RESEARCH ON ICT INNOVATION IN HUNGARIAN SMES

Adam Bela Horvath*[1]

[1] *Óbuda University, Bécsi street 96/B, Budapest, 1034, Hungary, horvath.adam@kgk.uni-obuda.hu, (+36303571127)*

Abstract

Aim of the research: the aim of the research was to assess the extent to which Hungarian enterprises use Industry 4.0 technologies, with a particular focus on Internet of Things (IoT) technology-based solutions. In contrast to most international research, IoT automated data collection and automated control technologies are treated separately. A secondary aim of the research is to analyse whether the application of innovative technologies is being addressed as a tactical/strategic issue alongside information security issues. in addressing these two issues, we will examine the short- and long-term impact of innovative solutions on the for-profit organizations. The research is based on the responses to a questionnaire survey recorded in 2018. The research included Hungarian for-profit-organizations that are free to choose how they design their ICT environment, so the regulatory environment does not have a binding effect on the IT solutions used by the respondent. The data obtained from the survey were firstly analysed using descriptive statistics, supplemented by some inferential statistical procedures. The results of the analysis proved that IoT devices should be analysed with a higher resolution than before, and that information security dimensions should not be neglected when implementing innovative devices.

Keywords

digital transformation; IoT; Industry 4.0; Information Security; Small- and Medium Enterprises

JEL Classification

O33 Technological Change: Choices and Consequences; Diffusion Processes

DOI: https://doi.org/10.14311/bit.2023.01.22

Editorial information: journal Business & IT, ISSN 2570-7434, CreativeCommons license published by CTU in Prague, 2023, http://bit.fsv.cvut.cz/

Introduction

The radical change and evolution of Information and Communication Technologies (ICT) solutions adopted by business organisations has fundamentally transformed the value creating activities of business organisations. This evolution, which has taken place in sensors, data storage and transmission technologies, and partly therefore in automated decision-making algorithms, has led to the direct integration of ICT infrastructure services into production and/or service processes [1]. This digital transformation has led to the integration of the physical environment and IT (information) systems in business organisations into an inseparable union, creating cyber-physical systems. The result is a flexible and customisable mode of production, where the value creation process (which can consist of production, manufacturing and/or services) is based on real-time data interaction between people, products and the elements of the infrastructure environment involved in production. These technological advances, which include the IoT devices considered in this research, are collectively referred to as Industry 4.0 [2].

In a study [3], Tarutė et al. demonstrated the operational, tactical, and strategic benefits of integrating IT solutions as widely as possible for a supply chain-integrated business organisation. The same study analysed the case of small businesses in the UK, which do not integrate some components of the ICT infrastructure into various business activities through a one-off implementation, but rather an evolutionary path from isolated business applications to the first (at least partially) integrated system implementation. Neirotti et al. [4], analysing the evolution of 284 companies, showed that they invest marginally in their IT infrastructure, especially in the early stages of its development. This may be partly the reason of that fact, according to an Australian survey [5], one third of companies with fewer than 100 employees do not take any preventive measures to guard against malicious acts using IT tools, and 87% of companies consider that only the installation of endpoint security applications (anti-virus programs) is sufficient for their operations. Information security incidents that are (also) attributable to inadequate information security measures can have several consequences: the most obvious consequence is the operational damage that results from the occurrence of the incident. [6] Considering that in the era of Industry 4.0, ICT infrastructure has become an integral part of the production/service processes through its services [9], the issue arises whether it is enough to discuss IT security alone in the life of Industry 4.0 architecture organisations or whether it is necessary to integrate an operational risk approach into the life of business organisations in these cases as well. After all, just as the business operations of financial institutions could be slowed down and temporarily halted by an IT-related failure in the pre-Industry 4.0 era, so in the Industry 4.0 era an IT disruption can bring the life of any company to a temporary standstill [7]. All this is associated with strategic damage, such as the deterioration of market image and positioning, and often has a knock-on effect within a company: it acts as a barrier to innovation decisions on future ICT solutions. In the longer term, this can hamper the development of business organisations. [6]

At the regional level (meaning Central and Eastern Europe and the so-called Visegrad Countries) [11] and specifically in Hungary [9], [10], the use of Industry 4.0 (and in particular: IoT tools) by SMEs has been investigated in several studies. The conclusion is that Hungarian SMEs are either not or minimally behind at regional level, but significantly behind at EU level. In this research I partly reflect on these studies. I will examine the interconnectedness of my data set with respect to IoT technology adoption and whether information security issues are being addressed at a tactical and/or strategic level in parallel to the implementation of innovative technologies.

Methodology of the research

The findings reported in this publication were the result of a non-anonymous questionnaire survey conducted in two waves (spring 2019 to autumn 2019). The aim of this broad survey is to analyse the

ICT infrastructure and information security of business organisations in the light of senior management satisfaction and innovation.

The questionnaire has been developed in line with the literature: the first version of the questionnaire was developed after the source material had been processed. The testing of the questionnaire was modified based on the experience gained from the test-retesting of the questionnaire according to the literature recommendations [12] [13]. The final version of the questionnaire contained a total of 78 questions. the questions were designed according to the following criteria:

- The questionnaire should be able to be completed by a single senior manager. In particular, the questions on the economic and technical conditions of the company should be of a depth that a senior manager can answer as realistically as possible.
- The questionnaire should take between 12 and 15 minutes to complete and should not be unduly burdensome.
- The questionnaire should not give the impression that a market research exercise is being carried out.
- Completion of the questionnaire should not threaten the interests of the respondent.

The questionnaire was completed online using a system called LimeSurvey. Respondents invited by e-mail were selected to have two completed years of business, as this would suggest that they had an established business process structure. Furthermore, it was considered that the respondent should not exclusively produce digital products/services and should operate in an industry that does not have requirements for ICT infrastructure and/or information security through its regulatory regime. (Financial services companies were therefore excluded from the scope of the survey. The questionnaire was not anonymous, as the aim was to be able to attribute accounting reporting data to the responses. the questionnaire survey coincided with the entry into force of the GDRP [14] and, given the unpublished legislation until then, there was a justified fear that the responses to the questions on information security incidents would admit to facts that were sanctioned by that legislation. This effect was reinforced by the fact that the lack of trust among Hungarian entrepreneurs is now a published scientific fact [15].

Consequently, there were a lot of incomplete questionnaires, with about 3-4 incomplete questionnaires for every 1 fully completed questionnaire. Nearly 22.000 companies were involved in the survey and a total of 498 evaluable responses were received. Another negative consequence is that, unfortunately, companies with less than 10 employees (54,90 %, n = 252) and companies with less than 10 million HUF (CZK 800.000 at the then exchange rate) (95,98%) were over-represented.

Results

This chapter presents the results of the questionnaire survey in detail. In the first chapter, I present the theoretical background underlying the analysis of the partial results presented in this paper, followed by a descriptive statistical analysis of the results from the questionnaire responses. The research questions formulated in the theoretical section are answered using the results of inferential statistics procedures.

Background

The sub-research presented in this publication assumes that a part of the respondents has already implemented Industry 4.0 technology-based solutions. I do not investigate what motivated the respondents in their decisions to innovate in ICT infrastructure but treat it as a fact that some of the respondents have adopted Industry 4.0 technologies, so that the operations of these enterprises are comparable to those that have not yet adopted such innovative solutions. As for the investment

decision in ICT infrastructure, I assume that it can be basically either a price-sensitive or a quality-based decision [16]. By quality in this case, I mean not only durability or non-failure, but also the diversity of the service spectrum according to the so-called product-onion model [17]. I also include information-security dimensions in the diversity of the service spectrum, so these aspects may be factors that a price-sensitive decision actor may consider dispensable. If these factors are not considered to the extent necessary, there may be consequences at the operational level and at the tactical/strategic level. In this paper, I seek to answer the following questions:

- Is there any evidence to confirm the hypothesis that price-sensitive decisions are overshadowed by innovation-related decisions?
- Is it possible to confirm the assumption that price-sensitive decisions are less sensitive to the information security dimension?
- If the information security dimensions are neglected when implementing Industry 4.0 technologies, can the short-term consequences be verified?
- If Industry 4.0 technologies are implemented in a way that the information security dimensions are neglected, can the long-term consequences be verified?

Related parts of the questionnaire and descriptives

In the sub-research presented in this publication, I included the following questions from the questionnaire (the name of the variable representing the question is given in brackets):

- **Are ICT infrastructure procurement decisions based on price or quality? (Variable: "cstpur".)** The question could be answered on a Likert-scale of 1 to 5, with one extreme being price-sensitive and the other extreme being decisions based on expected performance. In order to facilitate statistical processing, the values were normalised to 0, 0,25, 0,5, 0,75 and 1. 4.62% of the respondents answered 1 (n=23), 8,23% (n=41) answered 2, 38,55% (n=192) answered 3, 31,93% (n=159) answered 4 and 16,67% (n=83) answered 5.
- **To what extent has the ICT infrastructure had an impact on the structure and/or business processes of the company (variable: "icteff")** This question could also be answered on a Likert-scale of 1 to 5 and the answers were later normalised. 6,43% of the respondents answered 1 (n=32), 12,25% (n=61) answered 2, 24,70% (n=123) answered 3, 35,54% (n=177) answered 4 and 21,08% (n=105) answered 5.
- In one set of questions, **I measured whether the respondent regularly applies risk analysis procedures (riskm) and is prepared to deal with IT-related incidents (bcp).** I used both the risk management procedure as an "indicator" to assess the existence of preventive information security procedures in the first line and the business continuity plan as a "business continuity plan" to assess the existence of reactive information security procedures. The reason for including only tactical/strategic information security tools in this sub-analysis is that I started from the assumption that if tactical/strategic documents exist, they have the appropriate tools to implement the plan. There were five possible answers to this question: „not used“, „in planning“, „in implementation“, „partially used“, „fully used“. The empirical distribution of the responses received is shown in the

following figure 1.:

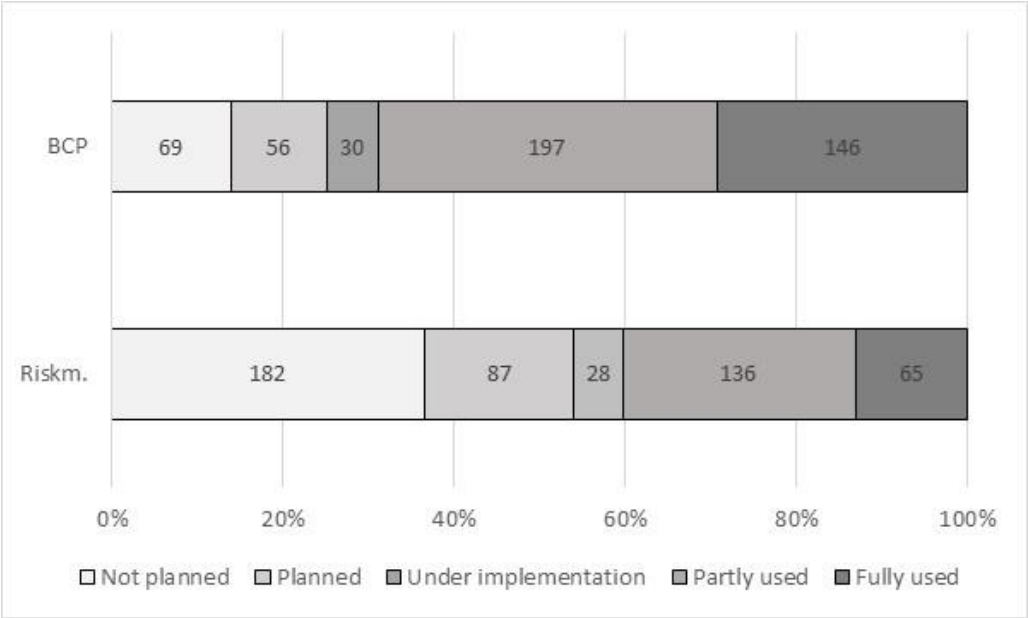

Figure 1: Intensity of use of risk management and business continuity (source: author)

In statistical processing, a value of 0 was assigned to responses where for whatever reason information security solutions are not used ("not planned" and "planned") and a value of 1 was assigned to those who are partially or fully used ("under implementation", "partly used" and "fully used" responses.)

- In a similar way to the previous case, respondents were **asked whether they use IoT tools to extract production data (idata) for automatic production control (ictrl).** The answers were processed in a similar way as it was described for the questions related to the information security procedures.

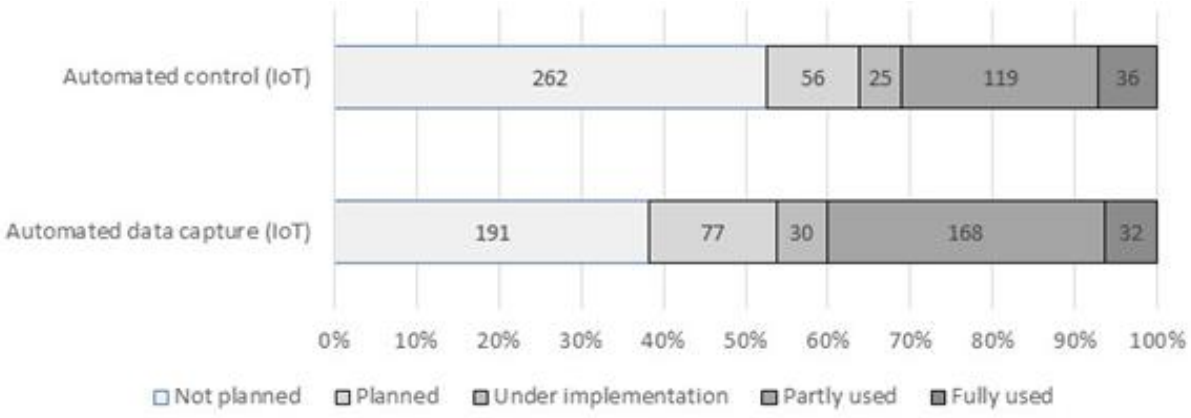

Figure 2: Intensity of use of risk management and business continuity (source: author)

If we analyse the cross-tabulation of idata and ictrl data, we can see that there was a big difference between automated data collection and automated control for respondents. Just over half of the respondents (279 respondents representing 56.20%) were in the 'main diagonal', i.e., they were at the same level of development as automated data collection and control. A further 99 (19.87%) show a 'one degree difference', with a quarter of respondents showing a large contrast between the two dimensions of IoT that I have treated separately (Table 1).

Table 1: The use of different IoT technologies by respondents (source: author)

		Automated data capture (IoT) - idata					
		Not Planned	Planned	Under impl.	Partly used	Fully used	Total
Automated control (IoT) - ictrl	Not Planned	161	30	5	59	7	262
	Planned	7	25	10	12	2	56
	Under impl.	2	4	8	10	1	25
	Partly used	12	14	6	75	12	119
	Fully used	9	4	1	12	10	36
	Total	191	77	30	168	32	498

- The sub-research presented in this paper included two information security incident questions, one on data loss and the other on IT-induced outages. The questionnaire originally had four response options: 'overall incident', 'partial incident', 'no incident' and 'don't know/no response'. As I pointed out in an earlier paper on this research, only those responses that do not include a "don't know/no answer" response can be considered for non-descriptive statistical analysis. The empirical distribution of responses for the two information security incidents is shown in Figure 3 below:

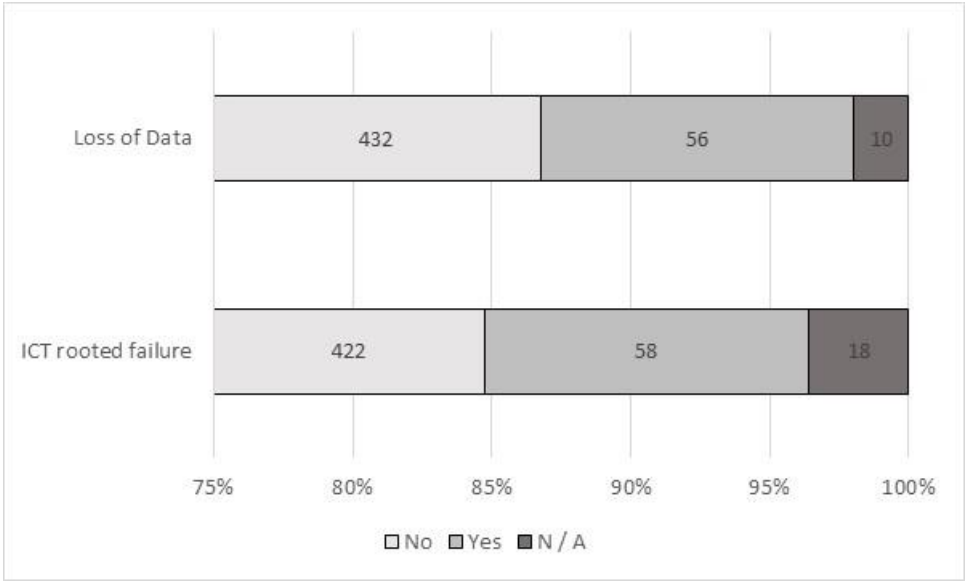

Figure 3: Frequency of information security incidents among respondents (source: author)

In my publication based on the same database [18] I pointed out that responses that contain "I don't know" answers to even one question cannot be included in deeper statistical analysis, so in the later paper, 467 (93.77%) of the 498-answer dataset can be included in deeper statistical analysis. Therefore, my more detailed analysis can be performed on a narrower data set.

Analysis of the replies

First, we investigate how the motivation for ICT infrastructure investments - i.e., whether they are based on price or quality - influences the adoption of IoT devices. (Table 2):

Table 2: The use of IoT technologies in the reflection of price-sensitive attitudes (source: author)

		Price-sensitive vs quality-sensitive investment-attitude - cstpur				
		1	2	3	4	5
Automated data capture (IoT) - idata	no	15 (68,18%)	23 (62,16%)	102 (56,35%)	70 (46,98%)	37 (47,44%)
	yes	7 (31,82%)	14 (37,84%)	79 (43,65%)	79 (53,02%)	41 (52,56%)
Automated control (IoT) - ictrl	no	18 (81,82%)	30 (81,08%)	115 (63,54%)	89 (59,73%)	45 (57,69%)
	yes	4 (18,18%)	7 (18,92%)	66 (36,46%)	60 (40,27%)	33 (42,31%)
Total		22 (100 %)	37 (100 %)	181 (100%)	149 (100%)	78 (100%)

Overall, we can see that, on the one hand, the less respondents base their investment decision on price and the more they base their investment decision on quality, the more likely they are to be open to the systematic implementation of innovative solutions. This table also confirms the findings that technologies implementing automated data collection and automated control should not be treated in the same way and should be assessed separately. Although there is a clear trend of improvement for both automated data collection and automated control, the $\chi 2$ test was significant only between price-sensitive purchase attitude and automated control ($\chi 2 = 12{,}379$, $p < 0{,}05$), the relationship between price-sensitive purchase attitude and automated data collection was not found to be statistically significant ($\chi 2 = 7{,}747$, $p = 0{,}1013$).

Similarly, I examine the impact of price-sensitive and service-based investment attitudes on information security attitudes (Table 3):

Table 3. Implementation of Information security tactical / strategic procedures in the reflection of price-sensitive attitudes (source: author)

		Price-sensitive vs quality-sensitive investment-attitude - cstpur				
		1 (price-sensitive)	**2**	**3 (balanced)**	**4**	**5 (quality-sensitive)**
Risk management - riskm	**no**	13 (59,09%)	29 (75,68%)	93 (51,38%)	79 (53,02%)	37 (47,44%)
	yes	9 (40,91%)	9 (24,32%)	88 (48,62%)	70 (46,98%)	41 (52,56%)
Business Continuity Plan - bcp	**no**	9 (40,91%)	16 (43,24%)	46 (25,41%)	31 (20,81%)	13 (16,67%)
	yes	13 (59,09%)	21 (56,76%)	135 (74,59%)	119 (79,19%)	65 (83,33%)
összesen		**22 (100 %)**	**37 (100 %)**	**181 (100%)**	**149 (100%)**	**78 (100%)**

The above table indicates that there is an evolution in both risk management and business continuity in the sense that the less price-sensitive (i.e., the more quality-oriented) the attitude towards ICT investments, the more importance is given to the consideration of both preventive and reactive information security factors. Considering the fluctuations, i.e., that this development does not follow a strictly monotonic trend, I tested the significance of the relationship between the variables using $\chi 2$-tests. The tests indicated both the relationship between risk management - price sensitivity ($\chi 2=9{,}084$; $p < 0{,}1$) and the relationship between business continuity plan and price sensitivity ($\chi 2=13{,}946$; $p < 0{,}01$) as significant.

Based on this result, I examined what percentage of respondents in each category reported an information security incident:

As previous research [18] has shown, respondents could have interpreted the question on the two incidents in many ways. One could imagine an information security incident with multiple dimensions (e.g., if a server goes down, it could result in data loss and downtime at the same time), two unrelated events, and two related events where one event is the trigger for the other. In designing the questionnaire, it is not possible to distinguish between these alternatives and respondents cannot be expected to evaluate in the same way information security incidents whose damage event involves more than one dimension. Therefore, I examined the average number of information security incidents reported by each respondent in the light of price sensitivity and each information security measure. The average, as a measure, is a good representation of information security exposure within the framework of the questionnaire (Table 4):

Table 4: Average frequency of information security incidents in relation to several factors (source: author)

Price-sensitive vs quality-sensitive investment-attitude - cstpur	Risk management - riskm		BCP -bcp	
	no	yes	no	yes
0	0,53	0,22	0,44	0,38
0,25	0,17	0,11	–	0,28
0,5	0,18	0,18	0,19	0,17
0,75	0,32	0,25	0,48	0,24
1	0,21	0,17	0,38	0,15

Two trends emerge from the table: on the one hand, regardless of whether they use risk management techniques or have a business continuity plan, the less price-driven their investments in ICT infrastructure, the less likely they are to experience an information security incident. In other words: the consequence of non-price sensitive ICT investments is that they can be expected not only to deliver a wider range of services in ICT infrastructure, but also to reduce the likelihood and impact of malfunctioning and its consequences. More specifically, the reduction in intensity may mean both a reduction in the probability of occurrence and lower losses.

The rate of intensity reduction clearly shows that the application of risk management procedures is less effective than the existence of a business continuity plan. An explanation for this phenomenon may be the fact that risk management is required by several standard procedures, even those that are not related to the operation of the ICT infrastructure (e.g., HACCP).

Last but not least, I should point out that in Table 4 I have examined 2*5=10 cases. Out of these 10 cases, the number of information security incidents decreased in 8 cases, remained unchanged in 1 case and in 1 case the change cannot be interpreted.

In the perspective of these findings, I have finally examined the combined impact of the use of IOT tools and IT security procedures on the performance of business organisations (Table 5):

Table 5: Impact of the factors examined in the survey on respondents' organizational functioning (source: author)

	idata	ctrl	riskm	bcp
Effect of ICT-infrastructe - icteff	χ^2= 37,56 p < 0,001	χ^2 = 31,94 p < 0,001	χ^2= 49,02 p < 0,001	χ^2= 49,08 p < 0,001

On this basis, the following regression model can be built:

$$icteff = 0{,}454^{***} + 0{,}062 * idata^{*} + 0{,}076 * ictrl^{***} + 0{,}111 * bcp^{***} + 0{,}085 * riskm^{**} \quad (1)$$

The regression model (1) is significant based on global testing (R^2 = 0,2605; $F_{4,462}$ = 20,7 and p < 0,001), and as can be read, for each variable, partial testing confirmed significance (significance indicators are: ***: p < 0,001; **: p < 0,01; *: p < 0,05)

The significance of the model is that the operation of the for-profit organizations is affected not only by the ICT infrastructure, but also by the tactical or strategic management of information security issues. Thus, if an entity unilaterally introduces innovation tools and/or ignores factors that should complement the ICT infrastructure, then long-term distortions in the life of the entity can be expected and the optimal operation expected from the technological infrastructure can not be expected.

Discussion and conclusion

One of the intended outcomes of the partial research in this paper was to highlight the short- and long-term adverse effects of price-sensitive purchasing. These results can be used to answer the research questions posed in the introduction to these publications:

The first research question was: " Is there any evidence to confirm the hypothesis that price-sensitive decisions are overshadowed by innovation-related decisions?"

From the data presented in Table 2, we can see that the less price-sensitive the ICT investment attitude of firms (which also means that they tend to make decisions based on the benefits of services), the more likely they are to be open to integrating technology around Industry 4.0. While it is true that the χ2 test did not show a significant relationship between price/quality sensitivity and automatic data collection, this phenomenon can also be explained by the fact that automatic data collection can be implemented not only with IoT tools (barcode, QR code, RFID) and respondents cannot necessarily be assumed to have all the technological knowledge at their disposal. Nevertheless, also considering that automated data collection has increased from 31.82% to 52.56% for price-sensitive decision makers, I consider this trend to imply that non-price-sensitive purchasing attitudes have a significant impact on ICT innovation. A similar finding can be made between price/quality sensitivity and automatic control, where although the rate of improvement is not as large, the χ2 test still reveals a significant relationship.

The second research question was: "Is it possible to confirm the assumption that price-sensitive decisions are less sensitive to the information security dimension?"

There is a much clearer way to answer this question in the affirmative than between a price-sensitive ICT investment attitude and the systematic adoption of IoT devices. As we have seen, both risk management and business continuity have increased in frequency (even if not in a strictly monotonic way in one case). The same fact is confirmed by the fact that those who consider themselves as fully price-sensitive investors on average adopt 1,00 of the two information security strategy tools, while for those who consider themselves as fully quality-oriented investors this ratio rises to 1,35 (the mean for the restricted sample is 1,21).

The third research question was: "*If the information security dimensions are neglected when implementing Industry 4.0 technologies, can the short-term consequences be verified*? "

As we have observed in Table 4, both the application of risk management procedures and the preparation and implementation of a business continuity plan significantly reduced the intensity of information security incidents. It should be added that other research on the same database has shown that the appropriateness of information security measures is not uniform and in many cases they are contingent. It should be added that in the same study I pointed out that, unfortunately, an information

security measure has a risk-reducing effect in the case of one type of risk and a risk-increasing effect in the case of another type of risk.

The fourth research question was: "*If the information security dimensions of the introduction of Industry 4.0 technologies are overshadowed, can the long-term consequences be verified?*"

By using the regression model presented in (1), I have shown that information security strategy procedures have an impact on the whole for-profit organisation. If they are not embedded in the life of the enterprises, it is not simply that they make it more operationally vulnerable to incidents.

References

[1] MITTAL, S., KHAN, M. A., ROMERO, D. & WUEST, T. (2018). A critical review of smart manufacturing & Industry 4.0 maturity models: Implications for small and medium-sized enterprises (SMEs*). Journal of Manufacturing Systems*, 49: 194–214. https://doi.org/10.1016/j.jmsy.2018.10.005

[2] ZHOU, K., LIU, T. &, ZHOU, L. (2018). Industry 4.0: Towards future industrial opportunities and challenges In: Tang, Z. (ed): *12th International Conference on Fuzzy Systems and Knowledge Discovery*, IEEE, Piscataway, NJ,. 2147–2152. https://doi.org/10.1109/FSKD.2015.7382284.

[3] TARUTĖ, A. & GATAUTIS, R. (2014). ICT impact on SMEs performance. *Procedia - Social and Behavioral Sciences*, 110:1218-1225. 10.1016/j.sbspro.2013.12.968.

[4] NEIROTTI, P., RAGUSEO, E. & PAOLUCCI, E. (2017). How SMEs develop ICT-based capabilities in response to their environment: Past evidence and implications for the uptake of the new ICT paradigm. *Journal of Enterprise Information Management,* 31(1): 10-37. https://doi.org/10.1108/JEIM-09-2016-0158.

[5] OFFICE OF THE AUSTRALIAN SMALL BUSINESS AND FAMILY ENTERPRISE OMBUDSMAN (2017). *Cyber Security: The Small Business Best Practice Guide*, Commonwealth of Australia 2017

[6] HARICH, T. W. (2021). *IT-Sicherheitsmanagement, 3. Auflage.* mitp-Verlag, ISBN: 9783747501467

[7] NOVAK, A. This is the name of the article. *This is the name of the journal*, 2-2014, pp. 22-25. http://dx.doi.org/10.1234/IV.2014.1234567

[8] SHIPANGA U.-T., LE ROUX, S. & DUBIHLELA, J. (2022). Operational risk factors and the sustainability of small and medium manufacturing enterprises in South Africa. *Insights into Regional Development,* 4(4):126-139. https://dx.doi.org/10.9770/IRD.2022.4.4(7)

[9] NAGY, J. (2017). Az ipar 4.0 fogalma, összetevői és hatása az értékláncra. *Műhelytanulmányok Vállalatgazdaságtan Intézet* (ISSN: 1786-3031), No.167.

[10] TICK, A., KÁRPÁTI-DARÓCZI, J. & SAÁRY, R. (2022). To familiarise or not to familiarise' - industry 4.0 implementation in SMEs in Hungary, In: Milan, Trumić (ed.): *Possibilities and barriers for Industry 4.0 implementation in SMEs in V4 countries and Serbia*, pp. 35-61.

[11] ZBOŘIL, M., SVATÁ, V. (2022). Comparison of cloud service consumption in the Czech republic, Visegrád group and European union. *E+M. Ekonomie a Management = Economics and Manage*ment, (25)3 158–173

[12] MOOSBRUGGER, H. & KELAVA A. (2020): *Testtheorie und Fragebogenkonstruktion*. Spriger Verlag, Berlin-Heidelberg. ISBN: 978-3-662-61531-7

[13] KIRCHHOFF S. (2013): Fragebogen. VS Verlag für Sozialwissenschaften, Wiesbaden. ISBN: 9783663100881

[14] DOGARU, T. C. (2021). National Paths on Implementing EU GDPR: A Legal Approach. *Curierul judiciar*, ID: 3793831. Available at SSRN: https://ssrn.com/abstract=3793831

[15] BALÁS G., CSITE A., SZABÓ-MORVAI Á. & SZEPESI B. (2010). *BIZALOM ÉS VÁLLALKOZÁS MAGYARORSZÁGON – KIINDULÓPONTOK*. HÉTFA Kutatóintézet, Budapest. ISBN: 978-963-08-0280-2

[16] ELHUSSEINY, H. M. & CRISPIM, J (2022). SMEs Barriers and Opportunities on adopting Industry 4.0: a Review. *Procedia Computer Science*, 196:864-871. https://dx.doi.org/10.1016/j.procs.2021.12.086

[17] ROYO, M. P., TRICÁS, J. & TOMÁS X. (2005). Improving quality in the spanish electrical sector: A QFD application. *Total Quality Management & Business Excellence*, 16(4):[15555-569, https://dx.doi.org/10.1080/14783360500078623

[18] HORVÁTH, Á. B. (2021). A magyarországi gazdálkodó szervezetek információbiztonsági jellemzőinek empirikus elemzése. BIZTONSÁGTUDOMÁNYI SZEMLE, 3(1): 79-90