sciendo

ICT Security Measures for the Companies within European Union Member States – Perspectives in COVID-19 Context

Georgeta-Madalina MEGHISAN-TOMA
Bucharest University of Economic Studies, Bucharest, Romania
Romanian Academy, National Institute of Economic Research "Costin C. Kiritescu", Bucharest, Romania
madalina.meghisan@fabiz.ase.ro

Vasile Cosmin NICULA
Bucharest University of Economic Studies, Bucharest, Romania
vasilecosminnicula@gmail.com

Abstract. *The development of ICT usage in households, by individuals or in enterprises is submitted to the requirements of security. This paper aims a statistical analysis of ICT security aspects from several perspectives: ICT policies, staff awareness of ICT security related issues, ICT security related activities. The methodology used for testing the hypotheses is based on descriptive statistics, chart case study, correlation and factor analysis. The results emphasize the importance of investing resources in cyber security, moreover, in the current pandemic situation generated by COVID-19.*

Keywords: ICT security, security policy, security measures, company ICT security, security incidents.

Introduction

The need for cybersecurity integration within the companies has developed together with the ICT usage. An increasing number of worldwide countries are aware of the importance of a constant investment in cybersecurity. For example, Singapore is considered to be "the most globally connected country in the world", being rated in "the top in the world of cybersecurity strategy" (Ter, 2018) The same author underlines that "at least 8% of the government's infocomm technology budget" (Ter, 2018) is allocated to the infrastructure of cybersecurity, in this country. For the companies, this approach needs to be an inspirational one, in order to raise awareness of the importance of surveilling the ICT security system within the organization.

The paper aims to analyze the following key factors: ICT security policies, staff awareness of ICT security related issues, ICT security related activities, at the level of the European Unions' member states, in order to find new perspectives for providing competitive ICT security measures in the new context, generated by COVID-19 crisis.

The research article has the following structure. In the "Literature review part", the focus is on the definition of cybersecurity and its effects on the current business environment. The "Research methodology" part uses a set of variables on ICT security policies, staff awareness of ICT security related issues, ICT security related activities. The "Results" part underlines the main findings of this research article, based on the set of hypotheses to be validated/ invalidated. The "Conclusions" part states the importance of this topic, in the current pandemic situation and opens up new research perspectives.

Literature review

Several authors defined the term of cyberspace. According to Gendron (2013), cyberspace represents "the entire spectrum of network information and communication technologies and systems worldwide as well as the physical hardware".

According to some researchers, "minor players with malevolent intentions can challenge the resources of states and major corporate entities" (Nam, 2019; Griffy-Brown et al., 2016; Miller and Griffy-Brown, 2018) In this context, small and medium-sized enterprises are considered to be "among the least mature and most vulnerable in terms of their cybersecurity risk and resilience" (Benz and Chatterjee, 2020).

The importance of this subject comes from the fact that cybersecurity damages are foreseen "to cost the world $6 trillion annually by 2021, up from $3 trillion just a year ago" (Benz and Chatterjee, 2020). That's why, in this context, the cybersecurity measures are closely linked to "organizational survival and growth" (Hooper and MckKissack, 2016; Benz and Chatterjee, 2020). Many researchers in this field underline the fact that the companies need to put in practice ICT security measures and policies, in a strong link to "a well- planned strategy" (Conick, 2017).

In order to face the security challenges, the organizations need cybersecurity workforce. However, according to several studies, "the existing cybersecurity workforce cannot satisfy the increasing demand for qualified cybersecurity professionals" (Cabaj et al., 2018), in the context of the current need "to implement sustainability in education through curriculum" (Dima and Meghisan-Toma, 2018) Thus, educational system should develop a new curriculum in this field, closely related to the business environment demands. McDuffie and Piotrowski (2014) suggest beginning from baccalaureate-level, by creating "specific cybersecurity baccalaureate-level degree programs".

Methodology

In order to assess how the companies from the European Union member states deal with the security issues, a set of variable was chosen, based on their availability on Eurostat database. The covered years were 2019 and, for some variables, also 2015 (Table 1).

Table 1. Variables for ICT security measures

Variabile	Years of analysis
(Item 1) Enterprises using any ICT security measure	2019
(Item 2) The enterprise's ICT security policy was defined or most recently reviewed within the last 12 months	2015, 2019
(Item 3) The enterprise's ICT security policy was defined or most recently reviewed more than 12 months and up to 24	2015, 2019
(Item 4) The enterprise's ICT security policy was defined or most recently reviewed more than 24 months ago	2015, 2019
(Item 5) The enterprise's ICT security policy was defined or most recently reviewed within the last 24 months	2015, 2019
(Item 6) Enterprises have document(s) on measures, practices or procedures on ICT security	2019
(Item 7) Enterprises make persons employed aware of their obligations in ICT security related issues by voluntary training or internally available information (e.g. information on the intranet)	2019
(Item 8) Enterprises make persons employed aware of their obligations in ICT security related issues by compulsory training courses or viewing compulsory material	2019
(Item 9) Enterprises make persons employed aware of their obligations in ICT security related	2019

issues by contract (e.g. contract of employment)	
(Item 10) Enterprises make persons employed aware of their obligations in ICT security related issues	2019
(Item 11) Enterprises don't make persons employed aware of their obligations in ICT security related issues	2019
(Item 12) The ICT security related activities are carried out by the own employees	2019
(Item 13) The ICT security related activities are carried out by external suppliers	2019
(Item 14) The ICT security related activities are carried out by own employees or external suppliers	2019

Source: Authors' own processing data based on Eurostat, https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database, accessed 01.06.2020

The current research is based on the following hypotheses:

H1. Enterprises that use any ICT security measure have documents on measures, practices or procedures on ICT security;

H2. The enterprise's ICT security policy was defined or most recently reviewed within the last 24 months the latest;

H3. Most often, enterprises make persons employed aware of their obligations in ICT security related issues;

H4. The ICT security related activities are carried out by own employees or external suppliers.

The methodology used for testing the hypotheses is based on descriptive statistics, chart case study, correlation and factor analysis.

H1. Enterprises that use any ICT security measure have documents on measures, practices or procedures on ICT security.

In order to validate/ invalidate this hypothesis, chart case study and correlation function were used, with the following variables (Figure 1):

- (Item 1) Enterprises using any ICT security measure;
- (Item 6) Enterprises have document(s) on measures, practices or procedures on ICT security.

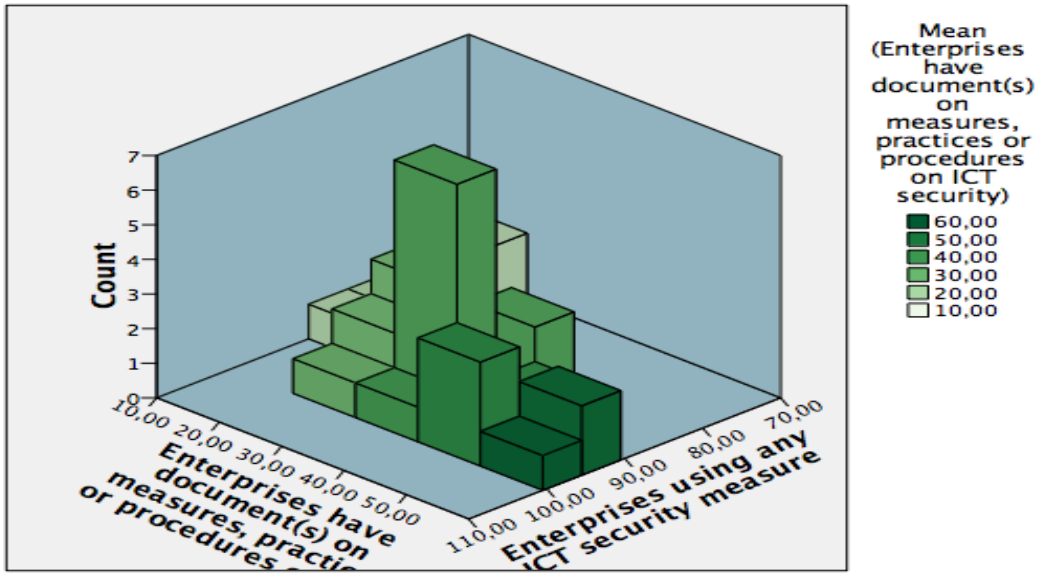


Figure 1. Chart case study on the ICT security measures

Source: Authors' own processing data using SPSS 21.00 software

The results from the Figure 1 show the relationship between (Item 1) Enterprises using any ICT security measure and (Item 6) Enterprises have document(s) on measures, practices or procedures on ICT security.

Spearman's correlation coefficient was used in order to assess the connection between (Item 1) Enterprises using any ICT security measure and (Item 6) Enterprises have document(s) on measures, practices or procedures on ICT security. Spearman's correlation coefficient is 0,625 (Table 2).

Table 2. Correlation matrix (Item 1, Item 6)

			Item 1	**Item 6**
Spearman's rho	Item 1	Correlation Coefficient	1,000	0,625**
		Sig. (2-tailed)	.	0,000
		N	28	28
	Item 6	Correlation Coefficient	0,625**	1,000
		Sig. (2-tailed)	0,000	.
		N	28	28
**. Correlation is significant at the 0.01 level (2-tailed).				

Source: Authors' own processing data using SPSS 21.00 software

H2. The enterprise's ICT security policy was defined or most recently reviewed within the last 24 months, the latest.

In order to validate/ invalidate this hypothesis, factor analysis and correlation analysis were employed. The factor analysis serves at the identification of the structure dimensions for the factor ICT security policy. The analyzed four dimensions are:

- (Item 2) The enterprise's ICT security policy was defined or most recently reviewed within the last 12 months;
- (Item 3) The enterprise's ICT security policy was defined or most recently reviewed more than 12 months and up to 24;
- (Item 4) The enterprise's ICT security policy was defined or most recently reviewed more than 24 months ago;
- (Item 5) The enterprise's ICT security policy was defined or most recently reviewed within the last 24 months;

The KMO and Bartlett's test measure the proportion in which the chosen variables form a coherent assembly. In order to represent an acceptable factor solution, its value has to be between 0,3 and 0,7. In the current analysis, KMO and Bartlett's Test value is 0,423 (Table 3).

Table 3. KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,423
Bartlett's Test of Sphericity	Approx. Chi-Square	356,562
	df	3
	Sig.	0,000

Source: Authors' own processing data using SPSS 21.00 software

The unidimensional solution explains the variation in a percentage of 88,359% (Table 4).

Table 4. Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2,651	88,359	88,359	2,651	88,359	88,359
2	0,348	11,597	99,956			
3	0,001	0,044	100,000			
Extraction Method: Principal Component Analysis.						

Source: Authors' own processing data using SPSS 21.00 software

The three variables that describe the data in a synthetically manner, for the factor ICT security policy, are (Table 5):

- (Item 2) The enterprise's ICT security policy was defined or most recently reviewed within the last 12 months;
- (Item 3) The enterprise's ICT security policy was defined or most recently reviewed more than 12 months and up to 24;
- (Item 5) The enterprise's ICT security policy was defined or most recently reviewed within the last 24 months;

Table 5. Component Matrix[a]

	Component
	1
The enterprise's ICT security policy was defined or most recently reviewed within the last 12 months	0,951
The enterprise's ICT security policy was defined or most recently reviewed more than 12 months and up to 24 months ago	0,874
The enterprise's ICT security policy was defined or most recently reviewed within the last 24 months	0,991
Extraction Method: Principal Component Analysis.	
a. 1 components extracted.	

Source: Authors' own processing data using SPSS 21.00 software

The coefficient Cronbach's Alpha is 0,850, the scale has an acceptable viability of internal coherence (Table 6).

Table 6. Reliability Statistics

Cronbach's Alpha	**N of Items**
0,850	3

Source: Authors' own processing data using SPSS 21.00 software

The level of connection between the chosen items is displayed in the Table 7. All the retained 3 items have a strong positive correlation between them.

Table 7. Correlations matrix (Item 2, Item 3, Item 5)

		Item 2	Item 3	Item 5
Item 2	Pearson Correlation	1	0,683**	0,983**
	Sig. (2-tailed)		0,000	0,000
	N		56	56
Item 3	Pearson Correlation		1	0,801**
	Sig. (2-tailed)			0,000
	N			56
Item 5	Pearson Correlation			1
	Sig. (2-tailed)			
	N			56
**. Correlation is significant at the 0.01 level (2-tailed).				

Source: Authors' own processing data using SPSS 21.00 software

H3. Most often, enterprises make persons employed aware of their obligations in ICT security related issues.

Descriptive statistics is employed for validating/ invalidating the hypothesis (Table 8):

- (Item 7) Enterprises make persons employed aware of their obligations in ICT security related issues by voluntary training or internally available information (e.g. information on the intranet) (with variations from 24% to 60% at the level of the EU-28);
- (Item 8) Enterprises make persons employed aware of their obligations in ICT security related issues by compulsory training courses or viewing compulsory material (with variations from 7% to 42% at the level of the EU-28);
- (Item 9) Enterprises make persons employed aware of their obligations in ICT security related issues by contract (e.g. contract of employment) (with variations from 14% to 57% at the level of the EU-28);
- (Item 10) Enterprises make persons employed aware of their obligations in ICT security related issues (with variations from 33% to 76% at the level of the EU-28);
- (Item 11) Enterprises don't make persons employed aware of their obligations in ICT security related issues (with variations from 20% to 52% at the level of the EU-28);

Table 8. Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
(Item 7) Enterprises make persons employed aware of their obligations in ICT security related issues by voluntary training or internally available information (e.g. information on the intranet)	28	24,00	60,00	43,4286	9,09794
(Item 8) Enterprises make persons employed aware of their obligations in ICT security related issues by compulsory training courses or viewing compulsory material	28	7,00	42,00	22,9286	8,95225
(Item 9) Enterprises make persons employed aware of their obligations in ICT security related issues by contract (e.g. contract of employment)	28	14,00	57,00	34,5714	11,26591
(Item 10) Enterprises make persons employed aware of their obligations in ICT security related issues	28	33,00	76,00	59,1786	10,08135

(Item 11) Enterprises don't make persons employed aware of their obligations in ICT security related issues	28	20,00	52,00	38,0000	9,18533
Valid N (listwise)	28				

Source: Authors' own processing data using SPSS 21.00 software

H4. The ICT security related activities are carried out by own employees or external suppliers.

Descriptive statistics is employed for validating/ invalidating the hypothesis (Table 9):

- (Item 12) The ICT security related activities are carried out by the own employees (with variations from 30% to 65% at the level of the EU-28);
- (Item 13) The ICT security related activities are carried out by external suppliers (with variations from 43% to 77% at the level of the EU-28);
- (Item 14) The ICT security related activities are carried out by own employees or external suppliers (with variations from 71% to 99% at the level of the EU-28);

Table 9. Descriptive Statistics

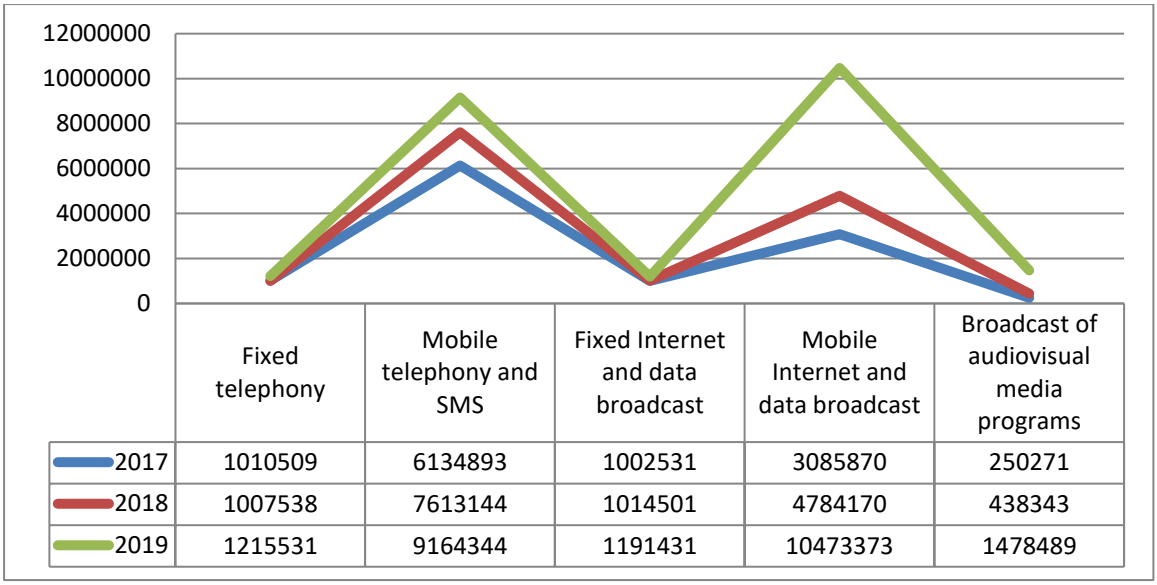
	N	Minimum	Maximum	Mean	Std. Deviation
(Item 12) The ICT security related activities are carried out by the own employees	28	30,00	65,00	42,4643	8,66445
(Item 13) The ICT security related activities are carried out by external suppliers	28	43,00	77,00	63,0000	8,94013
(Item 14) The ICT security related activities are carried out by own employees or external suppliers	28	71,00	99,00	85,6786	7,03459
Valid N (listwise)	28				

Source: Authors' own processing data using SPSS 21.00 software

Case study on Romania

The companies are not the only entities that are concerned by a secure network access for fulfilling their activities. Providers of public network electronic communications or electronic communications services for the individuals are also responsible for all the measures in order to diminish the threat of the security issues. Moreover, these providers must report the security issues to the National Authority for Management and Regulation in Communications of Romania (ANCOM) and must obey the national legislation and, more specific, Law no. 140/ 2012 for the approval of the Government Emergency Ordinance no. 111/ 2011 on electronic communications.

According to the data published within the Report regarding the issues that affected the security and the integrity of the electronic communications networks and services (ANCOM, 2020), 794 security related incidents were reported in 2019. The most affected networks were Mobile Internet and data broadcast services (10,473 mil. affected connections) and Mobile telephony and SMS services (9,164 mil. affected connections), at the level of the year 2019. (Figure 2) One of the main problems for security incidents was issued by the power supply problems at the national level (ANCOM, 2020).



	Fixed telephony	Mobile telephony and SMS	Fixed Internet and data broadcast	Mobile Internet and data broadcast	Broadcast of audiovisual media programs
2017	1010509	6134893	1002531	3085870	250271
2018	1007538	7613144	1014501	4784170	438343
2019	1215531	9164344	1191431	10473373	1478489

Figure 2. Number of connections affected by security incidents
Source: https://www.ancom.ro/uploads/links_files/Raport_incidente_2019.pdf , accessed 10.06.2020

Results and discussions

All the hypotheses are validated: H1. Enterprises that use any ICT security measure have documents on measures, practices or procedures on ICT security; H2. The enterprise's ICT security policy was defined or most recently reviewed within the last 24 months, the latest; H3. Most often, enterprises make persons employed aware of their obligations in ICT security related issues; H4. The ICT security related activities are carried out by own employees or external suppliers.

The cyberattacks towards the companies are more and more present. Thus, the cybersecurity concern became more pregnant in this reality generated by the COVID-19 pandemic situation where, the employees were determined to work from home, challenging companies' cyber security systems. What is more important is the fact that even after the sanitary crisis, most of the big companies will continue in this approach of working from home for their employees. This research opens up new perspectives of further development, mainly underlined by the changes in the business environment in the context of COVID-19.

Conclusion

In the context of this pandemic situation, the companies should pay a deeper attention to ICT security aspects by following more measures, practices or procedures on ICT security; defining and reviewing their ICT security policy in less than 12 months; assuring basic trainings for their own employees in order to rapidly recognize a cyberattack and correctly respond to the exposed situation; making partnerships with security specialized suppliers. In this aspect, the companies from the European Union member states should include greater amounts for ICT security products and services, in their expenses' budgets. Thus, an economic-financial analysis is needed to support the organizations' strategies (Buse et al., 2005), in close connection to the business climate indicators, which "provide an important class of information regarding the perception of current and further performance of economic activity" (Dascalu et al., 2016).

References

Benz, M., Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons,* 63, 531-540.

Buse, L, Siminica, M., Circiumaru, D., Marcu, N. (2005). *Economic-financial analysis (Analiza economic-financiara).* Bucharest: Economica Publishing House.

Cabaj, K., Domingos, D., Kotulski, Z., Respicio, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computer & Security,* 75, 24-35.

Conick, H. (2017). Four things middle market companies must do to improve cybersecurity. *American Marketing Association.* Retrieved from: https://www.ama.org/ marketing-news/four-things-middle-market-companies- must-do-to-improve-cybersecurity /.

Dascalu, E.D., Marcu, N., Pete, S., Ulici, M-L., Dumitrascu, V. (2016). Dependent business climate. A network-based analysis. *Romanian Journal of Economic Forecasting,* XIX(1), 138-152.

Dima, A.M., Meghisan-Toma, G.-M. (2018). Research on implementing education for sustainable development. *Proceedings of the international conference on business excellence,* 12(1), 300-310.

Griffy-Brown, C., Lazarikos, M., Chun, M. (2016). How do you secure an environment without a perimeter? Using emerging technology processes to support information security efforts in an agile data center. *J. Appl. Bus. Econom.,* 18(1), 90-102.

Hooper, V, McKissack, J. (2016). The emerging role of CISO. *Business Horizons,* 59(6), 585-591.

McDuffie, EL., Piotrowski, VP. (2014). The future of cybersecurity education. *Computer,* 47(8), 67-69.

Miller, H., Griffy-Brown, C. (2018). Developing a framework and methodology for assessing cyber risk for business leaders. *J. Appl. Bus. Econom.,* 20(3), 34-50.

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in society,* 58(2019), 101-122.

Ter, K.L. (2018). Singapore's cybersecurity strategy. *Computer Law & Security Review,* 34, 924-927.