve professional skills in the field of cybersecurity (RNBO, 2024), etc.

From 2025, new regulations related to cybersecurity in logistics will come into effect in the EU, in particular the updated NIS2 Directive (27.06.2024) and the Digital Operational Resilience Act (DORA). This emphasizes the importance of enterprises adapting to new requirements for ensuring supply chain security (Logist.fm, 2024).

Participation in cybersecurity development programs and compliance with relevant legislation will help Ukrainian businesses more effectively counter cyber threats, strengthen their market positions, and integrate into the European digital space.

Another reinforcement is the fact that the IT sector is developing in Ukraine, whose companies are also actively involved in creating and improving solutions, increasing digital resilience and cyber resilience of companies. Educational organizations and logistics companies in Ukraine are also revealing this issue, developing analytical reports and advice to increase awareness of possible dangers. For example, RMRF, BDO, KLS, Logos 3PL.

Let's consider in more detail what solutions scientists have been researching and offering in the last 2-3 years in the field of digital business transformation and cyber resilience of supply chains. Scientists in Ukraine who study the optimization of supply chains, including through digitalization, are Chornopyska N.V., Hryhorak M., Palyvoda O.M., Kyrylenko O.M., Tereshchenko S.I., Kryveshchenko V.V., Khmurkovsky G.V., Zrybneva I.P., etc. Digital transformation and cybersecurity of business and supply chains are studied by Kryvovyazyuk I.V., Boychenko M.V., Boyko V.D., Galushko O., Kostromina M.O., Seliverstova T., Fediyenko O.P., etc. (Chornopyska N., 24). Scientists abroad also study this area.

Sazid R. et al. in their study reveal the assessment of cyber resilience of supply chains in the field of additive manufacturing using data fusion methods. As a result, a cyber resilience index for supply chains was developed, it was found that the use of data from different sources allowed to increase the accuracy of risk detection and reduce the impact of cyberattacks (Sazid R et all., 2021).

Malka N. Halgamuge considers the problem of using deep learning to increase cyber resilience in renewable energy and proves that deep learning helps to detect threats in real time and ensure the security of communications [Halgamuge M. N., 2024].

Tabansky L. and Lichterman E. investigated the implementation of a sectoral approach to cyber resilience for complex socio-technical systems. The authors proposed the PROGRESS model to increase interaction between sector participants, improved mechanisms for assessing cyber resilience through the analysis of the relationships between system components (Tabansky L., Lichterman E., 2025).

Cyber risk management strategies for ensuring cyber resilience and integration in supply chains are reviewed in (Jazairy A. et all., 2024). The authors substantiate how integration between chain participants reduces risks and improves operational resilience.

Sanni B. in his work described the impact of cyber resilience on the efficiency and continuity of electronic supply chains. According to the results of the study, companies with strong cyber resilient frameworks maintain stable operation during incidents (Sanni B., 2024).

Reynolds S. in his work notes that the digitalization of supply chains is accompanied by challenges such as data integration, cybersecurity, financial constraints and cultural resistance. Among the main benefits of digitalization are increased efficiency, risk prediction, and improved customer service. The author argues that the implementation of IoT, AI, and blockchain will increase transparency and security, while the challenges are high technology costs and a lack of qualified personnel (Reynolds S., 2024).

Castro J. P. (Director of Cybersecurity & Technology, LATAM) argues that organizations face constant cyber threats, and traditional prevention measures are insufficient to ensure resilience. The main problem is the need for rapid adaptation and recovery from incidents (Castro J. P., 2025). The study developed a cyber resilience model that includes: Zero Trust Architecture, which provides strict access control and constant monitoring; A cyclical approach - combining risk management, detection, and response to incidents. Red Teaming Exercises for testing cyber defense and Continuous Cyber Risk Scoring for assessing risks in real time are proposed.

Yeboah-Ofori A. et al. examine the complexity of cyber threats in supply chains, in particular due to interdependencies between different systems and vulnerability to attacks. The authors of the study propose to use machine learning methods (Logistic Regression, Decision Tree, Naive Bayes, etc.) to predict cyber threats. The results of the study showed an accuracy of 70% for threat prediction. Reducing the attack surface is proposed by identifying critical assets and using controls, understanding and predicting threats (Yeboah-Ofori A. et all., 2022).

IV. RESULTS OF THE SURVEY

As part of the study, a survey of 40 companies in Ukraine was conducted in January-February 2025 on the state and prospects of cybersecurity in companies in order to identify what measures are applied in companies, what obstacles there are on the way to implementation, etc. Among the companies

that provided answers are companies operating in the fields of IT, logistics and transport, marketing, energy, trade, medical care, education, construction, financial services and consulting, etc. The companies involved have 6-20 employees (23,5%), 21-50 (15%), 51-100 (15%), more than 100 people (47,5%).

Employees assess the level of digitalization of their companies as very high (40,0%), high (37,5%), average (12,5%), low (7,5%), very low (2,5%). The lower level and average were indicated by companies with less than 50 employees.

The following results were obtained for the question "How important is it to implement cybersecurity measures and build a company's resilience to threats to the company's information systems and the entire supply chain (where 1 – is not important at all, 5 – is very important)" (Chart 1.).

Most companies answered "very important": for the company – 62,5%; for the supply chain – 57,5%); answers "important" - 27,5% and 30,0% respectively; "average" – 7,5% for the company, 12,5% for the supply chain; "not important" – 2,5% for the company, 0% for the supply chain. The answers differ slightly in the importance of cybersecurity measures for the company and the supply chain (2 more companies gave an importance rating of 3 for the supply chain than – these are companies providing services).

The results described above indicate that among the Ukrainian companies studied, there is an apparent belief in the importance of cybersecurity measures. Moreover, understanding the interdependence of business entities in establishing and implementing current cooperation, the requirements for cybersecurity within companies are almost the same as similar requirements for partners at all levels of the supply chain.

At the same time, an in-depth analysis indicates a somewhat simplified interpretation of the security issue in cyberspace, using primarily the simplest methods of threat prevention. The surveyed companies most often use data backup, use of only authorized applications as cybersecurity measures and multi-factor authentication, as well as other measures – only half and less of the companies (Chart 2).

CHART 1. THE IMPORTANCE OF CYBERSECURITY MEASURES FOR THE COMPANY AND THE SUPPLY CHAIN

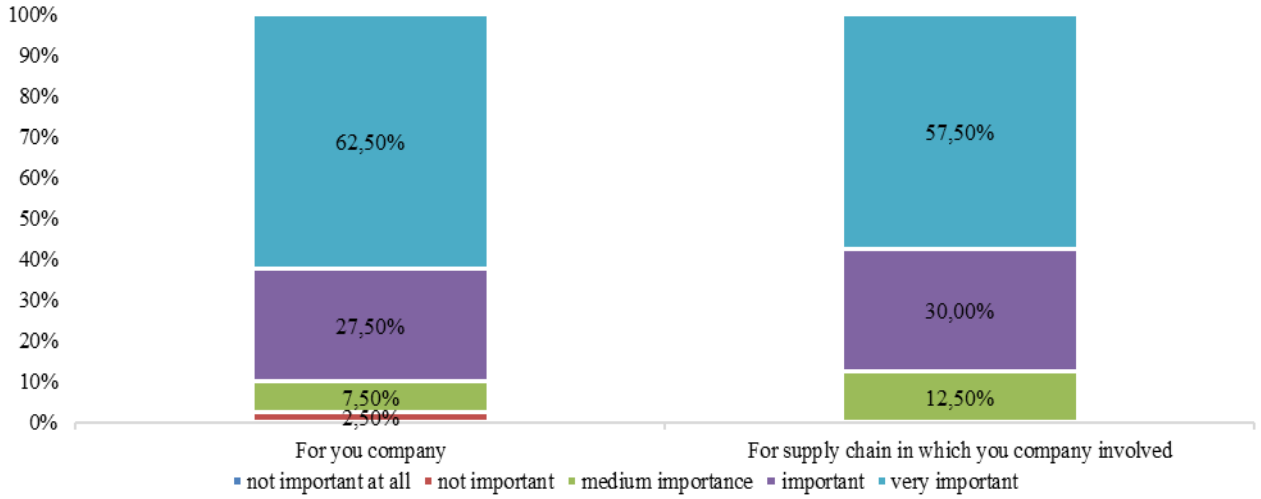
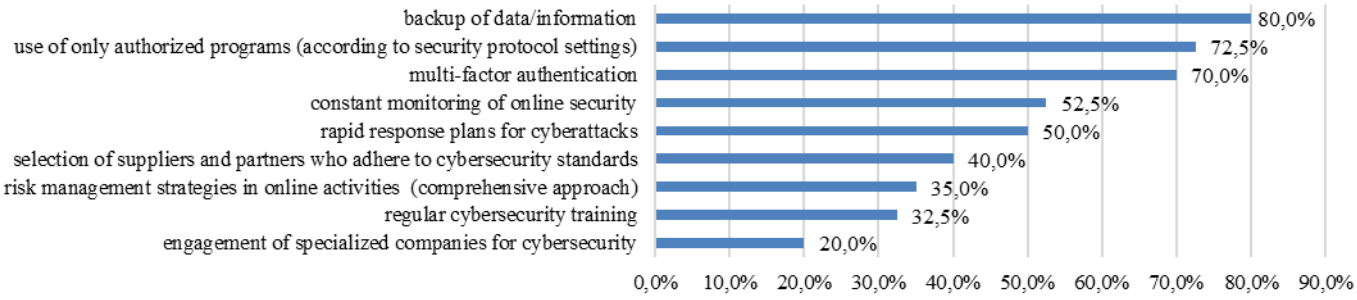


CHART 2. CYBERSECURITY MEASURES USED BY COMPANIES



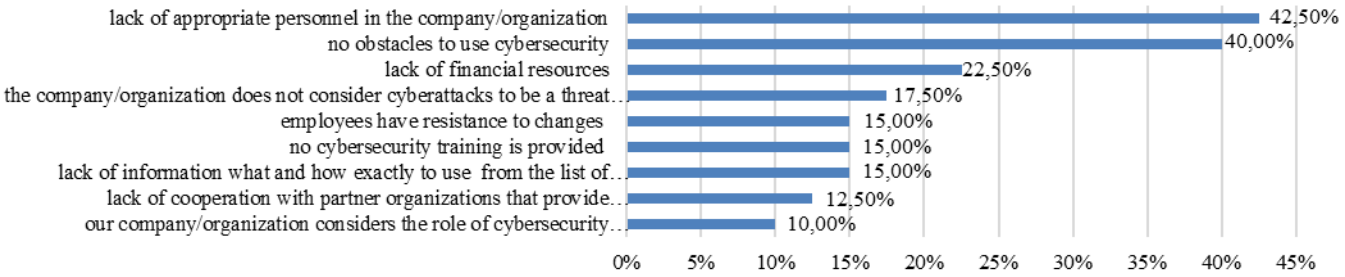
Therefore, the methods used by Ukrainian companies to ensure their cybersecurity, in most cases, provide only a prompt response to the threat that has occurred. In our assessment, the measures they implement as part of proactive actions are insufficient.

Cyberattacks occurred in 37,5% of surveyed companies (which operate in the IT, education, energy, construction, e-commerce, printing, insurance, and other services sectors). Companies reported that they had the following types of cyberattacks: Data corruption that was not recoverable, Service outage for more than 48 hours (DDoS); about 2 times per month, 1-3 of the sites the company works with are subject to

cyberattacks. They occur due to request overload and the sites' active protection is turned on, which annoys customers; Phishing that compromised access to the email service; Petya virus; Reputational losses; Personal data leaks; Financial.

The obstacles to implementing cybersecurity measures in companies are as follows (Chart 3.):

CHART 3. BARRIERS TO IMPLEMENTING CYBERSECURITY MEASURES



The personnel problem is the biggest obstacle to overcoming the problems with the cybersecurity of Ukrainian enterprises. This indicates that the issue of this type of security is still relatively new for Ukraine, and it has not been given enough attention in recent years. As a result, there is a shortage of personnel with specialized knowledge at the appropriate level.

Regarding cybersecurity awareness and the need to improve it, employees of the surveyed companies periodically undergo training (47,5%), plan to undergo training (10%), or cybersecurity is solely the responsibility of an outsourcing company (10%). Those companies that chose the answer “I do not know about training programs” (12,5%) are companies with 6-20 employees, those that chose the answer “I know, but do not plan to train” (12,5%) are companies with different numbers of employees.

According to the survey results, most companies consider cybersecurity important, both for the company and for the supply chains (Chart 1), however, most companies implement only basic, basic measures (Chart 2.). While 40% of companies responded that they had no obstacles to implementing cybersecurity measures (Chart 3.), some companies reported a lack of appropriate personnel (42,5%) and some companies reported a lack of financial resources (22,5%) - (and this was the response of companies of different sizes and fields of activity).

V. CONCLUSIONS

Therefore, this research made it possible to identify points that are important for companies on the path to building cyber resilience - by surveying companies, what strategies and methods for managing cybersecurity have been developed by scientists, and what programs companies can follow to increase staff awareness and implement more modern cybersecurity technologies. Also, the information collected in scientific publications and practical cases allowed us to structure the main recommendations that companies may use to implement or improve cybersecurity, in particular (Kostromina M.O., 2022; Chornopyska N., 2024; Yeboah-Ofori A. et all., 2022; Sazid R, 2021; Halgamuge M. N., 2025; Sanni B., 2024; Galushko O., 2022; Jazairy A., 2024; Castro J.-P., 2025; Tabansky L., Lichterman E., 2025):

1) Timely update of all software and operating systems; installation and correct configuration of antivirus and desktop firewalls; compliance with all compliance standards to protect confidential user data; ensuring the security of services and devices from numerous malicious actions; blocking all computer screens.
2) Modern security technologies and regular updates of device and network security: multi-factor authentication, data encryption, monitoring, offline backup, risk assessment and regular security audits, creating a single platform for information exchange between supply chain participants (Sazid R, 2021). Security protocols that allow only authorized programs to be launched (Galushko O., 2022).
3) Risk assessment. Conducting regular cyber risk assessments in supply chains, developing rapid response and recovery plans to ensure continuity of operations, using DDoS protection, antivirus solutions (Sanni B., 2024). Risk management strategies - vulnerability assessment and recovery plans, using data protection technologies, particularly encryption and monitoring automation (Jazairy A., 2024). Review recovery plans for public relations issues caused by a third-party cyberattack (Kostromina M.O., 2022).
4) Selecting reliable suppliers. Cooperating with suppliers that adhere to high cybersecurity standards and have appropriate certificates. Developing comprehensive cooperation models to integrate supply chain and third-party risks, introducing feedback loops between components for self-correction of systems (Tabansky L., Lichterman E., 2025).
5) Security standards. Applying international cybersecurity standards, such as ISO 27001, to ensure adequate information protection.
6) Blockchain (Galushko O., 2022; Chornopyska N., 2024).
7) Monitoring and response. Setting up real-time network monitoring to detect suspicious activities, regular penetration testing. In particular, continuous monitoring of systems using deep learning algorithms to detect

anomalies, creation of data quality management systems to improve the accuracy of security models (Halgamuge M. N., 2024). The importance of maintaining flexibility of system architecture and its adaptability to changes is emphasized. Using risk analysis to identify vulnerabilities (Yeboah-Ofori A. et all., 2022).

8) Personnel training. Conducting training for employees on recognizing and responding to cyber threats (Kostromina M.O., 2022; Sanni B., 2024). The importance of learning after incidents to improve security strategy is emphasized. Cyber resilience depends on the full integration of people, processes and technologies (Castro J.-P., 2025).
9) Adaptation to new regulations. Logistics companies should use the transition periods to adapt to new rules and train staff to meet the requirements of the NIS 2 and DORA regulations, which will come into force in 2025 (Jazairy A., 2024), etc.

There is a lot of methodological and practical advice in the research of scientists, especially of a technical nature for cybersecurity, but it is also worth developing management approaches to the formation of cyber resilience. Prospects for further scientific work are structuring the main management decisions for creating the cyber resilience of companies, in particular, determining priorities taking into account various factors of the external and internal environment.

The authors declare no conflict of interest.

VI. References

Boyko V.D., Vasylenko M.D., Kukharenko S.V. Cybersecurity in the EU and member states: genesis and problems of its improvement. Informacijna bezpeka lyudyny, suspilstva, derzhavy 2019, № 3, pp. 57-69.

Business.diia. Available online: https://business.diia.gov.ua/history-of-success/zakhyst-kompanii-vid-kiberzahroz-bezoplatni-posluhy-dlia-ukrainskoho-biznesu (accessed on 08.01.2025).

Castro J-P. Cyber Resilience - The Learning Phase of the Cybersecurity Compass Framework. Blog Trend Micro 2025. Available online: https://www.trendmicro.com/en_us/research/24/h/cyber-defense-strategy-framework.html (accessed on 15.01.2025)

Chornopyska N., Slobodzyanyk R. Digitalising supply chains: technology security or security technology. Marketing and logistics in the management system: challenges of digital globalization (in memory of Professor Yevhen Krykavskyy): abstracts of the XV International Scientific and Practical Conference, Lviv, Ukraine, 17-18 October 2024, pp. 443-444.

DIIA. Available online: https://business.diia.gov.ua/finance/program/programa_es_cifrova_evropa_2021_2027 (accessed on 12.01.2025).

EU4Digital. Available online: https://eufordigital.eu/uk/discover-eu/the-eu4digital-initiative/ (accessed on 14.01.2025).

Fediyenko O.P. European experience in legislative support for strengthening cyber resilience. Informaciya i pravo 2024, № 2(49), pp.178-189.

Galushko O., Seliverstova T. Cybersecurity in supply chain management (SCM). Naukovyy visnyk DSUIA. Special edition № 2. Derzhava i pravo v umovah vijskovogo stanu, 2022, pp.537-542.

Global Cybersecurity Index 2024, 5th Edition. Available online: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (accessed on 08.01.2025).

Halgamuge M. N. Leveraging Deep Learning to Strengthen the Cyber-Resilience of Renewable Energy Supply Chains: A Survey IEEE Communications surveys & tutorials, third quarter 2024, vol. 26, №3, pp. 2146–2175.

IT Ukraine Association. Available online: https://itukraine.org.ua/ukrayinskij-rinok-kiberbezpeki-zris-u-chotiri-razi-za-visim-rokiv/ (accessed on 08.01.2025).

Jazairy A., Manuj I., Goldsby T.J. Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness. International Journal of Physical Distribution & Logistics Management 2024, №54,11, pp.1-29.

Kostromina M.O., Garnatko L.O. Cyber resilience and cybersecurity: what's the difference. Suchasnyy zakhyst informaciyi 2022, №4 (52), pp.71-75.

Logist.fm. Available online: https://logist.fm/news/u-2025-roci-pochnut-diyati-novi-reglamenti-kiberbezpeki-u-logistici (accessed on 15.01.2025).

Myronova M. Analysis of the development of the digital economy in the world and in Ukraine. Mizhnarodnyi naukovyi zhurnal "Internauka". Seriia "Ekonomichni nauky", Shevchenko Scientific Society, Economic collection 2022, vol. 68, pp. 93–101.

NISS. Available online: https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/ataky-cherez-lantsyuzhky-postavok-formuvannya-stratehichnoyi (accessed on 11.01.2025).

NIST. Available online: https://www.nist.gov/ (accessed on 14.01.2025).

PROIT. Available online: https://proit.ua/63-it-orghanizatsii-stali-zhiertvami-atak-na-lantsiuzhki-postachannia-pz-za-ostanni-dva-roki-opituvannia/ (accessed on 12.01.2025).

Reynolds S. Examining the Challenges and Opportunities of Supply Chain Digitalization: Perspectives from Industry Leaders. Preprints 2024, pp.1-12.

RNBO. Available online: https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2024/Cyber%20digest_Mar_2024_UA.pdf (accessed on 15.01.2025).

Sanni B. Impact of Cyber-resilience on E-supply Chain Performance and Operational Continuity. Research gate 2024, pp.1-10.

Sazid R, Ullah Ibne Hossain N., Govindana K., Nurf F., Bappy M. Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: A model to generate cyber resilience index of a supply chainCIRP Journal of Manufacturing Science and Technology 2021, №35, pp. 911-928.

Tabansky L., Lichterman E. Progress: the sectoral approach to cyber resilience. International Journal of Information Security 2025, №24 (18), pp.1-11.

WEZOM. Available online: https://wezom.com.ua/ua/blog/kiberataki-na-lantsyug-postavok-v-logistitsi-vpliv-ta-naslidki (accessed on 11.01.2025).

Yeboah-Ofori A., Swart C., Opoku-Boateng F, Islam S. Cyber resilience in supply chain system security using machine learning for threat predictions. Continuity & Resilience Review 2022, Vol. 4 No. 1, pp. 1-36.

CISA. Available online: https://www.cisa.gov/ (accessed on 14.01.2025).