University of Salford A Greater Manchester University
University of Essex ESSEX BUSINESS SCHOOL International Centre for Entrepreneurship Research
The General Jonas Žemaitis Military Academy of Lithuania
Ministry of National Defence Republic of Lithuania
Vilnius Gediminas Technical University
RISEBA
Estonian Business School
NATO Energy Security Centre of Excellence
ENTREPRENEURSHIP AND SUSTAINABILITY CENTER
AVADA

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2017 March Volume 6 Number 3
http://dx.doi.org/10.9770/jssi.2017.6.3(10)

CYBERSECURITY FACETS: COUNTERFACTUAL IMPACT EVALUATION OF MEASURE "PROCESAS LT" IN ENTERPRISES OF THE IT SECTOR

Laura Baronienė[1], Vytautas Žirgutis[2]

[1]JSC "Softneta", Barsausko str. 59b, Kaunas, laura.baroniene@softneta.com
[2]Vytautas Magnus University, Economics and Management department. Daukanto str. 28, Kaunas,

E-mail: v.zirgutis@evf.vdu.lt

Received 13 November 2016; accepted 20 January 2017

Abstract. Growth trend of cyber security incidents is being monitored globally; the volume of cyber-attacks is increasing. Cyber statistics data, growing number of certified information management systems show the practical importance of data security at the internationally level. Scientific data security problems solving decisions are represented using technical point of view, protection motivation theory, security standards adopting. This article is created to develop scientific data security approach using productivity as one of the main measurement for the information management systems benefit. Data of measure "Procesas LT" in enterprises of the IT sector shows level of concern and counterfactual impact evaluation creates possibility to verify the expediency of EU funds.

Keywords: counterfactual evaluation, information security management systems, measure "Procesas LT", IT sector, labour productivity

Reference to this paper should be made as follows: Baronienė, L.; Žirgutis, V. 2017. Cybersecurity facets: counterfactual impact evaluation of measure "Procesas LT" in enterprises of the it sector, *Journal of Security and Sustainability Issues* 6(3): 445–456. http://dx.doi.org/10.9770/jssi.2017.6.3(10)

JEL Classifications: O32

1. Introduction

Security in general, is related to the important aspects of confidentiality, integrity and availability; they thus become building blocks to be used in designing secure systems. These important aspects of security, apply to the three broad categories of assets which are necessary to be secured, data, software and hardware resources (Zissis, Lekkas, 2012). The identified security requirements and selected security controls are introduced to the standard systems engineering process, to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability) (National Institute of Standards and Technology. Guide for mapping types of information and information systems to security categories, 2008).

Some articles described a technical point of view: in legally sensitive areas, such as processing of personal information or online voting, compliance with the legal specifications is of high importance, however, for the users' trust in an IT system and thus for the success of this system (Draws, Neumann, Kahlert, Richter, Grimm, Volkamer and Roßnagel, 2013); cloud security challenges are described in "Cloud computing – Implementation, Maangement and Security" (Rittinghouse, Randsome, 2016). Security and privacy challenges in cloud computing environments are mentioned by Takabi, Joshi, Ahn (2011, 2010), Catteddu and Hogben (2009). Trust management as a point of security was mentioned by Blaze et al. (2009), Zhang and Joshi (2009). Another

articles described protection motivation theory (PMT) to assess how its efficacy is influenced by the information security behaviour it is applied to (Karlzén, Hallberg, 2015).

We can find articles about implementation information management systems in several areas, for example, security standards applicable to healthcare industry including Control Objective for Information and related Technology (COBIT), ISO/IEC 27002:2005, ISO/IEC 27001:2005, NIST Special Publication 800-53, ISO 27799:2008, HITRUST Common Security Framework (CSF), ISO 17090:2008, ISO/TS 25237:2008, etc. (Akowuah, Yuan, Xu, Wang, 2013), the contingent effects of management support and task interdependence on successful information systems implementation (Sharma, Yetton, 2003).

Management Information Systems (MIS) can increase Productivity in the Workforce (Barzegar, Araghieh and Asgarani, 2012). Labour productivity experienced in the US in the 1990s was to a good extent attributed to the growth in MIS investment. For example, Oliner et al. (2000) stated that concluded that slightly over 20 percent of U.S. Moreover, 37 percent of labour productivity growth is attributed to "capital deepens" from the use of ICT (Information Communication Technology). Also, Jorgenson et al. (2000) calculated even a higher contribution of approximately 43 percent to total labour productivity growth. Canada is another country with discernible information on the impact of ICT and MIS on labour productivity. For example, in a study by the Bank of Canada, revealed that over the 1996- 2000 period, ICT contributed 0.53 percentage points of the 4.75 per cent growth in business sector output (Khan et al., 2002). Also, Goldstein et al. (2002) assert that introduction of ATMs has definitely increased labour productivity but not necessarily the total factor productivity. This demonstrates that effects of computer diffusion on growth were concentrated in a number of industries (OECD, 2003a).

Hesam Eshraghi, Farideh Ashraf Ganjouei and Mohammad Reza Esmaeili described effect of management information systems on productivity in faculties, groups and offices of physical education and sport sciences in Esfahan Islamic Azad Universities (2015). There was mentioned that the statistics of successes and failures of projects in the field of information technology implemented in developed countries of the world in 2004 reveals this fact that only about 20 percent of them (projects) achieved to a complete success; in other words, nature of projects performance have not been as described in the initial plans and proposals for them as goals. According to the previous studies, about 50% of projects face with partial failures and 30% have been experienced complete failure. NATO strategic security and defence concept of the security environment is defined by the frequency indicator of cyber-attacks.

In the Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organization, adopted by Heads of State and Government in Lisbon, is highlighted that „Cyber-attacks are becoming more frequent, more organized and more costly in the damage that they inflict on government administration, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks".

2. Security of information via cross-border level

Growth trend of cyber security incidents is being monitored globally, the volume of cyber-attacks is increasing (European Commission press release, 2013):

- According to the World Economic Forum data, there is 10 percent probability that in the next decade critical information infrastructure objects will suffer from substantial damage, with losses which could reach 250 billion US dollars.
- Cybercrime represents a significant part of the cyber-security incidents. „Symantec" estimated that worldwide cybercrime victims annually lose about 290 billion euros and „McAfee" revealed that cyber criminals make profit of 750 billion euros annually.
- Eurobarometer survey on cyber security (Special Eurobarometer 390 Cyber security report, 2012) in 2012 showed that 38 percent of EU Internet users have changed their behaviour because of these cyber-security problems: it seems that 18 percent of them will stop buying goods online, and 15 percent will no longer use internet banking. The survey also revealed that 74 percent of respondents think that the risk of becoming a victim of such crimes have increased, 12 percent already have faced with online fraud and 89 percent are

reluctant to disclose personal information.
- The public consultation on network and information systems security, 56.8 percent of respondents indicated that they had experience of networks and information systems security incidents that have had serious consequences for their activities in the last year.

The above-mentioned data show the practical importance of data security at the internationally level. Despite the security flaws and obvious losses, Eurostat data show that by January 2012 only 26 percent of EU companies had officially set in ICT security policy. Such data shows actuality of data security actions that can be implemented using technical and managerial means.

The need for actions to ensure data security confirms also forecast form Information Security Forum. Information Security Forum (ISF) sees five security trends that will dominate 2016 (Olavsrud, 2015):
- The unintended consequences of state intervention
- Big data will lead to big problems
- Mobile applications and the IoT
- Cybercrime causes the perfect threat storm
- Skills gap becomes anabyss for information security.

Each year the Information Security Forum releases its 'Threat Horizon' report to provide a forward-looking view of the biggest security threats over a two-year period. Here are the top nine threats to watch for through 2018 (Olavsrud, 2016):
- The IoT leaks sensitive information
- Opaque algorithms compromise integrity
- Rogue governments use terrorist groups to launch cyberattacks
- Unmet board expectations exposed by a major incident
- Researchers silenced to hide security vulnerabilities
- Cyber insurance safety net is pulled away
- Disruptive companies provoke governments
- Regulations fragment the cloud
- Criminal capabilities expand gaps in international policing

International standardization organization data shows growing interest to standardized information management systems as a way for security problem solving. Certification trends are presented in figure 1 and 2:

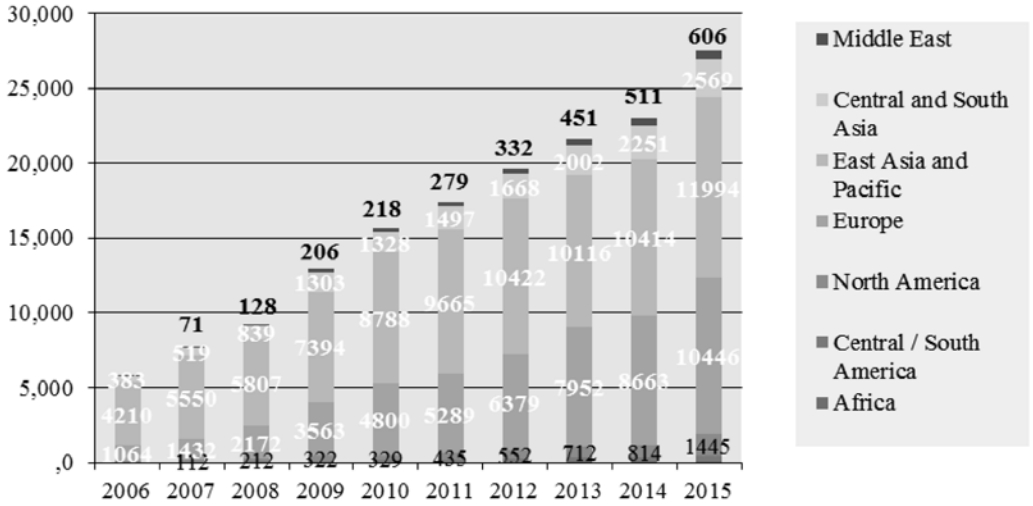

Figure1. ISO/IEC 27001 – Worldwide total

Data source: ISO

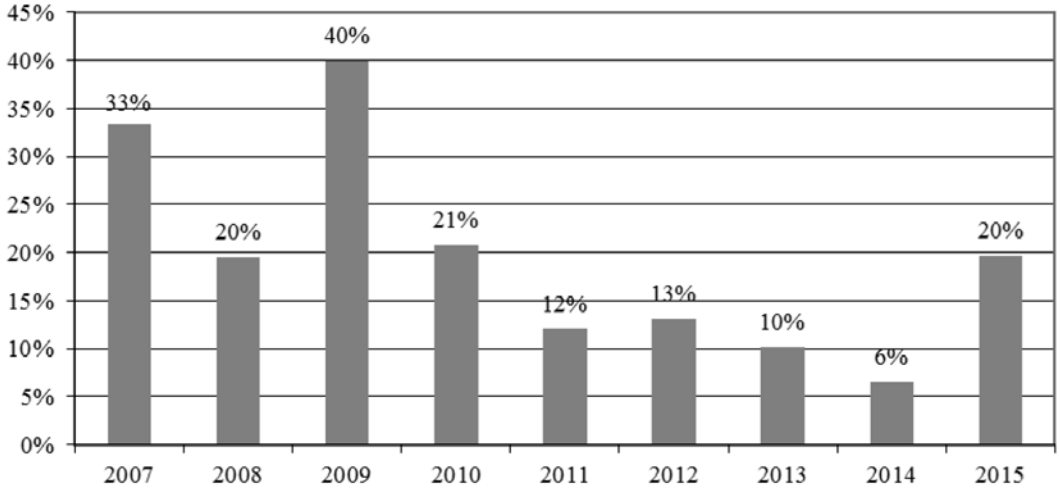

Figure 2. ISO/IEC 27001 – World annual growth (in %)

Data source: ISO

Certification trends show one of the usually optional way to ensure data security. Growing data of certificated information management systems in the world creates possibility to presume the benefit of these systems.

3. Situation in Lithuania

Cybersecurity till 2015 was based on legislation which had no clearly defined institutions which make and implement policies in this field. There was also no definition for duties and responsibilities of cyber security participants, nor as organizational and technical requirements of cyber security and cyber security measures.

At the end of 2014 the major changes in cybersecurity regulatory were made: adoption of the cyber security law, National Cyber Security centre was established by Cyber Security and Telecommunications Office under the Ministry Of National Defence Republic Of Lithuania (National official cyber-security centre, located in the General Jonas Lithuanian Military Academy complex in Vilnius, took place in July 2016), Cyber Security Council was gathered as well.

Cyber security report conclusions (State audit report "Cyber security environment in Lithuania", 2015) mention that „Technical and organizational implementation of cyber security and electronic information measurements in the public sector is insufficient, inadequately prepared to respond to cyber threats, because only 25 percent of organizational arrangements are used to ensure this field. Main disadvantages are associated with creation of security management system, incident management, business continuity, staff competence development and external cooperation".

Though over the past few years, the long and medium-term state planning documents declared support for electronic information security, cyber security development, Cyber Security Act came into force since 2015, every year recorded a growing number of reports of incidents in cyberspace:

- According to Communications Regulatory Authority data (The Communications Regulatory Authority of the National electronic communications network and information security incidents investigation unit in 2014. Activity report) security incidents compared to the previous year, increased by 43 percent in 2014.
- According to National Intelligence and Surveillance authorities data of 2015 (Threats to national security assessment, 2015) cyber-incidents, at least in the nearest future, will not decrease. Cyberspace itself will remain one of the key areas in espionage and will affect other critical infrastructure objects important to National Lithuanian Security and its defence power.
- SE „Centre of Registers" informs that they are constantly exposed to computer hackers and virus attacks, attempts to install spyware software: „working in a normal mode the company every hour captures and con-

trols about 40,000 information security incidents“ (Register centre, 2016).

- Lithuanian Communications Regulatory Authority of the national electronic communications network and information security emergency response team (CERT-LT) have processed 10.991 incidents during the second quarter of 2016 in accordance with Lithuanian electronic communication service providers, foreign CERT teams which are engaged in investigation of international incidents, and messages received from Lithuanian Internet users (www.esaugumas.lt, 2016). In comparison with the second quarter of 2015 (9 527 incidents), incidents have increased by 15.4 percent. CERT-LT reports that 40 percent of all incidents were related to user‘s computer network installations which contain dangerous security vulnerabilities - 4 417. CERT-LT notes that the number of extremely serious incidents - IS occupancy (2 290) and electronic data manipulation (147) – is growing: number of both types of incidents was nearly 80 percent bigger than a year ago. There is a significant increase of disturbance of electronic services In the second quarter of - 36 cases have been registered (I quarter - 10). Continuous disturbance of service attacks (Eng. DDoS) against the institutions, media, banking and private sector websites of the Republic of Lithuania took place in April and May of this year.

National Audit Office of Lithuania report („Cyber security environment in Lithuania“) emphasized that 2011-2019 five year electronic information security (cyber security) development program is inefficient: „Only 23 percent of planned indicators have been achieved till September 2015, 48 percent are partially achieved, 29 percent is not achieved. The overall realization of program objectives so far is only 21 percent“. It is obvious that the public sector is not yet ready to take the proper cyber security challenges.

One of the world‘s largest information technology (IT) companies “Cisco”, who presented an annual survey of Cisco Annual Security Report 2016“, focuses on cyber security challenges of the private sector and claims that the understanding of the potential threats are still insufficient. According to the survey, small and medium-sized enterprises are much less prepared to defend themselves from cyber-attacks than large corporations. EU Structural Funds measure “Process LT” have granted the opportunity for private businesses to take advantage for introducing innovative management systems (including administrative systems that ensure information security such as management systems in accordance with requirements of international standard ISO 27001).

Effectively implement information security management system not only helps to ensure more rigorous requirements to the data security of the interested parties, but also promote consumer confidence, increase labour productivity. Appropriate measures to protect cyberspace, fast and expedient organization’s response to cyber-attacks allows to define indicator of information management systems benefit performance: benefit of information management system can be measured by labour productivity indicator. Such indicator is chosen for the EU Structural Funds measure “Process LT”.

4. Application of counterfactual analysis

Counterfactual analysis is a quantitative evaluation method of the policy impact that allows estimating the net impact of the intervention. The counterfactual analysis aims at comparing the outcome achieved under the intervention with the outcome that would have been achieved in the absence of the intervention. The counterfactual impact evaluation is most suitable to assess the interventions intended to support enterprises (subsidies for business start or corporate development), to increase employment, as well as in the field of education. These interventions are most relevant for the counterfactual impact evaluation, as they are focused on behaviour change, homogeneous, repeatable and demonstrate a sufficient number of beneficiaries. In view of these criteria it has been determined that the tools of the counterfactual impact evaluation are appropriate for the evaluation of measure “Procesas LT” of priority 3 “Promotion of Competitiveness of Small and Medium Enterprises” of the 2014 – 2020 European Investment Funds.

To determine whether the counterfactual methods can be applied to the particular intervention, the four key attributes have been evaluated:
1. Behaviour change. In order to evaluate the impact of the intervention it is necessary to identify a clear criterion that would make it possible to assess whether the behaviour of entities belonging to the target group has changed.

With the purpose of evaluation of the impact of measure "Procesas LT" of priority 3 "Promotion of Competitiveness of Small and Medium Enterprises" of the 2014 – 2020 European Investment Funds (the measure is intended to encourage micro, small and medium sized enterprises to introduce innovative management methods and management systems in order to create favourable conditions for increasing enterprise productivity), the labour productivity indicators are analysed, showing the change in corporate behaviour.

2. Homogeneity. The counterfactual impact evaluation can be carried out only with regard to interventions that are properly homogeneous. It means that the entities shall be engaged in the identical or comparable activities which pursue the same objectives. Besides, homogeneous interventions are based on the equivalent intervention logic. The activities supported by measure "Procesas LT" comprise "development and establishment of non-technological innovations in manufacturing or service processes, providing the product, process and service standards for the implementation in SMEs, supporting innovative management methods and management systems for SMEs". This research is focused on the counterfactual impact evaluation of the organisations that have been granted the support for implementation and certification of the Information Security management system; therefore it can be stated that the analysed intervention is homogeneous.

3. Repeatability. The counterfactual impact evaluation provides the information necessary for deciding whether the intervention should be continued and its scope expanded. If the intervention is unique, it is not possible to apply the results of the counterfactual impact evaluation for improvement of new interventions; therefore such evaluation is not significant. In the course of this research the counterfactual impact evaluation is carried out with the intention of comparing the economic indicators (labour productivity) of the enterprises. Whereas after the intervention not all enterprises operating in Lithuania will have the management systems implemented according to the requirements of the international standards; and in view of the new financial perspective (2014–2020) further support is planned for implementation of innovative management methods, it can be presumed that there are all conditions for repeatability.

4. Number of beneficiaries. For the purpose of this research the target group is Lithuanian organisations operating in the IT sector that have been granted the support and have implemented the projects under measure "Procesas LT", which provide for implementation and certification of the Information Security Management Systems in accordance with the requirements of international standard ISO 27001. In the beginning of 2016 3.303 enterprises were operating in the IT sector. The enterprises of the IT sector that have been granted the support under measure "Procesas Lt" and implemented and certified Information Security management System in accordance with the requirements of ISO 27001 include 3 very small (from 1 to 9 employees) and 4 small (from 10 to 49 employees) sized enterprises. The research further narrows to the analysis of these enterprises. The control group encompasses the organizations representing IT sector, which are differentiated by their size. The relatively small amount of the beneficiaries in the overall proportion of the sector enterprises ensures credibility of the outcome, by integrating the results of the target group into the results of the control group.

The conformity of all the attributes with the application requirements of the counterfactual impact evaluation method provides the basis for conducting the counterfactual impact evaluation of the support under measure "Procesas LT" of priority 3 "Promotion of Competitiveness of Small and Medium Enterprises" of the 2014 – 2020 European Investment Funds in the organizations of the IT sector, which have utilised the funding for implementation and certification of the Information Security Management System compliant with the requirements of ISO 27001.

5. Evaluation of measure "Procesas Lt"

In measuring labour productivity of a sector of the domestic economy, the amount of the gross value added created is used to represent the volume of production. The Department of Statistics of Lithuania applies the same principle for calculating labour productivity of a sector of the domestic economy that is used in the European System of National and Regional Accounts, according to which the compilation of statistics of the national accounts across the EU follows the same common internationally recognized definitions and rules. In this method labour productivity is expressed as the gross value added created per hour actually worked per employee (for-

mula 1) (Department of Statistics of Lithuania, 2009).
Labour productivity = Gross value added/Number of hours actually worked (1)
Accordingly,

Gross value added = Labour productivity * Number of hours actually worked (2)

This calculation method is used for the impact evaluation of measure "Procesas LT" of priority 3 "Promotion of Competitiveness of Small and Medium Enterprises" of the 2014 – 2020 European Investment Funds on changes of the value added in enterprises of the IT sector upon implementation of the Information Security Management System. Labour productivity in enterprises of the IT sector for the period of 2009-2014 is provided in Table 1.

Table 1. Labour productivity in the IT sector

	2009	2010	2011	2012	2013	2014
Enterprises of the IT sector, Euro/h	10,1	12,1	12,0	10,8	17,0	19,8

The statistical data show that labour productivity ir enterprises of the IT sector is growing continuously (this growth is conditioned by the macroeconomic factors). During the analysed period labour productivity in the IT sector increased from 10,10 euro per hour up to 19,8 euro per hour or by 196% (almost twice). Based on the historical trends and using the extrapolation method, the forecasted change in labour productivity has been calculated in the enterprises of the IT sector, which is determined by the macroeconomic factors. The calculations are provided in Table 2.

Table 2. Forecasted labour productivity of the IT sector

	2015	2016	2017	2018
Enterprises of the IT sector, Euro/h	19,7	21,6	23,3	25,1
Change, %	-0,51	9,64	7,87	7,73

The historical and forecasted data of average labour productivity are provided in Figure 3.

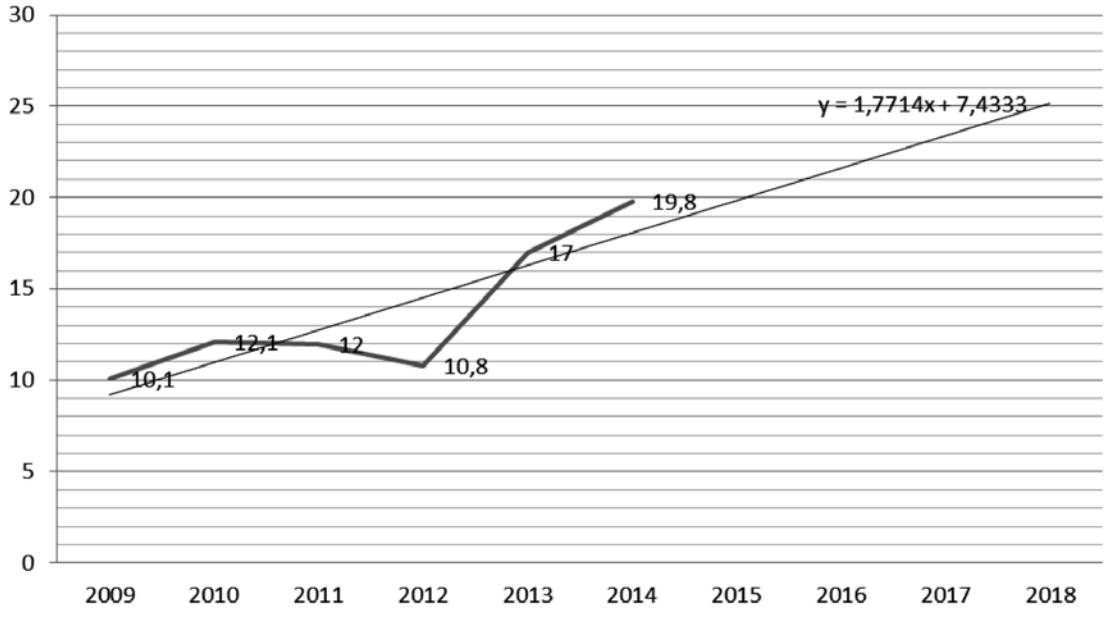

Figure 3. Changes and forecast of labour productivity in the IT sector

Based on the historical data of labour productivity in the IT sector, the forecasted average labour productivity for 2016 – 2018 will grow from 19,7 euro per hour up to 25,1 euro per hour. This suspected grow is driven by IT sector macroeconomics driving forces, such as increase of prices of product or services, development of work automation tools et cetera. However, this forecast presents overall sector tendencies and it is assumed that the factors affecting labour productivity in the entire sector will also affect labour productivity of the enterprises under research, and this effect will be of the same strength.

It is necessary to forecast change of labour productivity of every enterprise of target group because of IT sector macroeconomics driving forces (or sector specific trends) during the period analysed. This forecast requires knowing initial labour productivity however information of such a kind is secure and usually is treated as commercial secret. Trying to avoid possible damage researchers used data that was calculated. Calculations were based on general work schedule rules (8 hours working day, 5 working days per week, 252 working days per year and 28 holydays) and number of employees. The financial statements of the enterprises of target group were analysed for determination of amount of gross value added in every enterprise. Sector specific trends were applied for calculated initial labour productivity in enterprises of the target group. Anonymised calculations are provided in Table 3 (and hereinafter in the text), following the guidelines of the research ethics.

Table 3. Forecasted labour productivity of the enterprises under research, considering the sector-specific trends

Enterprise	Calculated labour productivity, Eur/h	Forecasted labour productivity, Eur/h		
	2015	2016	2017	2018
E1	30,41	33,34	35,97	38,75
E2	42,57	46,68	50,35	54,24
E3	85,34	93,57	100,93	108,73
E4	21,29	23,34	25,18	27,12
E5	22,60	24,78	26,73	28,79
E6	60,64	66,48	71,71	77,26
E7	175,71	192,65	207,82	223,88

Based on the calculation of the forecasted labour productivity of the enterprises under research (considering the impact of the macroeconomic factors), the forecasted value added has been calculated, to be created by the same enterprises in 2016–2018, by assuming that the number of employees will remain unchanged (compare to the end of the 2015) in the enterprises under research. The calculations are provided in Table 4 (there will be 1856 working hours per each year under research).

Table 4. Forecasted value added created by the enterprises under research (considering the macroeconomic factors)

Enterprise	Number of employees, pcs.	Forecasted value added created, Euro		
	2015	2016	2017	2018
E1	3	185.637	200.281	215.760
E2	6	519.828	560.698	604.017
E3	6	1.041.996	1.123.956	1.210.817
E4	10	433.190	467.341	503.347
E5	10	459.917	496.109	534.342
E6	14	1.727.416	1.863.313	2.007.524
E7	11	3.933.142	4.242.853	4.570.734
Total:		**8.301.127**	**8.954.550**	**9.646.541**

According to the calculations provided, the value added created by the enterprises under research will amount to 26.902.219 euro as for the period of 2016–2018.

Enterprises applying for the support under measure "Procesas Lt" shall declare the existing labour productivity and undertake to implement modern management method and thus to increase their labour productivity. Modern management method has to be implemented during 2016 – 2017 and on 2018 enterprises will benefit from increased labour productivity. Thus, "benefiting" means creation more value added than investments for implementing modern management method (or Information Security management system according to ISO 27001 requirements). Investment for establishment of Information Security management system consists of support under measure "Procesas Lt" and own funds of enterprise. According to the same assumptions regarding number of hours actually worked it is possible to count minimum expected labour productivity. The calculations are provided in Table 5.

Table 5. Forecasted of minimum

Enterprise	Forecasted value added (because of sector driving forces) in 2018	Investment for establishmentof ISMS		Minimum expected value added	Minimum expected labour productivity
		"Procesas Lt" funds	Enterprise own funds		
E1	215.760	6.739,50	6.739,50	229.239	41,17
E2	604.017	7.146,50	7.146,50	618.310	55,52
E3	1.210.817	11.126,50	11.126,50	1.233.070	110,73
E4	503.347	7.973,33	7.973,33	519.294	27,98
E5	534.342	6.745,00	6.745,00	547.832	29,52
E6	2.007.524	10.331,50	10.331,50	2.028.187	78,06
E7	4.570.734	7.415,00	7.415,00	4.585.564	224,61
Total:	9.646.541	57.477	57.477	9.761.496	

It is assumed that the projects of implementation of modern management methods funded under measure "Procesas Lt" will be successful: the enterprises that have been granted the support and achieved the project objectives will fulfil the targeted labour productivity obligations. According to the calculations provided, the value added created by the enterprises under research should amount to 9.761.496 euro in 2018. This amount is only 1,19 % higher than the one calculated considering the effect of the macroeconomic factors. In order to identify the minimum expected impact of measure "Procesas Lt", the counterfactual comparison has been carried out with regard to every single enterprise under research; the calculations are provided in Table 6.

Table 6. Counterfactual comparison of measure "Procesas Lt"

Enterprise	Calculated labour productivity in 2015, euro per hour	Minimum expected labour productivity in 2018, euro per hour	Counterfactual comparison, euro per hour	Counterfactual comparison, %
E1	30,41	41,17	10,76	35%
E2	42,57	55,52	12,95	30%
E3	85,34	110,73	25,39	30%
E4	21,29	27,98	6,69	31%
E5	22,60	29,52	6,92	31%
E6	60,64	78,06	17,42	29%
E7	175,71	224,61	48,9	28%

According to the analysed sample and selected assumptions, the support for test group companies should be given only if their minimum obligations to implement modern management methods to increase productivity is from 28 to 35 percent. Counterfactual impact evaluation creates possibility to verify the expediency of EU funds, but the Lithuanian Business Support Agency refused to present data of EU founds received enterprises for the research purposes. Verification could be made by the labour productivity measurement comparison: enterprises obligations to increase labour productivity compare to the estimated value (from 28 to 35 percent).

Conclusions

- Globally growing trend of cyber security incidents, increasing cyber-attacks statistic data shows growing level of concern at the international and at the national level.
- EU founds, directed to ensure labour productivity, are one of the possible ways to implement information management system, but this measure used just few enterprises of Lithuania.
- Data of measure "Procesas LT" in enterprises of the IT sector shows small level of concern.
- Total support according to "Process LT" was designed for 91 companies in 2015. 10 of them next to other systems will integrate 27001 as well. Due to the fact that in 2014 Lithuania had 2 660 information and communication sector owned enterprises, it is estimated that support was given to 0.38 percent of enterprises.
- According to Department of Statistics of Lithuania data, 6.3 percent Lithuanian companies in 2014 was faced with electronic security problems. In assessing the relevance of the support on the identification of cyber security issues, as well as the assumption that the information and communication sector companies belonging to the mentioned problem facing the same extent (6.3 percent of all companies in this sector, - 168 enterprises) support enables the possibility to solve cyber security challenges and increase the productivity of 5.95 percent of enterprises.
- Support under the measure "Process LT" intended for information security management problems solution, has been given to 0.38 percent of Lithuanian information and communication sector companies.
- Support shares the possibility to solve security problems and to increase the productivity of 5.95 percent of Lithuanian information and communication sector companies that encounter security problems.
- According to the analysed sample and selected assumptions, the support for test group companies should be given only if their minimum obligations to implement modern management methods to increase productivity is from 28 to 35 percent.
- Counterfactual impact evaluation creates possibility to verify the expediency of EU funds, but the Lithuanian Business Support Agency refused to present data of EU founds received enterprises for the research purposes. Verification could be made by the labour productivity measurement comparison: enterprises obligations to increase labour productivity compare to the estimated value (from 28 to 35 percent).
- Counterfactual evaluation method is an appropriate measure to provide assistance to ensure conditions which help to ensure effective distribution of support, however there is a need of past data systematic analysis and projections.

References

Barzegar N. Araghieh A. and Asgarani M. 2012. The Role of Management Information Systems (MIS) to Increase Productivity in the Workforce (Case Study of Iran). J. Educ. Manage. Stud., 3(3): 191-194.

Cyber Security and Telecommunications Authority Regulations/ Lietuvos Respublikos krašto apsaugos ministro 2014-12-29 įsakymu Nr. V-1321 patvirtinti Kibernetinio saugumo ir telekomunikacijų tarnybos prie Krašto apsaugos ministerijos nuostatai.

Cyber Security Council Regulation/ Lietuvos Respublikos Vyriausybės 2015-04-23 nutarimu Nr. 422 patvirtinta Kibernetinio saugumo taryba ir jos reglamentas.

D. Catteddu and G. Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," ENISA, 2009; www.enisa.europa.eu/act/rm/ files/deliverables/cloud-computing-risk-assessment/ at_download/fullReport.

Daniela Simić-Draws, Stephan Neumann, Anna Kahlert, Philipp Richter, Rüdiger Grimm, Melanie Volkamer and Alexander Roßnagel. Holistic and Law Compatible IT Security Evaluation: Integration of Common Criteria, ISO 27001/IT-Grundschutz and KORA. International Journal of Information Security and Privacy (IJISP), 2013. Volume 7, issue 3.

Dimitrios Zissis, Dimitrios Lekkas. Addressing cloud computing security issues. Future Generation Computer Systems. Volume 28, Issue 3, March 2012, Pages 583–592.

European Commision press release. EC ciber security plan is created to ensure open internet, electronic freedom and possibilities, Brusel, 2013-02-07.

Eurostat statistics, viewed 2016-11-06 < http://ec.europa.eu/eurostat/statistics-explained/index.php/Main_Page>

Francis Akowuah, Xiaohong Yuan, Jinsheng Xu, Hong Wang. A Survey of Security Standards Applicable to Health Information Systems. International Journal of Information Security and Privacy (IJISP), 2013. Volume 7, issue 4.

Goldstein, A. & O'Connor, D. (Eds.). (2002). Electronic Commerce for Development. Paris: OECD.

H. Takabi, J. B. D., Joshi, G-J. Ahn. Security and privacy challenges in cloud computing environments are mentioned. (2016). IEEE Security and Privacy Magazine. January 2011.

H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Proc. 1st IEEE Int'l Workshop Emerging Applications for Cloud Computing (CloudApp 2010), IEEE CS Press, 2010, pp. 393–398.

Hesam Eshraghi, Farideh Ashraf Ganjouei and Mohammad Reza Esmaeili. Effect of management information systems on productivity in faculties, groups and offices of physical education and sport sciences in Esfahan Islamic Azad Universities. Indian Journal of Fundamental and Applied Life Sciences ISSN: 2231– 6345 (Online) An Open Access, Online International Journal Available at www.cibtech.org/sp.ed/jls/2015/03/jls.htm 2015 Vol. 5 (S3), pp. 1010-1017.

ISO survey. Viewed at 2016-10-23 <http://www.iso.org/iso/iso-survey>.

J. W. Rittinghouse, J. F. Randsome. Cloud computing – Implementation, Maangement and Security", CRC Press, 2016.

Jorgenson, D. &Stiroh, K. (2000). Raising the Speed Limit: U.S. Economic Growth in the Information Age. Brookings Papers on Economic Activity 1(125236).

Khan, H. & Santos, M. (2002). Contribution of ICT Use to Output and Labour Productivity Growth in Canada. Ottawa and Ontario: Bank of Canada.

Lithuanian Republic Law on Cyber Security/ Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428.

M. Blaze et al., "Dynamic Trust Management," Computer, vol. 42, no. 2, 2009, pp. 44–52. 10. Y. Zhang and J. Joshi, "Access Control and Trust Management for Emerging Multidomain Environments," Annals of Emerging Research in Information Assurance, Security and Privacy Services, S. Upadhyaya and R.O. Rao, eds., Emerald Group Publishing, 2009, pp. 421–452.

Measure "Procesas LT" of priority 3 "Promotion of Competitiveness of Small and Medium Enterprises" of the 2014 – 2020 European Investment Funds financing conditions/ LR Ūkio ministro įsakymas "Dėl 2014-2020 metų Europos Sąjungos fondų investicijų veiksmų programos 3 prioriteto "Smulkiojo ir vidutinio verslo konkurencingumo skatinimas" priemonės Nr. 03.3.1-LVPA-K-807 "Procesas LT" projektų finansavimo salygų aprašo Nr. 1 patvirtinimo. 2015-10-13 Nr. 4-642.

National Institute of Standards and Technology. Guide for mapping types of information and information systems to security categories, NIST 800-60, 2008.

OECD. (2003a). ICT and Economic Growth: Evidence from OECD Countries, Industries and Firms. Paris: Organization for Economic Cooperation and Development.

Oliner, S. & Sichel, D. (2000). The Resurgence of Growth in the Late 1990's: Is Information Technology the Story? Journal of Economic Perspectives, 14, 2-22.

R. Sharma and P. Yetton. The contingent effects of management support and task interdependence on successful information systems implementation. *MIS Quarterly* Vol. 27, No. 4 (Dec., 2003), pp. 533-556. Published by: Management Information Systems Research Center, University of Minnesota.

Register Centre every hour record 40,000 information security incidents/ RC kas valandą fiksuoja 40.000 informacinės saugos incidentų Viewed at 2016-10-10 <http://vz.lt/sektoriai/informacines-technologijos-telekomunikacijos/itt/2016/01/12/rckas-valanda-fiksuoja-40000-informacines-saugos-incidentu>.

Special Eurobarometer 390 Cyber security report, 2012. Viewed 2016-11-06 <http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf>.

State audit report "Cyber security environment in Lithuania"/ Valstybinio audito ataskaita "Kibernetinio saugumo aplinka Lietuvoje", 2015 m. gruodžio 9 d, Nr. VA-P-90-4-16.

Strategic Concept for the Defency and Security of The Members of the North Atlantic Treaty Organization. Adopted by Heads of State and Government in Lisbon.

T. Sommestad, H. Karlzén, J. Hallberg. A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. International Journal of Information Security and Privacy (IJISP), 2015. Volume 9, issue 1.

tions Regulatory Authority of the National electronic communications network and information security incidents investigation unit in 2014. Activity report/ Ryšių reguliavimo tarnybos Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio 2014 m. veiklos ataskaita https://www.cert.lt/statistika.html.

Thor Olavsrud, 5 information security trends that will dominate 2016.. Viewed at 2016-10-25 <http://www.cio.com/article/3016791/security/5-information-security-trends-that-will-dominate-2016.html#tk.drr_mlt> 2015

Thor Olavsrud, 9 biggest information security threats through 2018. Viewed at 2016-10-25 <http://www.cio.com/article/3046760/security/9-biggest-information-security-threats-through-2018.html#tk.drr_mlt>. 2016-03.

Threats to national security assessment/ Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos 2015 m. parengto Grėsmių nacionaliniam saugumui vertinimas, 22 psl.

Viewed at 2016-10-10 <http://www.esaugumas.lt/lt/pradzia_7.html>.

Viewed at 2016-11-04 <http://www.ekspertai.eu/vilniuje-oficialiai-atidaromas-nacionalinis-kibernetinio-saugumo-centras>.

Y. Zhang and J. Joshi, "Access Control and Trust Management for Emerging Multidomain Environments," Annals of Emerging Research in Information Assurance, Security and Privacy Services, S. Upadhyaya and R.O. Rao, eds., Emerald Group Publishing, 2009, pp 421–452

Laura Baronienė, Master's degree in management at Kaunas Technology University, Economics and Management department. Her research areas are quality management, management decisions, innovation management.

Vytautas Žirgutis, Phd is lecturer at Vytautas Magnus university, Economics and Management department. His research areas are strategic management, quality management and stakeholders management.