European Research Studies Journal
Volume XXIV, Issue 2B, 2021

pp. 240-256

Cybersecurity as the Main Challenge to the Effective Use of Digital Technology Platforms in E-Commerce

Submitted 19/03/21, 1st revision 17/04/21, 2nd revision 28/05/21, accepted 10/06/21

Krzysztof Bartczak[1]

Abstract:

Purpose: *The article discusses the issues related to the use of digital technology platforms in e-commerce. It focuses on presenting the challenges associated with ensuring security in this area of commerce and looks at the threats that may emerge during the conduct of e-commerce business and the use of digital technology platforms, as well as their impact on how the management of e-commerce businesses views the platforms.*
Design/Methodology/Approach: *In addition to theoretical considerations, the article presents the results of the author's research study, which covered a sample of 120 businesses – beneficiaries of the Innovative Economy Operational Programme in the area of implementation and development of digital technology platforms. The research was based on computer-assisted telephone interviewing (CATI) and resulted in producing a model of attitudes towards digital technology platforms.*
Findings: *It further demonstrated that the use of such platforms in e-commerce might entail certain risks as a result of possible data theft as well as hardware and network failures. Failures of this sort were one of the main reasons behind the negative attitude towards digital technology platforms among the management staff of the businesses covered by the study.*
Practical Implications: *It is, therefore, essential to take actions to neutralize the threats above. This could be achieved by adopting formal security policies and implementing various systems and tools, including such designed to protect users from malware.*
Originality/Value: *In the specific case of digital technology platforms, the process could be accelerated with the help of users who could participate in bug bounty programs such as those implemented by Google or Facebook.*

Keywords: *E-commerce, digital technology platforms, challenges, threats, cybersecurity.*

JEL Classification: *O31, O32.*

Research type: *Research article.*

[1] *Faculty of Management, Warsaw University of Technology, Warsaw, Poland* *krzysztof.bartczak@pw.edu.pl*;

1. Introduction

In this day and age, when speaking of economy, it is common to use the term 'digital economy. This term can take on several meanings, among them the possible ways in which digital technologies can be used in economy or the existence of digital infrastructure consisting of IT networks, devices, and digital applications and systems designed for data management, which enable users on individual markets to make contact and enhance cooperation (Digital Economy Report, 2019)

Several different components underpin the digital economy. These include information and communication technologies (ICT), data transmission and exchange tools (smartphones, tablets, laptops), or robotics and automation technologies. Bukit and Heeks (2017) added new digital models – a category to which they assigned digital platforms. The latter include digital technology platforms (DTPs). Due to their immense popularity and great usefulness for commercial and personal use alike, these platforms serve an essential role in the development of the contemporary economy, for instance, by contributing to the strengthening of relationships between particular actors on the market and by stimulating innovation (Ciriello, Richter and Schwabe, 2018).

One of the most significant challenges of using digital technology platforms (which holds for the entire e-commerce industry and digital economy) is cybersecurity. In the digital environment, security is exposed to many threats; it is, therefore, essential to implement effective countermeasures (Spremić and Simunić, 2018; Hopper *et al.*, 2016). This article discusses such threats in the context of digital technology platforms and argues whether cybersecurity is an obstacle to the effective use of DTPs in e-commerce. The focus here is on two essential matters. The first one is to provide an overview of the essence of the threats mentioned above. The second one is to determine whether these threats act as determinants of the attitudes towards DTPs among the management staff. In this regard, the author conducted their research that resulted in producing a model of attitudes towards digital technology platforms.

2. Literature Review

Although the term 'digital technology platform' is not new, it has not been adequately defined. One of the reasons for this situation is that individual authors use several terms with similar meanings. These include, for instance, digital platforms, seven digital business technology platforms, eight or – strictly in the context of electronic commerce – e-commerce platforms (Huo, Chen, and Yang, 2016). It should be further noted that the market abounds in various platforms, and new ones are still being developed, making it even more difficult to pinpoint their ever-changing character and basic features.

Many authors attempted to come up with their definitions of digital (technology) platforms. Gawer10 defined DTP as a building block (foundation, primary function) of an (IT, technological, etc.) system that makes it possible to implement new functionalities and develop complementary products, services, or technologies. In literature, DTPs, or, more broadly speaking, digital platforms, are also viewed as tools used to make contact and strengthen relationships between various market participants, including entrepreneurs, customers, or even public administrative authorities. These actors are offered the opportunity to enter into transactions, including business ones, and communicate with each other through the Internet. As a direct result, market participants become business partners and form business networks (Sun Keating and Gregor, 2015). Therefore, the purpose of DTPs is to enable the interaction between various stakeholders (Constantinides, Henfridsson, and Parker, 2018).

Due to the multitude, complexity, and diversity of definitions of DTPs, this article provides an original interpretation that draws on the definitions already in existence. According to this interpretation, the platforms are electronic (digital) tools that can take the form of services or content and can be used to lay the foundations for making contact and strengthening relationships between various market participants, and, as one of the most critical features, offer the possibility to expand them by adding new modules or functionalities.

As the article mentions e-commerce platforms, it is practical to define this term. According to the International Trade Centre (ITC) (Jansen *et al.*, 2016), e-commerce platforms connect buyers and sellers of products or services by enabling the former to increase the visibility of their products or services and reach more leads and customers while providing the latter with the opportunity to browse through numerous offers from various sellers in different locations and to use price comparison tools.

In a report by OECD (2014), it was pointed out that such platforms enable integration between sellers and buyers of products and services and make it easier for them to enter into transactions via the Internet. E-commerce platforms help to create more opportunities on the market, primarily by providing the option to sell products and services virtually on a global scale. More importantly, the platforms feature several functionalities that, on the one hand, aid in making purchase decisions and building a positive brand image on the market (review and rating tools) and on the other, enable customers to choose products that suit their needs (deal matching tools and search results in a web browser).

E-commerce platforms can also be defined as service ecosystems that generate mutual benefits and enable the co-creation of value by various actors involved in the operation of the platforms, such as website owners, sellers, customers, managers, developers, or even other competing platforms. The platforms enable users to exchange resources and thus generate specific benefits, including increased innovation (Botti and Maione, 2018).

A subcategory of e-commerce platforms are social business platforms, nine also known as social media platforms (Curzi, Lecoq, and Noémier, 2016), i.e., platforms based on social media such as Facebook. Their principal characteristic is that users are actively involved in their creation and operation. In the context of the e-commerce industry, it consists of the users' sharing information about individual products or services and promoting them among other users in a way that can influence purchase decisions related to such products or services.

The Use of Digital Technology Platforms in E-Commerce and the Problem of Cybersecurity: It is virtually impossible to run an e-business, especially in the e-commerce industry, without using a digital platform. The platforms offer sellers a unique opportunity to reach a wider audience, enabling them to grow their commercial business, expand into new markets and acquire new customers. Moreover, with DTPs, it is easier for businesses to keep up with technology changes as they implement and constantly upgrade innovative solutions in the area of, e.g., customer order management or payment. By that, they contribute substantially to increasing competitiveness (Hristoski *et al.,* 2017).

There are close connections between the e-commerce industry and DTPs. They manifest in the fact that e-commerce is primarily based on the operation of such platforms. According to V. Apte (2018) provides essential digital tools for electronic commerce while enabling its intensification and accomplishment of the strategic objectives of e-commerce businesses. Businesses use DTPs as a way to build their strategies and expand the range of business transactions (Al-Ani, 2009). Examples include Amazon, eBay, AliExpress, Mercado Libre, Rakuten, TMall, or Allegro, sometimes called online marketplaces (Merton, 2020). DTPs enable contact and closer cooperation between sellers and buyers, and that fosters business growth.

Importantly, not all platforms require users to pay to be able to access and sell their products. Some are available as Free and Open Source Software (FOSS). Using Magento, PrestaShop, OsCommerce, or OpenCart, users can create and develop their online store (Ferreira, Pedrosa, and Bernardino, 2018; Rohilla, 2014). Similar platforms offer a wide range of functionalities, including e-commerce website administration, marketing tools, SEO support, development of various payment systems, or access to statistics and reporting, which attract many commercial businesses that use them at practically no cost.

The ITC mentioned above report (Jansen *et al.*, 2019) points to the following significant factors that contribute to the development of digital technology platforms for e-commerce:

- Ability for sellers to reach a wider market – a characteristic feature of each platform is that it has a global nature, which means that it can be accessed from any location where the Internet is available.
- Ability to conduct market research through the platform and, consequently, match products and services to customer needs, also in terms of the price.

- Credibility – by requiring sellers to register and verifying their details, platforms authenticate sellers and ensure legitimacy of transactions.
- Reputation – the platforms offer seller rating systems that help sellers build reputation among buyers (provided that the sellers ensure professional handling of transactions) and alert buyers to dishonest sellers.
- Security – security of online payments.

Therefore, security has been listed as one of the factors that drive the development of DTPs for e-commerce. In this context, it refers to cybersecurity, defined in the literature in multiple aspects (Craigen, Diakun-Thibault, and Purse, 2014). One such definition says that it involves minimizing the risk of exposure to attacks carried out by computer or web-based malware. The risk can be neutralized using various systems and tools, including antivirus, encryption, or authentication software (Amoroso, 2006). This definition seems too narrow. In addition to cyberattacks on networks or computers, cybersecurity addresses many other threats such as cyber terrorism or failures of telecommunications infrastructure.

Given the above, it seems more reasonable to use the definition proposed by Seema, Nandhini, and Sowmiya (Seemma, Nandhini, and Sowmiya, 2018), which states that cybersecurity means the protection from all sorts of threats, designed to maintain confidentiality, integrity, and availability of data held by an entity. Such protection aims to reduce the risk of exposure of the entity to a cyberattack or failure. Characteristically, the protection is not limited to virtual space, but it extends to physical threats (for instance, unauthorized access to data stored on a CD).

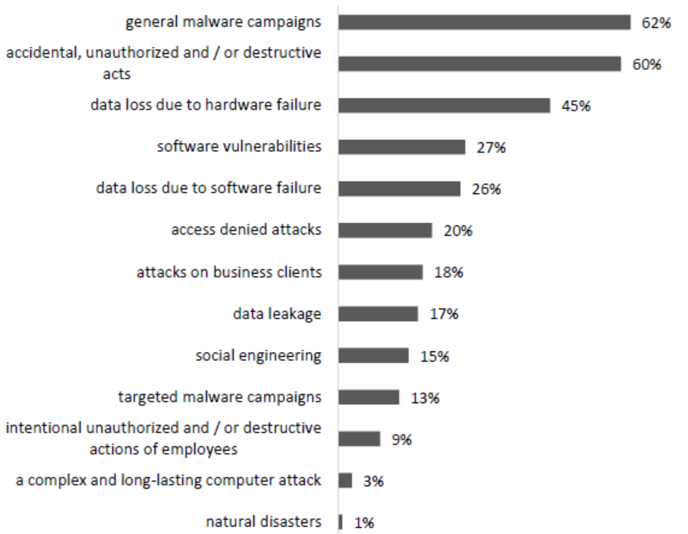
There is voluminous literature on cybersecurity threats faced by e-commerce businesses. Rahman and Lackey (2013) distinguished the following risks:

- Direct financial loss: fines or other legal repercussions that could occur due to a violation of regulations or contracts about e-commerce business.
- Indirect loss: loss of credibility among business partners and customers due to security issues; loss in productivity due to failure or unavailability of e-commerce systems; disclosure of confidential information, including trade secrets, as a result of theft; blackmail involving the takeover of a business's system and demand for compensation to restore it to regular operation.
- Technical issues: damage to files or systems, incorrect configuration of systems or applications stored on servers.

In the context of the challenges above and threats, Khan (2019) paid particular attention to the risk of unauthorized access and use or even destruction of data collected by e-commerce businesses. These comprise technical attacks (for instance, a teardrop attack that causes systems to crash or brute-force password attack, submitting all possible passwords to hack into an account) and non-technical attacks (phishing or social engineering) (Patel and Lakhtaria, 2017). Other authors pointed to threats to privacy and confidentiality of data and their significant impact on levels of trust in the services of online stores among customers (Marchany and Tront, 2019).

There are several different reasons and motives for the emergence of cybersecurity issues in e-commerce and other areas. They include intentional actions of specific people or groups of people designed to steal data for ransom, using methods similar to terrorism (cyber terrorism) to achieve a specific effect, including psychological impact (instilling fear in societies), or expose authorities to ridicule or generate publicity (hacktivism) (Ablon, 2018). In this context, mention should be made of the so-called mixed motives, which are becoming more and more common in the virtual environment, especially among computer criminals (Patton *et al.*, 2019). Another aspect worth mentioning is the insufficient efforts to protect computer systems and networks from all sorts of failures that may occur due to reasons other than cyberattacks, such as neglect on the part of businesses. Such neglect may lead to hardware or software failures (Kremer *et al.*, 2019), a common problem being the use of obsolete technology and the management's failure to address the need to modernize computer hardware and software (Özkan and Bulkan, 2019). In this context, it seems expedient to mention the results of a study conducted by Gliń and Stasiak-Betlejewska (Gliń and Stasiak-Betlejewska, 2019).Figure 1 presents its findings.

Figure 1. *Cybersecurity threats according to study conducted by Gliń and Stasiak-Betlejewska.*



Source: *Own study.*

The study found that the most significant cybersecurity threats were general malware campaigns (62%), accidental or unauthorized acts, including such of employees (60%), hardware failures leading to data loss (45%), software vulnerabilities (27%), potentially caused by obsolete technology, and software failures (26%).

Due to the multitude of security challenges and threats facing e-commerce businesses, it is essential to neutralize them. In addition to various antivirus software and systems, users can apply specific standards. Such standards aim to ensure CIA, that is, Confidentiality, Integrity, and Availability of data. Standards worth mentioning include ISO/IEC 27001 and ISO/IEC 29100, and PAS standards: 555:2013 and 754:2014 (Parn and Edwards, 2019). It is also advisable to formulate a written policy outlining the safety rules for the digital environment, implement physical security measures such as video surveillance and access control systems (password or biometric scanners), or use authentication systems or even cryptography solutions (hashing, i.e., encrypting data and creating a unique key) (Rahman and Lackey, 2013). In 2018 KPMG conducted a study on the security measures that should be implemented (by e-commerce and other businesses) to ensure security in the digital environment (KPMG, 2018). Figure 2 below presents the findings.

Figure 2. *Advisable investments in the security of digital environment of Polish businesses according to 2018 study conducted by KPMG.*

Source: *Own creation.*

The solutions identified as the most useful in eliminating cybersecurity threats in the perspective of coming years were application of business continuity plans containing an outline of procedures to follow in case of failure or data leakage, implementation of malware protection, ensuring the security of the Internet connection, and responding to all security incidents, even those which on the surface have no adverse impact on the business operations.

3. Research Methodology

The author conducted their research on the use of DTPs in e-commerce. The study investigated how DTPs contribute to developing new business models and looked at certain aspects of cybersecurity. The study was conducted on 18-28 February 2019 using computer-assisted telephone interviewing (CATI). CATI is a quantitative survey characterized by a high level of standardization. Its primary advantage is that the results of surveys are generalizable to the entire population (Gerring, 2001). The quantitative information collected through computer-assisted telephone interviewing (CATI) was subject to quantitative analysis in line with the classic paradigm for this kind of research. In the first step, the data was subject to tabular analysis using two-variable tables. Inductive analyses of differences between groups followed the analysis.

The research was based on a survey questionnaire containing 23 questions, which was provided to representatives of 120 businesses that had received funds for the implementation and development of digital technology platforms from the Innovative Economic Operational Programme. It should be noted that 28 (23.1%) of the businesses included in the sample operated in the commercial sector. Some of them engaged in e-commerce.

One of the questions concerned the signs of negative attitude towards the implementation and use of digital technology platforms among the management staff of the respondents. The answers of the respondents are summarised in Table 1.

Table 1. *Signs of negative attitude towards the implementation and use of DTPs among the management staff of the respondents.*

Question 7. Please indicate how the negative attitude towards the implementation and use of digital technology platforms within your organisation manifests among the staff.				
		Answers		Percentage of observations
		N	Percentage	
	considerable resistance related to the phase of implementation of digital technology platforms due to potential changes in the organisational structure and employment within the organisation	2	40.0%	100.0%
	multiple concerns associated with financial aspects (high implementation costs and potential cuts in other functional areas of the organisation)	1	20.0%	50.0%
	multiple concerns associated with cybersecurity	2	40.0%	100.0%
Total		5	100.0%	250.0%

Source: *Own creation.*

40% of the respondents stated that the reluctance towards using digital technology platforms among the management staff was due to concerns related to cybersecurity. It is noteworthy that these concerns were indicated alongside organizational and employment issues as the most prominent sign of the management's negative attitude towards the use of DTPs within their organizations. It suggests that cybersecurity and the risks involved in it pose one of the biggest obstacles in the path of widespread and unlimited use of digital technology platforms within organizations, including e-commerce businesses.

During the CAT interviews, the respondents were also asked about cybersecurity-related consequences that their organizations suffered due to using digital technology platforms. The results are shown in Table 2.

Table 2. *Consequences of using DTPs for cybersecurity.*

Question 8. Please indicate whether any of the following negative events or cybersecurity threats occurred within your organisation as a direct consequence of the implementation of digital technology platforms.				
		Answers		Percentage of observations
		N	Percent age	
	hardware failure	65	36.1%	53.7%
	network failure, e.g., due to an overload caused by digital technology platforms	43	23.9%	35.5%
	leakage of business, employee or business partner data	6	3.3%	5.0%
	leakage of customer data	6	3.3%	5.0%
	phishing, i.e., posing as a legitimate institution on the web	12	6.7%	9.9%
	pharming, i.e., misdirecting users to fraudulent websites and web servers	10	5.6%	8.3%
	loss of money	6	3.3%	5.0%
	cyber spying	3	1.7%	2.5%
	none	28	15.6%	23.1%
Total		180	100.0%	148.8%

Source: *Own creation.*

Only 28 respondents (15.6%) stated that their organizations had not experienced any adverse events due to the implementation and use of digital technology platforms. Therefore, as many as 92 respondents, i.e., 84.4% of the sample, reported such events. In most cases, they reported hardware failures (N=65, 36.1%) or network failures (N=43, 23.9%) that could have resulted from the network being overloaded by DTPs. Data leaks and attacks are known as phishing, and pharming was far less common.

Therefore, it must be acknowledged that DTPs were the source of numerous cybersecurity threats for the businesses covered by the study. However, most of the reports concerned failures of computer hardware and networks. In the specific case of e-commerce businesses, failures of this sort can prevent normal operations and lead to downtime. This is likely to have repercussions on fulfilling customer orders and promoting a positive brand image on the market. For the preceding reasons, it is essential to prevent potential failures effectively.

In addition to CATI, the author's research study was based on regression analysis with categorical variables (categorical regression, CATREG) to quantify categorical data and optimal scaling (measuring particular variables based on other variables), leading to the production DTP model. The model was used to measure the attitudes towards digital technology platforms within organizations based on the assumption that the cybersecurity factor, related to new IT challenges associated with hardware and software, would be one of the dimensions in which the organization could be subject to transformation as a result of the use of digital technology platforms.

This issue was addressed in Question 8 of the survey "Please indicate whether any of the following negative events or cybersecurity threats occurred within your organization as a direct consequence of the implementation of digital technology platforms." In the case at hand, the variable had a nominal measurement scale (multiple choice question). However, it was converted to a variable measured on a ratio scale (number of reports).

The production of the model was completed in several phases. They followed a top-down approach with the following steps:

- Embedding in the model a set of variables (including cybersecurity) which, according to the author, impact the independent variable (attitude towards DTPs).
- Reordering variables by repetition of iterations to achieve the highest possible result.
- Model building and evaluation.
- Reducing the number of variables by eliminating the weakest predictor.
- Reduced model building.
- Comparing the previous and modified (reduced) models.
- Repeating steps 4 to 6 until the numerical results are considered satisfactory.

Thanks to the model it is possible to determine which factors have the greatest impact on the attitudes towards digital technology platforms. In the context of the cybersecurity dimension, the following measures were adopted:

- Beta coefficient (β), also called standardized regression coefficient (independent of the involved variable, computed using the slope coefficient).
- Allows for comparison of individual predictors on a regression model, its value ranges from -1 to +1, where any value close to zero indicates a weak, or non-existent correlation between the predictor and the dependent variable.
- Significance – a parameter used to describe individual predictors.
- F-statistic – a summary measure of the goodness of fit representing the ratio of variance; as a model is built, variables with the lowest F-statistic are eliminated in sequence.
- Correlation matrix – it shows zero-order correlations, partial correlations, and semi partial correlations, zero-order correlations are isolated correlations between an independent variable and a dependent variable, in partial

correlations, the predictor and dependent variable are correlated with other variables in the model, while semi partial correlations involve controlling for the interaction between an independent variable and other variables in the model. However, they do not consider the correlation between the dependent variable and other predictors; the correlations can take on values between -1 and +1.

– Validity – it represents the significance of individual variables in the model; it can take on values up to one (1 being the maximum value); the higher the validity of a predictor, the higher its importance in the model; it can be expressed as a percentage.
– Tolerance – it is a measure of collinearity of variables; it is the inverse of R^2 (tolerance = $1 – R^2$) and takes on values from 0 to 1; the closer the predictor value is to one, the lower the degree of collinearity between the predictor and other variables in the model; collinearity is a phenomenon that should be avoided – the closer it is to zero, the higher the extent to which a variable is excessive and provides redundant information. In an ideal model, variables should be highly correlated with the dependent variable, but only slightly correlated with each other; an essential phase of model building is model validation – it requires identification and handling of outliers; CATREG models are susceptible to outliers Table 3 presents the values of the above measures for each analysed dimension, that is, cybersecurity, the structural factor, the structural-demographic factor, the human factor, and the economic factor.

Table 3. *Factors influencing attitudes towards digital technology platforms*.

Name of model component (predictor)	Beta coefficient	Number of degrees of freedom (df)	F	Significance	Zero-order correlation
Structural (socio-demographic) factor	0.261	0.201	1	10.682	0.197
Structural factor	0.147	0.163	3	0.816	0.488
Human factor	0.141	0.163	2	0.749	0.475
Economic factor	0.070	0.207	3	0.114	0.952
Cybersecurity factor	-0.138	0.159	1	0.756	0.386
Name of model component (predictor)	Partial correlation	Semipartial correlation	Validity	Tolerance after transformation	Tolerance before transformation
Structural (socio-demographic) factor	0.274	0.262	0.254	0.547	0.944
Structural factor	0.140	0.154	0.145	0.157	0.975
Human factor	0.145	0.148	0.139	0.157	0.972
Economic factor	0.105	0.072	0.067	0.056	0.932

Cybersecurity factor	-0.078	-0.141	-0.133	0.083	0.928

Source: *Own creation.*

The analysis of the data shown in Table 3 shows that the most significant factor influencing attitudes towards DTPs is the structural-demographic factor. It accounts for 25.4% of the variance of the independent variable (validity of 0.254). The cybersecurity dimension appears as the least important among the factors listed in Table 3 (validity of -0.133). Cybersecurity had little influence on the respondents' attitudes towards the digital technology platforms compared to the other factors.

Table 4. *Security of use of digital technology platforms depending on usage time.*

Question 8. Has any of the following negative events or cybersecurity threats occurred within your organisation as a direct consequence of the use of digital technology platforms?	Question 2. Please indicate how long your organisation has been using digital technology platforms.			
	less than 3 years		more than 3 years	
	N	%	N	%
hardware failure	30	51.7	35	56.5
network failure, e.g., due to an overload caused by digital technology platforms	19	32.8	24	38.7
leakage of business, employee or business partner data	4	6.9	1	1.6
leakage of customer data	4	6.9	1	1.6
phishing, i.e., posing as a legitimate institution on the web	5	8.6	7	11.3
pharming, i.e., misdirecting users to fraudulent websites and web servers	3	5.2	7	11.3
loss of money	4	6.9	1	1.6
cyber spying	2	3.4	1	1.6
none	13	22.4	15	24.2
Intergroup comparison with Mann-Whitney U test	hardware failure v. usage time – ni. network failure v. usage time – ni. business data leakage v. usage time – ni. customer data leakage v. usage time – ni. phishing v. usage time – ni. pharming v. usage time – ni. loss of money v. usage time – ni. cyber spying v. usage time – ni. none v. usage time – ni.			
Pearson's chi-squared test for significance of the correlations between variables and Cramer's V contingency coefficient	hardware failure v. usage time – ni. network failure v. usage time – ni. business data leakage v. usage time – ni. customer data leakage v. usage time – ni. phishing v. usage time – ni. pharming v. usage time – ni.			

	loss of money v. usage time – ni. cyber spying v. usage time – ni. none v. usage time – ni.

Source: *Own creation.*

In the next step, the research was supplemented with cross (two-variable) tables and intergroup comparisons which made it possible to present data concerning potential correlations between the variables. In this context, the cybersecurity factor was analysed about the usage time of DTPs (Question 2 of the survey questionnaire). The results are shown in Table 4.

Table 5. *Security of use of digital technology platforms depending on business size.*

Question 8. Has any of the following negative events or cybersecurity threats occurred within your organisation as a direct consequence of the use of digital technology platforms?	Enterprises by business size							
	micro		small		medium		large	
	N	%	N	%	N	%	N	%
hardware failure	3	25.0	11	39.3	23	56.1	28	71.8
network failure, e.g., due to an overload caused by digital technology platforms	4	33.3	9	32.1	20	48.8	10	25.6
leakage of business, employee or business partner data	0	0.0	2	7.1	1	2.4	2	5.1
leakage of customer data	0	0.0	0	0.0	4	9.8	1	2.6
phishing, i.e., posing as a legitimate institution on the web	3	25.0	1	3.6	3	7.3	5	12.8
pharming, i.e., misdirecting users to fraudulent websites and web servers	2	16.7	2	7.1	3	7.3	3	7.7
loss of money	0	0.0	2	7.1	1	2.4	2	5.1
cyber spying	0	0.0	1	3.6	1	2.4	1	2.6
none	7	58.3	9	32.1	6	14.6	6	15.4
Intergroup comparison with Kruskal–Wallis H test and Mann-Whitney U test	hardware failure v. business size - H (χ^2 (3, N=120) = 11.46; $p \leq 0.05$ micro v. small – ni. micro v. medium – U(N=54)=178.5; $p \leq 0.05$ micro v. large – U(N=52)=130.0; $p \leq 0.05$ small v. medium – ni. small v. large – U(N=67) =368.5; $p \leq 0.05$ medium v. large – ni. network failure v. business size – ni. business data leakage v. business size – ni. customer data leakage v. business size – ni. phishing v. business size – ni. pharming v. business size – ni. loss of money v. business size – ni. cyber spying v. business size – ni. none v. business size – ni.							
Pearson's chi-squared test for significance of the correlations between variables and Cramer's V contingency coefficient	hardware failure v. business size - χ^2 (3, N=121) =12.46; $p \leq 0.05$, V=321 network failure v. business size – ni. business data leakage v. business size – ni.							

	customer data leakage v. business size – ni. phishing v. business size – ni. pharming v. business size – ni. loss of money v. business size – ni. cyber spying v. business size – ni. none v. business size – ni.

Source: *Own creation.*

The two groups, i.e., businesses that had been using DTPs for less than three years and those that had been doing so for more than three years, were not significantly different from each other in terms of the reported number of adverse events and threats arising from the use of digital technology platforms. Whether the businesses had been using the platforms for less or more than three years, the most frequently reported issue was hardware failure (reported by more than half of the respondents) and network failure due to an overload caused by the platforms. It is worth mentioning that one in five businesses (in each group) did not report any adverse events.

The data concerning cybersecurity threats were subject to analysis with controlling for the size of the business. The results are shown in Table 5.

The frequency distribution of particular threats and adverse events associated with the use of digital technology platforms is similar for all business sizes (measured based on the number of employees). The only statistically significant difference observed between the businesses concerned the frequency of occurrence of hardware failures. Events of this sort were more common in medium and large enterprises. In both groups, more than 50% of the respondents (56.1% of medium enterprises and 71.8% of large enterprises). A correlation was found between the occurrence of failures and business size. As the number of employees increased, so did the number of occurrences of network failure.

To sum up the author's research study results, it should be stressed that in the analysed sample (where 23.1% were e-commerce businesses), the cybersecurity factor had no significant impact on the attitudes towards DTPs. It was found to be the least significant among the other factors, including the structural factor and the economic factor. Nonetheless, besides the concerns related to organizational structure and employment changes, it was the main reason behind the negative attitudes towards digital technology platforms among the management staff.

Given that slightly over 36% of the analysed businesses experienced a hardware failure and nearly 24% had to deal with a network failure due to the use of DTPs, those concerns are not unreasonable. It leads to the conclusion that even though digital technology platforms are a necessary component of a modern business, especially an e-commerce business, and significant determinants of competitiveness, there are reasonable concerns about their use from the point of view of cybersecurity. It is important to note that these concerns are not limited to cyberattacks, and they extend to failures of hardware and the Internet. From the author's research, it emerges that cybersecurity, widely associated with cyberattacks, covers a much more comprehensive range of issues that can harm the operation of electronic commerce businesses.

Given the above, individual businesses need to implement effective systems and tools to eliminate threats such as the failures mentioned above and for the platforms themselves to guarantee users an adequate level of security. In this context, some advocate applying specific standards (ISO, PAS) and implementing systems and solutions that protect from malware or ensure continuous security monitoring of the digital environment. In digital technology platforms, the security could be effectively improved by launching the so-called bug bounty programs, which offer platform users who report security vulnerabilities various rewards (depending on the type of reported vulnerability). Bug bounty programs have been implemented within the platforms of organizations such as Google or Amazon (Malladi and Subramanian, 2020) Acknowledgements, avoiding identifying any of the authors prior to peer review.

References:

Ablon, L. 2018. The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. Santa Monica (CA), Rand Corporation.

Abte, V. 2018. Digital Economy and Development of E-Commerce. International Journal of Trend in Scientific Research and Development, 10, 234-237.

Al-Ani, M. 2009. Next Generation Digital Commerce Technologies. International Journal of Interactive Mobile Technologies, 2, 58-62.

Amoroso, E. 2006. Cyber Security. Summit (NJ), Silicon Press.

Barometr cyberbezpieczeństwa. 2018. Cyberatak zjawiskiem powszechnym. Warszawa Poland, KPMG.

Botti, A., Maione, G. 2018. E-Commerce Platforms as Service Ecosystems. Open Journal of Economics and Commerce, 2, 8-19.

Brynjolfsson, E, Kahin, B. 2002. Understanding the Digital Economy. Cambridge (MA), Massachusetts Institute of Technology.

Bukht, R., Heeks, R. 2017. Defining, Conceptualising and Measuring the Digital Economy. Manchester (UK), University of Manchester.

Ciriello, R.F., Richter, A. 2018. Schwabe G. Digital Innovation. Business and Information Systems Engineering, 6, 563-569.

Constantinides, P., Henfridsson, O., Parker, G. 2018. Platforms and Infrastructures in the Digital Age. Information Systems Research, 2, 1-20.

Craigen, D., Diakun-Thibault, N., Purse, R. 2014. Defining Cybersecurity. Technology Innovation Management Review, 12, 13-21.

Curzi, V., Lecoq, W., Noémier, Q. 2019. The Impact of social media on E-Commerce Decision Making Process. International Journal of Technology for Business, 1, 1-9.

Digital Economy Report 2019. 2019. Value Creation and Capture: Implications for Developing Countries. United Nations Conference on Trade and Development: New York.

Ferreira, T., Pedrosa, I., Bernardino, J. 2018. Evaluating Open-Source E-commerce Tools using OSSpal Methodology. In: Hammoudi, S., Smialek, M., Camp, O., Filipe, J., eds. Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS) 2018; 2018 Mar 21-24; Funchal Portugal, SciTePress, 213-220.

Gawer, A. 2014. Bridging differing perspectives on technological platforms: Toward an integrative framework. Research Policy, 7, 1239-1249.

Gerring, J. 2001. Social Science Methodology: A Criterial Framework. New York, Cambridge University Press.

Gliń, W., Stasiak-Betlejewska, R. 2020. Threats in Cyber Safety – outline of the Problem. In: Proceedings of the 8th International Conference System Safety: Human - Technical Facility - Environment CzOTO 2019; Zakopane, Warsaw, Poland. De Gruyter Poland, 349-356.

Hopper, A., McCanny, J., Anderson, R., Bond, P., Borrett, M., Creese, S., Murdoch, S., Sasse, A., Someren van, A., Vishik, C. 2016. Progress and research in cybersecurity. Supporting a resilient and trustworthy system for the UK. London (UK), The Royal Society.

Hristoski, I., Kostoska, O., Kotevski, Z., Dimovski, T. 2017. Factors Affecting the Competitiveness of E-Commerce Firms: A Critical Appraisal. In: Dimitrov. D.K., Nikoloski, D., Yilmaz, R., eds. Proceedings of 3rd International Balkan and Near Eastern Social Sciences Congress Series (IBANESS) 2017; 2017 Mar 4-5; Edirne Turkey, University of Agribusiness and Rural Development - University „St. Kliment Ohridski" - Bitola, 1079-1090.

Huo, Y., Chen, H., Yang, S. 2016. Research on the Business Model of E-commerce Platform based on Value Co-creation Theory. International Journal of u and e-Service. Science and Technology, 3, 415-424.

Jansen, M., Lan, J., Carbone, I., Soprana, M., Singhal, A., Zhao, Q. 2016. Bringing SMEs onto the E-commerce Highway. Geneva Switzerland, International Trade Centre.

Khan, S.W. 2019. Cyber Security Issues and Challenges in E-Commerce. In. Pratap, R., Kaurav, S., eds. Proceedings of 10th International Conference on Digital Strategies for Organizational Success 2019; Gwalior India, Prestige Institute of Management, 1197-1204.

Kremer, S., Ludovic, M., Rémy, M., Roca, V. (Ed). 2019. Cybersecurity. Current challenges and India's research directions. Rocquencourt France, The National Institute for Research in Computer Science and Automation.

LeHong, H., Howard, C., Gaughan, D., Logan, D. 2016. Building a Digital Business Technology Platform. Stamford (CT), Gartner.

Malladi, S.S., Subramanian, H.C. 2020. Bug Bounty Programs for Cyber Security. Practices, Issues and Recommendations. IEEE Software, 1, 31-39.

Marchany, R.C., Tront, J.G. 2002. E-Commerce Security Issues. In. Sprague, R.H., ed. Proceedings of the 35th Annual Hawaii International Conference on System Sciences 2002; 2002 Jan 10; Big Island (HI). Los Alamitos (CA): The Institute of Electrical and Electronics Engineers, 35-45.

Merton, K. 2020. The World's Top Online Marketplaces. London (UK), WebRetailer; Retrieved from: https://www.webretailer.com/b/online-marketplaces/.

Özkan, B.E., Bulkan, S. 2019. Hidden Risks to Cyberspace Security from Obsolete COTS Software. In: Mirnik, T., Alatalu, S., Biondi, S., Signoretti, M., Tolga, I., Visky, G., eds. Proceedings of the 11th International Conference on Cyber Conflict: Silent Battle 2019; Tallinn Estonia, NATO OCD COE Publications, 61-80.

Patel, P., Lakhtaria, K.I. 2017. A Study on E-Commerce Security Threats. International Journal of Innovative Research in Computer and Communication Engineering, 3, 5545-5549.

Patton, A., Bandla, K., Brady, M., Bryan, K., Catalan, B., Dunn, C., George, R., Gordon, R., Kolling, C., Misra, D. 2019. Cyber Threat scape Report. Dublin (Ireland), Accenture.
Parn, E.A., Edwards, D. 2019. Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. Engineering, Construction and Architectural Management, 26, 245-266.
Rahman, S.M., Lackey, R. 2013. E-commerce Systems Security for Small Business. International Journal of Network & Its Applications, 2, 193-210.
Reuver de, M., Sørensen, C., Basole, R.C. 2015. The digital platforms: a research agenda. Journal of Information Technology, 4, 124-135.
Rohilla, N. 2017. Content Management System for E-commerce Website Development. International Journal of Engineering Sciences & Research, 6, 490-495.
Seemma, P.S., Nandhini, S., Sowmiya, M. 2018. Overview of Cyber Security. International Journal of Advanced Research in Computer and Communication Engineering, 11, 125-128.
Spremić, M., Simunić, A. 2018. Cyber Security Challenges in Digital Economy. Proceedings of The World Congress of Engineering, 1, 341-346.
Sun, R., Keating, B., Gregor, S. 2015. Information Technology Platforms: Definition and Research Directions. In: Burstein, F., Scheepers, H., Deegan, G., eds. Proceedings of the 26th Australasian Conference on Information Systems (ACIS) 2015; Auckland (New Zealand). Adelaide (Australia): Australasian Association for Information Systems, 1-17.
Unpacking E-commerce. Business Models. 2019. Trends and Policies. Paris France, Organisation for Economic Cooperation and Development.