Bartczak, Krzysztof

**Article**

# The use of digital technology platforms in the context of cybersecurity in the industrial sector

Foundations of Management

**Provided in Cooperation with:**
Faculty of Management, Warsaw University of Technology

*Suggested Citation:* Bartczak, Krzysztof (2021) : The use of digital technology platforms in the context of cybersecurity in the industrial sector, Foundations of Management, ISSN 2300-5661, De Gruyter, Warsaw, Vol. 13, Iss. 1, pp. 117-130, https://doi.org/10.2478/fman-2021-0009

This Version is available at:
https://hdl.handle.net/10419/237028

# THE USE OF DIGITAL TECHNOLOGY PLATFORMS IN THE CONTEXT OF CYBERSECURITY IN THE INDUSTRIAL SECTOR

Krzysztof BARTCZAK

Warsaw University of Technology, Faculty of Management, Warsaw, POLAND
e-mail: krzysztof.bartczak@pw.edu.pl

***Abstract:*** This study discusses the use of digital technology platforms (DTPs) in the context of cybersecurity in the industrial sector, with a focus on digital industry (industrial) platforms (DIPs). A definition of DTPs is presented, including the author's interpretation, as well as the scope of DTP application in the industrial sector, which includes, in particular, European Digital Platforms (EDPs) and Polish Digital Platforms (PDPs), such as non-ferrous metals PDP or intelligent transport systems PDP. This is followed by a section covering the theoretical basis of the study that highlights the key challenges and risks associated with the use of DTPs as well as the methods for their neutralization in the form of specific concepts and systems that can be employed in the industrial sector. The subsequent section of the study is based on results of the author's own survey which collected information from a total of 120 companies operating in Poland, which were granted subsidies under the Operational Program Innovative Economy for investments involving the implementation and development of DTPs. The survey was carried out using a questionnaire developed by the author, which consisted of 23 questions. In this respect, as shown by the author's own studies, of greatest relevance are hardware failures and Internet outage events. Most importantly, concerns about such risks are some of the major factors underlying the negative attitudes of management staff of industrial companies toward DTPs, and therefore, it is so important to ensure that any such risks can be effectively addressed. They can be avoided through the use of certain concepts and systems such as STOE or CVSS. A typical company may know the model of DTPs in the context of challenges in the field of cybersecurity through this study; in particular, it can improve IT security.

***Keywords****:* platform economy, digital technology platforms, cybersecurity, risks, industrial sector.

***JEL Classification:*** M11, M15, D20.

## 1 Introduction

The modern economy is characterized by a widespread use of knowledge and a strong reliance on advanced technologies (Hretcanu, 2015). Knowledge is a corporate resource, being the ground for initiating activities, primarily innovative ones (Śliwa and Patalas-Maliszewska, 2016). This is clear, inter alia, from the use of digital technology platforms (DTPs) which – most importantly – are present in the lives of most people while exerting a powerful influence on education, professional, and social domains. Currently, it is fair to speak of platform economy (Busch, et al., 2016; Neittaanmäki, Galeieva, and Ogbechie, 2016). Platforms are used in a number of industries and economic sectors, including the industrial sector (Kenney, et al., 2019). What is of relevance here is that their use is associated to a significant degree with cybersecurity issues because they are based on the Internet and advanced technologies (Kaplan, Richter, and Ware, 2019). This study analyzes the use of DTPs in the industrial sector in the context of cybersecurity (Diego, et al., 2021).

## 2 Core features of DTPs and their use in the industrial sector

DTPs are widely used by companies, public institutions or private users, and the scope of their potential applications seems to be without limits. In the context of the industrial sector, there are digital industry (industrial) platforms (Sun, Keating, Gregor, 2015), technology platforms (Stig, 2015), and digital manufacturing platforms (Gerrikagoitia, et al., 2019). The existing definitions of DTPs or, taken more broadly, digital platforms indicate that they are a

class of instruments associated with specific content and services that allow establishing and strengthening relations between various entities such as companies and consumers. Platforms are, therefore, used for carrying out a variety of transactions, including business transactions, or for the purpose of communication via the Internet, which helps to connect business partners (Constantinides, Henfridsson and Parker, 2018; Sun, Keating and Gregor, 2015). Another approach points to the fact that DTPs correspond to modern business models which need various types of technologies to function, including IT technologies, and which generate value in that they provide the basis for establishing interactions between representatives of different professional and social groups. Such interactions can involve manufacturers and consumers, facilitating sales processes, or only companies, promoting collaboration between individual operators with a view to developing and launching innovative products or services (Morgan, Hintermann and Vazirani, 2016).

In the context of the industrial sector, the definition formulated by De Reuver, Sørensen, and Basole (2015) should be taken into account. These authors proposed that DTPs can be analyzed in terms of two – technical and sociotechnical – perspectives. The first perspective highlights the fact that DTPs are databases of codes which make it possible to continuously add new modules and functionalities, thus extending the opportunities for the use of the platforms. Based on this approach, the use of DTPs is associated with openness or interoperability. The sociotechnical perspective gives emphasis to the fact that DTPs comprise technical elements, for example, software and hardware, as well as organizational processes and standards which are closely related to them.

On the other hand, the author's definition of DTPs is as follows: DTPs are considered electronic (digital) tools which can take the form of services or content and be used for creating attitudes oriented toward establishing and strengthening interactions between various business operators, where a highly important feature of such platforms is the possibility of extending them on a continuous basis with the aim of including new modules and functionalities.

As already mentioned, DTPs find use in a number of sectors, including the industrial sector. In the context of the industrial sector, there are platforms that are used for the purposes of collaboration and communication between individual companies while making it possible to virtualize a wide range of processes, including manufacturing processes, or to develop new business models and generate innovations (this is possible because users have access to open machine data prior to their algorithmization). Moreover, of significant importance are platforms that enable conducting mediation and negotiation processes through electronic means, adjusting the range of products and services offered by industrial companies, integrating sellers and buyers of certain products and services (electronic markets and exchanges) or automatic handling and processing of payments (clearing platforms) (Oxera Consulting, 2015). Currently, in Poland also, works are underway into platforms described as "sandboxes," which are aimed to enable creating architecture for subsequent IT systems or providing conditions oriented toward incubators of structural innovations and sources of hard industrial data (Borowik, et al., 2018). These sandboxes can also serve as industry sandboxes. They consist of a number of components, including data collections, reference architecture, consulting spaces, or user assessment mechanisms (Wintermeyer and Markowa, 2017).

One of the flagship examples of how DTPs can be put to use in the industrial sector is the implementation of European Technology Platforms (ETPs) and Polish Technology Platforms (PTPs), which have been in operation since 2003 (in Poland since 2004). They are employed for the purpose of developing innovative research and technology projects based on strategies implemented by a number of partners, such as science and research centers, companies generating innovative solutions, universities, and other higher-education institutions. They are operated in several areas, including steel industry (PTP for non-ferrous metals, casting and steel), energy sector (PTP for biofuels and biocomponents, nuclear technologies, hydrogen and fuel cells, sustainable energy systems and clean carbon energy), transport segment (PTP for intelligent transport systems, space technologies), or advanced materials (PTP for con-

struction industry, manufacturing processes, sustainable chemistry) (Krajowy Punkt Kontaktowy [*National Point of Contact*], 2003; Stouffer, 2004; Sibalija, 2011).

In the industrial sector, the use of DTPs leads to:

- transformations or even operational disruptions and disintegration of traditional industrial areas, where aspects related to innovativeness have a decisive role,
- increased participation of operators originating from the business environment of the industrial sector, which is possible because DTPs bring together users, business associates, and partners and which results in the generation of innovation ecosystems,
- testing possibilities for new business models through platforms,
- greater accessibility of funds to be allocated to financing innovations (e.g. crowd-funding platforms), and
- increased expansion and measures oriented toward diversification among industrial companies (Busch, et al., 2016).

DTPs serve a significant role in the modern economy and in the industrial sector as they help to consolidate collaboration between individual companies and generate innovative solutions.

## 3 Cybersecurity challenges in the context of the use of DTPs in the industrial sector

DTPs promote a variety of benefits for companies or consumers; however, it should also be noted that they can be a source of various types of risks. This is specifically important in the context of Industry 4.0, which relies to a considerable extent on automatic real-time data processing and transmission, an extensive use of the Internet of Things, as well as an integration of IT and operational technologies. This gives rise to some enormous challenges in the area of cybersecurity (Ervural and Ervural, 2017; Deloitte, 2017; Kozłowski, 2017). It is worth pointing out that based on a report available at statista.com, the greatest number of attacks against critical infrastructure in 2017 were observed in the energy sector (26% of all attacks) and a large percentage of such attacks were directed against the manufacturing sector (22%) (Statista, 2017). Such attacks, therefore, affect the industrial sector to a large extent, which demonstrates the considerable scale of relevant cybersecurity challenges.

The essential risks affecting the industrial sector in cyberspace are shown in Fig. 1.

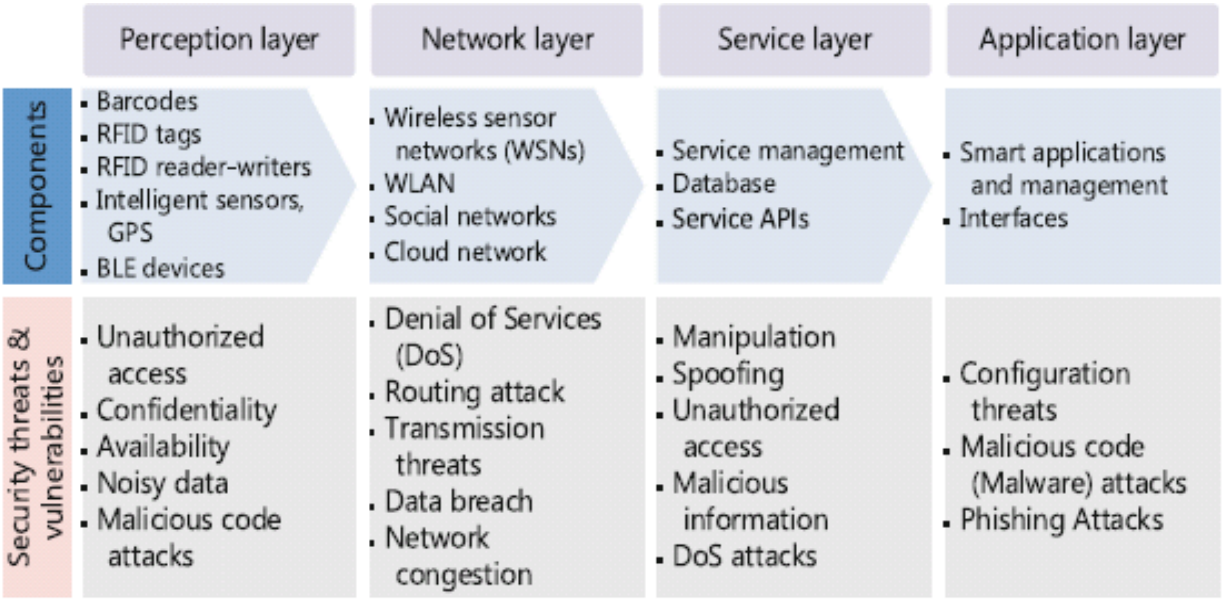


Figure 1. The major risks for the industrial sector in cyberspace; RFID: radio-frequency identification (*Source:* Ervural and Ervural, 2017)

The risks for the operation of the industrial sector in cyberspace can be analyzed in terms of perception, networks, services, and applications. All these layers can be associated with specific threats, including when distinct components of systems, digital platforms, and IT structures are taken into account. As far as the technologies of barcodes and radio-frequency identification (RFID) are concerned, the relevant threats include unauthorized access and malicious code attacks, while in the case of social networks or cloud computing, which are examples of particular DTPs, there is a risk of network congestion or protocol-oriented attacks.

Nowadays, one of the major problems is not only the possibility of hacking attacks against digital platforms and their users, but also the fact that individual platforms are significantly different in terms of architecture, requirements, or implemented security tools, which prevents an effective supervision over the platforms in the event of their integration as part of specific systems. As a result, there is currently a strong need for the creation of platforms which will enable a complex and coherent approach to security-related issues. The relevant requirements are connected with the design of IT solutions and the architecture for individual platforms (PwC, 2016).

In the context of cybersecurity, appropriate rules must be followed when using DTPs in the industrial sector. In this respect, it is proposed that:

- there is an appropriate corporate architecture oriented toward cybersecurity management, covering all types of systems, platforms, digital and IT tools, including, in particular, industrial control systems (ICSs), and
- a system for diagnosing the risks for the industrial sector, including identification of cyberattacks and damaged areas of existing systems, is organized as a fully automated and digitalized system, so that it can be put to use as an online system (Kozak, et al., 2016).

In reference to the first area, it becomes necessary to ensure that as many industrial companies as possible implement concepts that enable effective cybersecurity management through the creation of suitable cybersecurity architecture. A good example is the concept underlying the system target of evaluation (STOE), that is, a system-wide target of an assessment process, which is used as part of ICSs. The STOE was developed by the US National Institute of Standards and Technology (NIST) as part of the System Protection Profile (SPP) (Stouffer, 2004; Leszczyna, 2019). This concept provides for harmonization of actions aimed at ensuring confidentiality and coherence in the collection and use of data by companies operating in the industrial sector as well as maintaining the operating systems and technology platforms in a state of continuous readiness without disrupting any functions of the security system. The STOE can take advantage of various system-wide security functions, such as user authentication and access control features (which enable remote diagnostic inspections or function checks), securing the limits of industrial sites and data authorization, which should also include control signals (Borysiewicz and Michalik, 2007). The essential features associated with the use of the STOE are listed in Table 1.

Table 1. The essential features of the STOE (*Source:* Borysiewicz and Michalik, 2007)

| Feature | Description |
|---|---|
| Audit | Recording – in an audit register – information about users' operations that were unsuccessful |
| Authorization | • Use of configuration modifications that cover control algorithms or border points<br>• Authorization of users who have access to control systems or actuation mechanisms |
| Operational preparedness | Protection against loss of operational readiness of control servers or communication lines |
| Access control | Inspections of system and platform interfaces, their functions, modifiable configurations, and critical processes |

Table 1. The essential features of the STOE, cont. (*Source:* Borysiewicz and Michalik, 2007)

| Feature | Description |
|---|---|
| Monitoring | Detection of unauthorized operations on an ongoing basis |
| Recovery | Existence of tools for critical elements and processes aimed at data recovery at the time of failure |
| Confidentiality | Data protection against unauthorized disclosure (relevant data are determined based on a risk assessment and they mostly include operational, control, and financial information) |
| Security procedures | Existence of plans and policies relating to security management, business continuity, or assignment of roles and responsibilities |
| Self-check | Performance of self-tests used for validation of the integrity of security functions |
| Coherence | Protection against unauthorized changes to the information flow or configuration of systems and platforms |
| Border protection | Protection against attempts aimed at slipping across physical and digital logic borders of a system or platform |

It should be highlighted that all DTPs that are used by companies in the industrial sector should be covered by the STOE. This can help to ensure that platforms are fully secure and do not give rise to any additional risks or threats to a company.

In reference to the second area of DTP use in the industrial sector in the context of cybersecurity, that is, diagnosing, one cannot leave unnoticed the common vulnerability scoring system (CVSS) which was developed by the National Infrastructure Assurance Council (NIAC). The primary purpose of the CVSS is to ensure cybersecurity with respect to information technology, which is achieved based on analyses of susceptibility of systems and IT platforms to threats and risks. This concept uses metrics which are used for calculating susceptibility to threats, which in turn enables implementing relevant remedies at specific points of systems as well as IT and digital platforms. It should be highlighted that both the STOE and the CVSS are improved on a continuous basis while taking into account contextual information that are unique to each organization, business environment, and user. This is of particular importance in the context of the use of increasingly extensive and innovative DTPs by companies (Mell, Scarfone and Romanosky, 2007; Michalik and Borysewicz, 2009; Scarfone and Mell, 2009).

In the case of DTPs, the security could be effectively improved by launching the so-called bug bounty programs which offer various rewards to the platform users who report security vulnerabilities (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).

## 4 Cybersecurity in the context of the use of DTPs in the industrial sector: own study results

The use of DTPs in the industrial sector in the context of cybersecurity was analyzed based on the author's own surveys. They covered a broad range of aspects related to the impact of DTPs on the generation of new business models, including cybersecurity issues. The surveys were conducted from 18 through 28 February 2019 based on computer-assisted telephone interviews (CATIs). This method is characterized by a high level of standardization and forms part of a quantitative paradigm (Gerring, 2001). The survey questionnaire, which consisted of 23 questions, was submitted to representatives of 120 companies which received funding under the Operational Program Innovative Economy for the implementation and development of DTPs. It should be emphasized that 25 out of all the companies whose representatives participated in the survey (20.7%) originated from the industrial sector.

The sample was random. The final sample consisted of N = 320 records, of which it was assumed that

effective interviews would be carried out with the number of entities N = 120. The randomization algorithm built into the phone testing software gave every record in the database an equal chance of being in the sample.

In the course of the study, telephone contact was established with each of the companies. One hundred and twenty interviews were conducted, 49 enterprises refused to participate in the study, 2 enterprises declared that they did not implement any platforms, and the interviews were not completed with the assumed dates of the survey.

One of the questions asked about manifestations of the negative approach of management staff of the surveyed companies toward the implementation and use of DTPs. The survey results are shown in Table 2 according to responses given by the survey participants.

Table 2. Manifestations of the negative approach of management staff of the surveyed companies toward the implementation and use of digital technology platforms (*Source:* Own study)

| Question 7. Please specify how the negative attitude of management staff toward the implementation and use of digital technology platforms manifests itself in your company | | | | |
|---|---|---|---|---|
| | | Responses | | Percentage of observations |
| | | n | Percentage | |
| | High-level resistance toward the implementation of digital technology platforms due to potential changes to the organizational and employment structure in the company | 2 | 40.0 | 100.0 |
| | A number of concerns attributable to economic factors (high costs of implementation and possible cost reductions in other operational areas of the company) | 1 | 20.0 | 50.0 |
| | Numerous cybersecurity concerns | 2 | 40.0 | 100.0 |
| Total | | 5 | 100.0 | 250.0 |

A total of 40.00% of the survey participants stated that the resistance of management staff of the surveyed companies toward the use of DTPs is provoked by cybersecurity concerns. It should be noted that such concerns, besides organizational or employment-related problems, were indicated as the most significant manifestations of the negative attitude of management staff toward DTPs. This shows that cybersecurity and potential risks affecting cybersecurity are some of the major obstacles on the way toward a wide and unlimited use of DTPs by companies.

As part of CATIs, the survey participants were also asked about cybersecurity-related consequences suffered by their companies due to the use of DTPs. Results are presented in Table 3.

Only 28 persons, that is, 15.6% of the survey respondents, stated that their companies experienced no negative events which would be associated with the implementation and use of DTPs. Such events were indicated by 92 respondents, that is, 84.4% of all the survey participants. The greatest percentage of the survey participants referred to hardware failure (n = 65, 36.1%) and Internet outage events, which could be attributable to network congestion due to the use of DTPs (n = 43, 23.9%). Data leaks, phishing, and pharming were significantly less frequently indicated by the survey respondents.

Therefore, it should be concluded that the use of DTPs generates numerous cybersecurity risks and threats affecting the surveyed companies, which mostly include hardware failures and Internet outage events. It can be easily imagined that such failures and outage events can even cause downtime in industrial companies, and accordingly, it is so important to ensure effective preventive remedies.

Table 3. Cybersecurity-related consequences of the use of DTPs in companies
(*Source:* Own study)

| Question 8. Please specify if your company experienced any of the below-specified negative events or cybersecurity risks which were directly associated with the use of DTPs | | | | |
|---|---|---|---|---|
| | | Responses | | Percentage of observations |
| | | n | Percentage | |
| | Hardware failure | 65 | 36.1 | 53.7 |
| | Internet outage attributable to, for example, network congestion due to the use of digital technology platforms | 43 | 23.9 | 35.5 |
| | Leak of information relating to company, employees, or business partners | 6 | 3.3 | 5.0 |
| | Customer data leak | 6 | 3.3 | 5.0 |
| | Phishing – a fraudulent attempt to obtain sensitive information or data by disguising a website as a trustworthy entity in an electronic communication | 12 | 6.7 | 9.9 |
| | Pharming – redirection to fake websites | 10 | 5.6 | 8.3 |
| | Loss of financial means | 6 | 3.3 | 5.0 |
| | Internet spying | 3 | 1.7 | 2.5 |
| | No negative events | 28 | 15.6 | 23.1 |
| | Total | 180 | 100.0 | 148.8 |

The added value that stands out from other works in addition to CATIs, the author's own studies also used a categorical regression (CATREG) which allows a quantitative assessment of qualitative data and optimum scaling (to predicting values of specific variable based on the values of other variables), which resulted in the creation of a DTP model. The model measures attitudes toward DTPs in companies while assuming that one of the domains in which a company is transformable as a result of the use of DTPs is the cybersecurity domain that involves new IT challenges associated with hardware and software. This aspect was referred to in Question 8 of the survey questionnaire: *Please specify if your company experienced any of the below-specified negative events or cybersecurity threats which were directly associated with the use of DTPs.* In reference to the domain referred to above, the scale of measurement of the variable was nominal (multi-response question) and it was transformed into a ratio variable (calculation of the number of responses).

Depending on the type and number of variables in the model, different result values are obtained, and this method does not decide which of the built models is optimal – the choice is made by the researcher based on the structure of the results obtained. A limitation is also a congenital defect of all regression methods, that is, one can find out about the existence or absence of relationships between variables, but it does not provide knowledge about the causal relationship of the studied relationships.

The model development process consisted of several stages as part of a descending method that was involved, which are given as follows:

1) inclusion in the model of those variables (including cybersecurity) which in the researcher's opinion are relevant in terms of the independent variable (attitude toward DTPs),
2) changes in the sequence of variables with the aim of achieving the maximum possible result,
3) development and evaluation of the model,
4) reduction in the number of variables by removing the weakest predictor,
5) development of a reduced model,

6) comparison of the previous and the resulting (reduced) model, and
7) iteration of steps 4–6 until the most numerically satisfactory results are obtained.

Based on the developed model, it was possible to determine which factors are most relevant to attitudes toward DTPs. In this respect, in connection with the cybersecurity domain, the following numerical results were taken into consideration:

- Beta coefficient (β)

A so-called standardized regression coefficient (independent of the range of a variable and calculated based on the slope that is also referred to as a gradient of a line). Beta coefficient enables comparing individual predictors in a regression model and ranges from –1 to +1, which means that values oscillating near zero correspond to a weak or zero relationship between a predictor and a dependent variable.

- Significance

This parameter is used for characterizing individual predictors.

- F-statistic

It describes the overall goodness-of-fit that shows the level of variance to be explained; when developing a model, variables with the lowest F-statistic values are sequentially eliminated.

- Correlation matrix

Zero-order correlations as well as partial and semipartial correlations. Zero-order correlations are isolated correlations between an independent and a dependent variable; partial correlations account for the correlations between a given predictor as well as a dependent variable and the other variables in a model; and semipartial correlations account for the interactions between a given independent variable and the other variables in a model. However, they do not allow for correlations between a dependent variable and other predictors; the correlation values range from –1 to +1.

- Validity

The significance of individual variables in a model, given as a unit fraction (the maximum value is 1); the higher the validity assigned to a given predictor, the more crucial the role of the predictor in a model. The value of this parameter can be given as a percentage.

- Tolerance2

It measures the collinearity of variables; this is the inverse of R-squared (tolerance = $1 - R^2$). Tolerance ranges from 0 to 1, and the closer the tolerance of a predictor is to one, the lower the collinearity of the predictor with the other variables in a model. Collinearity should be avoided – the closer this coefficient is to zero, the greater the redundancy of a given variable and the more useless information it conveys, given that variables included in a model should be strongly correlated with a dependent variable while being weakly correlated with each other. Of relevance to the structure of a model is the phase of data validation, when the question of outlying observations should be addressed. CATREG models are highly sensitive to outliers (Mider, 2017).

Table 4 shows the numerical results for all the analyzed domains, including – in addition to cybersecurity – structural, structural demographic, human, and economic factors.

Table 4. Factors relevant to attitudes toward digital technology platforms (*Source:* Own study)

| Model component (predictor) | Beta coefficient | Number of degrees of freedom (df) | F | Significance | Zero-order correlation |
|---|---|---|---|---|---|
| Structural (sociodemographic) 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 |

Table 4. Factors relevant to attitudes toward digital technology platforms, cont. (*Source:* Own study)

| Model component (predictor) | Partial correlation | Semipartial correlation | Validity | Post-transformation tolerance | Pre-transformation tolerance |
|---|---|---|---|---|---|
| Structural (sociodemographic) 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 |

When analyzing data presented in Table 4, it should be noted that the most important factor having relevance to attitudes toward DTPs is the structural demographic factor. It explains as much as 25.4% of variability of an independent variable (validity at 0.254). Among the factors taken into account in Table 4, the cybersecurity domain is of least importance (validity at –0.133). This means that attitudes of staff members of the surveyed companies toward DTPs are conditioned by cybersecurity to a relatively insignificant extent.

As part of the surveys, the resulting model was extended to include cross-correlation (two-variable) tables and intergroup comparisons, which made it possible to present any identified correlations between variables. In this respect, the analysis also included the cybersecurity factor when taking into account the duration of use of DTPs (Question 2 of the survey questionnaire). The relevant study results are shown in Table 5.

Table 5. The security domain during the use of digital technology platforms vs the duration of their use (*Source:* Own study)

| Question 8. Has your company experienced any of the below-specified negative events or cybersecurity risks which were directly associated with the use of DTPs? | Question 2. Please specify how long your current company has been using digital technology platforms | | | |
|---|---|---|---|---|
| | Up to 3 years | | More than 3 years | |
| | n | % | n | % |
| Hardware failure | 30 | 51.7 | 35 | 56.5 |
| Internet outage attributable to, for example, network congestion due to the use of digital technology platforms | 19 | 32.8 | 24 | 38.7 |
| Leak of information relating to company, employees, or business partners | 4 | 6.9 | 1 | 1.6 |
| Customer data leak | 4 | 6.9 | 1 | 1.6 |
| Phishing – a fraudulent attempt to obtain sensitive information or data by disguising a website as a trustworthy entity in an electronic communication | 5 | 8.6 | 7 | 11.3 |
| Pharming – redirection to fake websites | 3 | 5.2 | 7 | 11.3 |
| Loss of financial means | 4 | 6.9 | 1 | 1.6 |
| Internet spying | 2 | 3.4 | 1 | 1.6 |
| No negative events | 13 | 22.4 | 15 | 24.2 |

Table 5. The security domain during the use of digital technology platforms vs the duration of their use, cont. (*Source:* Own study)

| Question 8. Has your company experienced any of the below-specified negative events or cyber-security risks which were directly associated with the use of DTPs? | Question 2. Please specify how long your current company has been using digital technology platforms |
|---|---|
| Intergroup comparisons using the Mann-Whitney U-test | • Hardware failure vs duration of use – not statistically significant<br>• Internet outage vs duration of use – not statistically significant<br>• Company data leak vs duration of use – not statistically significant<br>• Customer data leak vs duration of use – not statistically significant<br>• Phishing vs duration of use – not statistically significant<br>• Pharming vs duration of use – not statistically significant<br>• Loss of financial means vs duration of use – not statistically significant<br>• Internet spying vs duration of use – not statistically significant<br>• No negative events vs duration of use – not statistically significant |
| Test for significance of relationships between Pearson's chi-square and Cramer's V contingency coefficient | • Hardware failure vs duration of use – not statistically significant<br>• Internet outage vs duration of use – not statistically significant<br>• Company data leak vs duration of use – not statistically significant<br>• Customer data leak vs duration of use – not statistically significant<br>• Phishing vs duration of use – not statistically significant<br>• Pharming vs duration of use – not statistically significant<br>• Loss of financial means vs duration of use – not statistically significant<br>• Internet spying vs duration of use – not statistically significant<br>• No negative events vs duration of use – not statistically significant |

Both the surveyed groups, that is, companies which have used DTPs for less than or more than 3 years, are not statistically significant in terms of the incidence of negative events and threats secondary to the use of DTPs. Both the companies which have been using DTPs for up to 3 years and those with a longer use of DTPs experience such events mostly in the form of hardware failures (more than half of the surveyed companies) and Internet outage events due to network congestion attributable to the use of DTPs. It should be highlighted that one in five companies (in both groups) experienced no negative events.

An analysis should also be carried out for data on cyber threats as a function of company size. The data are presented in Table 6.

Table 6. Security domain during the use of digital technology platforms vs company size (*Source:* Own study)

| Question 8. Has your company experienced any of the below-specified negative events or cybersecurity risks which were directly associated with the use of DTPs? | Company size | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Micro-sized companies | | Small-sized companies | | Medium-sized companies | | Large-sized companies | |
| | n | % | n | % | n | % | n | % |
| Hardware failure | 3 | 25.0 | 11 | 39.3 | 23 | 56.1 | 28 | 71.8 |
| Internet outage attributable to, for example, network congestion due to the use of digital technology platforms | 4 | 33.3 | 9 | 32.1 | 20 | 48.8 | 10 | 25.6 |
| Leak of information relating to company, employees, or business partners | 0 | 0.0 | 2 | 7.1 | 1 | 2.4 | 2 | 5.1 |
| Customer data leak | 0 | 0.0 | 0 | 0.0 | 4 | 9.8 | 1 | 2.6 |
| Phishing – a fraudulent attempt to obtain sensitive information or data by disguising a website as a trustworthy entity in an electronic communication | 3 | 25.0 | 1 | 3.6 | 3 | 7.3 | 5 | 12.8 |
| Pharming – redirection to fake websites | 2 | 16.7 | 2 | 7.1 | 3 | 7.3 | 3 | 7.7 |
| Loss of financial means | 0 | 0.0 | 2 | 7.1 | 1 | 2.4 | 2 | 5.1 |
| Internet spying | 0 | 0.0 | 1 | 3.6 | 1 | 2.4 | 1 | 2.6 |
| No negative events | 7 | 58.3 | 9 | 32.1 | 6 | 14.6 | 6 | 15.4 |
| Intergroup comparisons using the Kruskal–Wallis H-test and Mann-Whitney U-test | • Hardware failure vs company size $H(\chi^2)(3, n = 120) = 11.46, p \leq 0.05$<br>• Micro-sized vs small-sized companies – not statistically significant<br>• Micro-sized vs medium-sized companies $U(n = 54) = 178.5, p \leq 0.05$<br>• Micro-sized vs large-sized companies $U(n = 52) = 130.0, p \leq 0.05$<br>• Small-sized vs medium-sized companies – not statistically significant<br>• Small-sized vs large-sized companies $U(n = 67) = 368.5, p \leq 0.05$<br>• Medium-sized vs large-sized companies – not statistically significant<br>• Internet outage vs company size – not statistically significant<br>• Company data leak vs company size – not statistically significant<br>• Customer data leak vs company size – not statistically significant<br>• Phishing vs company size – not statistically significant<br>• Pharming vs company size – not statistically significant<br>• Loss of financial means vs company size – not statistically significant<br>• Internet spying vs company size – not statistically significant<br>• No negative events vs company size – not statistically significant | | | | | | | |

Table 6. Security domain during the use of digital technology platforms vs company size, cont.
(*Source:* Own study)

| | |
|---|---|
| Test for significance of relationships between Pearson's chi-square and Cramer's V contingency coefficient | • Hardware failure vs company size<br>H ($\chi^2$) (3, n = 121) = 12.46, p ≤ 0.05, V = 321<br>• Internet outage vs company size – not statistically significant<br>• Company data leak vs company size – not statistically significant<br>• Customer data leak vs company size – not statistically significant<br>• Phishing vs company size – not statistically significant<br>• Pharming vs company size – not statistically significant<br>• Loss of financial means vs company size – not statistically significant<br>• Internet spying vs company size – not statistically significant<br>• No negative events vs company size – not statistically significant |

The frequency distributions for individual risks and negative events associated with the use of DTPs are similar for all surveyed companies (taking into account their size defined as the number of employees). The only significant difference between the surveyed companies is related to the incidence of hardware failures, which are more common in medium- and large-sized companies.

In both groups, hardware failures were declared by more than 50% (56.1% in medium-sized and 71.8% in large-sized companies) of the survey participants. There is also a correlation between the incidence of hardware failures and company size because the incidence of hardware failures increases with greater level of employment.

To summarize the results of the author's own studies, it should be noted that among the surveyed companies, of which about 20% were operators originating from the industrial sector, the cybersecurity factor had no substantial impact on attitudes toward DTPs. This is because cybersecurity is of least importance as compared to other – structural or economic – factors.

Besides concerns about changes to organizational and employment structure, it is of greatest relevance to attitudes of management staff toward DTPs. Such concerns are undoubtedly, at least partially, justified because slightly more than 36.0% of the surveyed companies suffered hardware failures and nearly 24.0% suffered Internet outage events due to the use of DTPs. It can, accordingly, be concluded that DTPs are indispensable elements of business operations pursued by modern companies, including operators in the industrial sector, as well as importance competitiveness factors; however, their use gives rise to reasonable cybersecurity concerns. Importantly, not only the threat of hacking attacks, but also the risk of hardware failures or Internet outage events causes concern.

It is, therefore, required to recommend that all industrial companies using DTPs ensure appropriate conditions for their implementation and use. This includes the need to use systems and concepts described earlier in this study, that is, the STOE or CVSS.

## 5 Conclusions

To summarize the study results, it should be pointed out that DTPs are widely used in the industrial sector which brings both new opportunities as well as challenges in the form of cybersecurity risks. In this respect, as shown by the author's own studies, of greatest relevance are hardware failures and Internet outage events.

Most importantly, concerns about such risks are some of the major factors underlying the negative attitudes of management staff of industrial companies toward DTPs, and therefore, it is so important to ensure that any such risks can be effectively addressed. This is possible through the implementation of appropriate risk management policies and the use of relevant systems such as STOE or CVSS.

## 6 References


[1] Borowik, M., Maśniak, L., Kroplewski, R., Romaniec, H., 2018. *Przemysł +. Gospodarka oparta o dane* (*Industry +. Data-driven Economy*). Warszawa (Poland): Ministerstwo Cyfryzacji.

[2] Borysiewicz, M.J., Michalik, J.S., 2007. *Cyberbezpieczeństwo przemysłowych systemów sterowania. Bezpieczeństwo Pracy* (*Cybersecurity of Industrial Control Systems. Work Safety)*, 10, pp.8-11.

[3] Busch, C., Dannemann, G., Schulte-Nölke, H., Wiewiórkowska-Domagalska, A., Zoll, F., 2016. Research Group on the Law of Digital Services, Discussion Draft of a Directive on Online Intermediary Platforms. *Journal of European Consumer and Market Law*, 5, pp.164-169.

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

[5] Corin Stig, D., 2015. *Technology Platforms. Organizing and Assessing Technological Knowledge to Support its Reuse in New Applications*. Gothenburg (Sweden): Department of Product and Production Development Chalmers University of Technology.

[6] Deloitte, 2017. *Industry 4.0 and Cybersecurity. Managing Risk in Age of Connected Production*. London (UK): Deloitte University Press.

[7] De Marco, C.E., Di Minin, A., Marullo, C., Nepelski, D., 2019. *Digital Platform Innovation in European SMEs. An analysis of SME Instrument Business Proposals and Case Studies*. Luxembourg (Luxembourg): Publications Office of the European Union.

[8] De Reuver, M., Sørensen, C., Basole, R.C., 2015. The Digital Platforms: A Research Agenda. *Journal of Information Technology*, 4, pp.124-135.

[9] Diego G.S. Pivoto, Luiz F.F. de Almeida, Rodrigo da Rosa Righi, Joel J.P.C. Rodrigues, Alexandre Baratella Lugli, Antonio M. Alberti, 2021. Cyber-physical Systems Architectures for Industrial Internet of Things Applications in Industry 4.0: A literature review. *Journal of Manufacturing Systems*, Volume 58, Part A, pp.176-192, ISSN 0278-6125, https://doi.org/10.1016/j.jmsy.2020.11.017.

[10] Ervural, B.C., Ervural, B., 2017. Overview of Cyber Security in the Industry 4.0 Era. In: A. Ustundag, E. Cevikcan (Eds.), *Industry 4.0: Managing The Digital Transformation*, pp.267-284). Cham (Switzerland): Springer.

[11] Frühwirth, C., Männistö, T., 2009. Improving CVSS-based Vulnerability Prioritization and Response with Context Information. In: *2009 3rd International Symposium on Empirical Software Engineering and Measurement*, pp.535-544. Massachusetts (DC): ILEE Computer Society.

[12] Gerrikagoitia, J.K., Unamuno, G., Urkia, E., Serna, A., 2019. Digital Manufacturing Platforms in the Industry 4.0 from Private and Public Perspectives. *Applied Sciences*, 9, pp.2934-2946.

[13] Gerring, J., 2001. *Social Science Methodology: A Criterial Framework*. New York (NY): Cambridge University Press.

[14] Hretcanu, C.I., 2015. Current Trends in the Knowledge Economy. *Ecoforum*, 2, pp.170-175.

[15] Kaplan, J., Richter, W., Ware, D., 2019. *Cybersecurity: Linchpin of the Digital Enterprise. As Companies Digitize Businesses and Automate Operations, Cyberrisks Proliferate; Here Is How*. New York (NY): McKinsey & Company.

[16] Kenney, M., Rouvinen, P., Seppälä, T., Zysman, J., 2019. Platforms and Industrial Change. *Industry and Innovation*, 8, pp.871-879.

[17] Kozak, A., Kościelny, M., Pacyna, P., Gołębiewski, D., Paturej, K., Świątkowska, J., 2016. *Cyberbezpieczeństwo instalacji przemysłowych – fundament projektu „Industry 4.0" i szansa dla Polski* (*Cybersecurity of Industrial Installations - the Foundation of the "Industry 4.0" Project and an Opportunity for Poland*). Kraków (Poland): Instytut Kościuszki.

[18] Kozłowski, A., 2017. *Cyberbezpieczeństwo kluczem do sukcesu przemysłu 4.0* (*Cybersecurity Is the Key to the Success of Industry 4.0*). Retrieved from https://fibis.pl/zagadnienia/czynniki/.

[19] Krajowy Punkt Kontaktowy (2003). *Polskie Platformy Technologiczne* (*Polish Technology Platforms*). Retrieved from https://www.kpk.gov.pl/innowacje/polskie-platformy-technologiczne.

[20] Kukuła, A.J., 2013. Knowledge-based Economy as an Economic Development Strategy for the Twenty-first Century. In: M. Chorośnicki, J.

Węc, A. Czubik, A. Głogowski, I. Krzyżanowska-Skowronek, A. Nitszke, E. Szczepankiewicz-Rudzka, M. Tarnawski (Eds.), *New Strategies for the New Century. The limits and possibilities of regional and global integration*, pp.563-574. Kraków (Poland): Kontekst Press.

[21] Leszczyna, R., 2019. *Cybersecurity in the Electricity Sector: Managing Critical Infrastructure*. Cham (Switzerland): Springer.

[22] Maass, M., Sales, A., Chung, B., Sunshine, J., 2016. A Systematic Analysis of the Science of Sandboxing. *PeerJ Computer Science*, 2, pp.1-36.

[23] Malladi, SS, Subramanian, HC., 2020. Bug Bounty Programs for Cyber Security: Practices, Issues and Recommendations. IEEE Software, 1, pp.31-39.

[24] Mell, P.M., Scarfone, K.A., Romanosky, S., 2007. *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*. Gaithersburg (MD): National Institute of Standards and Technology.

[25] Michalik, J.S., Borysiewicz, M.J., 2009. Poważne awarie i zagrożenia terrorystyczne instalacji chemicznych – metody oceny podatności na zagrożenia (Serious Failures and Terrorist Threats of Chemical Installations - Methods of Vulnerability Assessment). *Bezpieczeństwo Pracy*, 1, pp.2-5.

[26] Mider, D., 2017. *Polacy wobec przemocy politycznej* (*Poles Against Political Violence*). Warszawa (Poland): Dom Wydawniczy „Elipsa".

[27] Morgan, L., Hintermann, F., Vazirani, M., 2016. *Five Ways to Win with Digital Platforms*. Dublin (Ireland): Accenture.

[28] Neittaanmäki, P., Galeieva, E., Ogbechie, A., 2016. *Platform Economy & Digital Platforms*. Jyväskylä (Finland): Jyväskylän yliopisto.

[29] Oxera Consulting, 2015. *Benefits of online platforms*. Retrieved from https://www.oxera.com/getmedia/84df70f3-8fe0-4ad1-b4ba-d235ee50cb30/The-benefits-of-online-platforms-main-findings-(October-2015).pdf.aspx?ext=.pdf.

[30] PwC, 2016. *W obronie cyfrowych granic, czyli 5 rad, aby realnie wzmocnić ochronę firmy przed cyber atakiem* (*In Defense of Digital Borders, or 5 Tips to Really Strengthen Your Company's Protection against Cyber Attacks*). Warszawa (Poland): PwC.

[31] Scarfone, K., Mell, P., 2009. An Analysis of CVSS Version 2 Vulnerability Scoring. In: *3rd International Symposium on Empirical Software Engineering and Measurement*, pp.516-525. Massachusetts (DC): ILEE Computer Society.

[32] Sibalija, T., 2011. *European Technology Platforms as a generator of new technologies and innovation*. Retrieved from https://www.researchgate.net/publication/259485228_European_Technology_Platforms_as_a_generator_of_new_technologies_and_innovation.

[33] Siemaszko, A., Snarska-Świderska, M., 2012. Polskie Platformy Technologiczne. In: A. Bąkowski, M. Mażewska (Eds.), *Ośrodki innowacji i przedsiębiorczości w Polsce. Raport* (*Innovation and Entrepreneurship Centers in Poland. Report*) 2012, pp.169-172. Warszawa (Poland): Polska Agencja Rozwoju Przedsiębiorczości.

[34] Statista, 2017. *Industries Impacted by Cyber Attacks Worldwide*. Retrieved from https://www.statista.com/statistics/784590/cyber-attacks-on-industries-worldwide-2017/.

[35] Stouffer, K.A., 2004. *System Protection Profile - Industrial Control Systems Version 1.0*. Gaithersburg (MD): National Institute of Standards and Technology.

[36] Sun, R., Keating, B., Gregor, S., 2015. Information Technology Platforms: Definition and Research Directions. In: F. Burstein, H. Scheepers, G. Deegan (Eds.), *Proceedings of the 26th Australasian Conference on Information Systems (ACIS)*, 2015, pp.1-17. Auckland (New Zealand): University of Technology Sydney.

[37] Śliwa, M., Patalas-Maliszewska, J., 2016. A Strategic Knowledge Map for the Research and Development Department in a Manufacturing Company. Foundations of Management, Vol. 8, Issue 1, pp.151-166. https://doi.org/10.1515/fman-2016-0012.

[38] Wintermeyer, L., Markowa, D., 2017. *A Development in Open Innovation. Industry Sandbox Consultation Report*. London (UK): Industry Sandbox.