DIGITALIZATION AND INDUSTRY 4.0 ASPECT OF INFORMATION SECURITY

Keywords

Information security, security auditing, ISO/IEC 27001:2013

Abstract

Building security management systems is essential to protect the company's assets from losses. Such protection is essential in the dynamic development determined by digitization in Industry 4.0. In our article we analyze data from 152 information security audits performed in Czech and Slovak companies in 2019 in order to identify the most problematic areas in information security management systems. The data – audit findings – were analyzed based on the size of the audited company and the type of audit. We divided the companies into small (up to 50 employees), medium-sized and large (over 250 employees) companies. We divided the audits into four categories – initial, periodic, certification and others. The audits were performed in compliance with the ČSN EN ISO 19011 standard according to the ISO/IEC 27001: 2013 standard. The data were analyzed in MS Excel using contingency tables. The results show that the "A12" category – Operations Security – is the biggest problem for today's organizations. The "A18" category – Compliance – is another problematic area. The positive conclusion is that the shortcomings identified by the audit are not serious shortcomings that could jeopardize the companies' safe operation.

1. Introduction

The Digital Economy with its features as digitalization and Industry 4.0 has been defined as the worldwide network of economic activities enabled by information and communication technologies (ICT) (Industry, 2016). It can also be defined more simply as an economy based on digital technologies (Lin, Chiang, 2011; Hanclova at al., 2015). The whole development of the regional and global economy is closely connected with the rush penetration of ICT into the world economy and pressures the education system to prepare graduates of all levels for more complex knowledge and skills for their future jobs (Mangir, Erdogan, 2011). Nowadays, it is no longer necessary to educate people in what 4.0 trends are and what they can bring. 4.0 trends are already in

full swing in companies, at least in some partial ways, and what's more, their dynamics correspond to the overall higher pace of changes (Kuncova, Sekničkova, 2019). And it is not only about technological stimuli, but also about other demographic and climate stimuli. Therefore, the question is now how quickly these trends will penetrate into the practical life of businesses and society as a whole (Manďák, Nedomova, 2014; Kuncova, Doucek, Novotný, 2018).

Various preparedness indexes and maturity models can facilitate and speed-up companies' decision-making about where and how fast to build industry 4.0. These indexes and models show not only the companies' actual position but also the position of their competition, both at the macroeconomic and microeconomic levels. The focus thus shifts to tasks related to the implementation of necessary changes and to the specification of not only higher profits but also the main expectations associated with their implementation. For instance, achieving maximum flexibility, increasing the availability of products and services, further cost reductions, lower resources consumption and a lower impact on the environment, etc. (Basl, Doucek, 2018; Basl, Doucek, 2019).

However, the penetration and integration of ICT into economic processes also brings phenomena that their actors and participants consider negative. These include e.g. the areas of shared economy (Svecova, Veber, 2018) that clearly demonstrate that the legal aspects of the economy and businesses significantly lag behind ICT and its implementation in economic processes. Legal shortcomings lie mainly in the area of taxes and liability as well as in the processing of personal data and overall security of processed transactions.

In our article we would like to focus primarily on ensuring the security of data processed by companies. The emphasis on this area is clearly shown by European Union legislation such as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data General Data Protection Regulation (GDPR, 2016). This regulation came into force on 25 May 2018 and it has been followed up with an amendment to Czech Act No. 101/2000 of Coll., on the protection of personal data, to make sure that the Czech law is in compliance with the EU's law (Novák, Doucek 2017) and with new Czech Act No. 110/2019 of Coll., on the processing of personal data (Act č.110/2019 sb.). In addition to personal data, it is also necessary to protect other classified data that companies process and save in their information systems in order to avoid risks (Eling, Schneell, 2016). With this article, we follow up on a presentation at the IDIMT conference in 2018 and analyze data obtained from independent information security audits performed in Czech and Slovak companies in 2019. Our research questions are as follows:

RQ1: What are the main identified problematic areas (according to the ISO / IEC 27001: 2013 standard) in information security in 2019 based on the size of the audited company?

RQ2: What are the main identified problematic areas (according to the ISO / IEC 27001 standard) in information security in 2019 based on the type of audit?

2. Data Collection and Methodology

In order to find out the answer to these research questions, we had to specify the method of data collection and evaluation in two different methodological areas. The first one was data collection and the second one was the way an audit was performed in different security areas, as specified in the ISO/IEC 27001: 2013 standard.

2.1. Data collection

The data that we used for our conclusions came from the analysis of information system security audits in various industries in the Czech Republic and the Slovak Republic. Since the number of employees in the companies differed, we divided the audited companies into three categories according to the number of their employees: small companies with up to 50 employees, medium-sized companies with 50-250 employees and large companies with over 250 employees. Another criterion was the type of audit performed. The abbreviation IA means initial audit, PA means periodical audit in compliance with the general principles for management systems, RA means recertification audit and Oth. means other audits (Purcarea et al., 2011). The last type of audit was another one – Oth. In total, we used 152 different audits. Their numbers are provided in Tab. 1 (by company size) and Tab. 2 (by audit type).

Tab. 1 Data sample by company size

Company size	Number of performed audits
Small	31
Medium	36
Large	85
Total	**152**

Tab. 2 Data sample by audit type

Audit type	Number of performed audits
IA/initial audit	7
PA/periodical audit	78
RA/recertification audit	57
Oth/Other	10
Total	**152**

We also analyzed the audit findings based on the seriousness of identified irregularity. Here again, we used four categories: CAT1 – serious, CAT2 – medium, OBS – observation, OFI – opportunity. This criterion is mentioned only at the end of the article and is not used in our analysis.

2.2. Method of auditing by area

Audit definition – for the purposes of this text, an audit means a systematic, independent and documented process to obtain and objectively evaluate evidence from the audit in order to determine the extent to which the audit criteria are met (ČSN EN ISO 19011, 2019) (Kaziliunas, 2008). Audit criteria means a set of policies, procedures and requirements used as a basis against which audit evidence is compared (EN ISO 19011, 2019; Hoy, Solei, 2015).

All security audits were performed in compliance with the provisions of the applicable ISO/IEC 27001: 2013 standard and the identified non-conformities were divided according to individual areas

of the ISO/IEC 27001: 2013 (ISO/IEC 27001) standard. The numerically marked audit categories correspond to the sections of this standard as following:

- Category “4” – Context of the Organization – Understanding of the organization, its needs and expectation of interested parties and scope of the information management system.
- Category “5” – Leadership – Leadership and commitment, security policy, organizational roles, responsibilities and planning to achieve them.
- Category “6” – Planning - Action to address risks and opportunities, information security objectives and planning to achieve them.
- Category “7” – Support – Resources, competencies, awareness, communication and documented information.
- Category “8” – Operation – Operational planning and control, information security risk assessment and treatment.
- Category “9” – Performance Evaluation – Monitoring, measurement, analysis and evaluation, internal audit, management review.
- Category “10” – Improvement – Nonconformity and corrective action, continual improvement. (ISO 27001:2013).

The next categories marked with an A before the number correspond to the sections of the annex to this standard:

- Category “A05” – Information Security Policies – To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
- Category “A06” – Organization of information security – To establish a management framework to initiate the implementation and operation of information security within the organization and to ensure the security of teleworking and use of mobile devices.
- Category “A07” – Human Resource Security – To assure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered
- Category “A08” – Asset Management – Responsibility for Assets, Information Classification, Media Handling.
- Category “A09” – Access Control – Business requirements on access control, User access management, User responsibilities, System and application access control.
- Category “A10” – Cryptography – To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
- Category “A11” – Physical and Environmental Security - Secure areas, Equipment.
- Category “A12” – Operations Security - Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring, Control of operational software, Technical vulnerability management, Information system audit and consideration.
- Category “A13” – Communication Security – Network security management and information transfer.

- Category “A14” – System acquisition, development, and maintenance – Security requirements of information systems, security in development and support process and data testing.
- Category “A15” – Supplier relationships – Information security in supplier relationship and supplier service delivery management.
- Category “A16” – Information Security Incident Management - To ensure a consistent and effective approach to the management for information security incidents, including communication n security events and weaknesses.
- Category “A17” – Information security aspects of business continuity management – Information security continuity shall be embedded in the organization´s business continuity management system.
- Category “A18” – Compliance – Compliance with legal and contractual requirements, Information security review. (ISO 27001:2013).

In total, there are 21 categories (sections of the standard and its Annex A). In the following text or in the tables with results, the categories are shown in a shortened version only, i.e. either as a number only – for the categories from the text of the standard or as A and a number – for the areas listed in Annex A of the standard.

The standard statistical functions of MS Excel were used to evaluate the obtained data (Kuncova, Sekničkova 2018).

3. Results

Based on the above criteria, we evaluated the findings based on the size of the company. It is very interesting that no irregularities were identified for area “5” – Leadership – Leadership and commitment, security policy, organizational roles, responsibilities and planning to achieve them for the entire one-year period and therefore it does not appear in the evaluation of audit findings.

3.1. Evaluation by company size

First, we analyzed audit data from audits, i.e. audit irregularities by company size. The numbers of identified irregularities in audits based on the size of the company are shown in Table. 3.

Tab. 3 Audit findings by company size

	4	6	7	8	9	10	A06	A07	A08	A09	A10	A11	A12	A13	A14	A15	A16	A17	A18
1 Small	2	2	2	3	1	1			5	4			12		1	1	1	1	6
2 Medium	3	2	3	1	4		4		6	6		1	5	1	4			7	7
3 Large		10	6	1	6		2	4	8	4	1	10	13	8	1	1	6	7	10
Total	5	14	11	5	11	1	6	4	19	14	1	11	30	9	6	2	7	15	23

Table 3 shows that the biggest problems in small companies involve the “**A12**” category – **Operations Security** - Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring, Control of operational software, Technical vulnerability management, Information system audit and consideration., i.e. operations security. Smaller companies also have problems in the following areas:

- Category “A18” – Compliance – Compliance with legal and contractual requirements, Information security review.
- Category “A08” – Asset Management – Responsibility for Assets, Information Classification, Media Handling.
- Category “A09” – Access Control – Business requirements on access control, User access management, User responsibilities, System and application access control.

Medium-sized companies have the biggest problems with:

- Category “A17” – Information security aspects of business continuity management – Information security continuity shall be embedded in the organization´s business continuity management system.
- Category “A18” – Compliance – Compliance with legal and contractual requirements, Information security review.
- Category “A08” – Asset Management – Responsibility for Assets, Information Classification, Media Handling.
- Category “A09” – Access Control – Business requirements on access control, User access management, User responsibilities, System and application access control.

In the case of large companies, the biggest problem is in the “**A12**” category – **Operations Security –** Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring, Control of operational software, Technical vulnerability management, Information system audit and consideration **–** operations security. Other areas with identified problems include:

- Category “6” – Planning – Action to address risks and opportunities, information security objectives and planning to achieve them.
- Category “A11” – Physical and Environmental Security – Secure areas, Equipment.
- Category “A18” – Compliance – Compliance with legal and contractual requirements, Information security review.

When evaluating the problematic areas in terms of the number of findings in 2019, we can see the most frequent irregularities in the “**A12**” category **– Operations Security –** Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring, Control of operational software, Technical vulnerability management, Information system audit and consideration for the entire time period. We can also see a lot of irregularities in the “**A18**” category – Compliance – Compliance with legal and contractual requirements, Information security review and “A08” category – Asset Management – Responsibility for Assets, Information Classification, Media Handling. Although this area is not significant in any category, it has gradually obtained points in audits in all analyzed categories.

3.2. Evaluation by audit type

Another evaluated criterion that we used when analyzing the data identified by audits included findings broken down by audit type.

Tab. 4 Audit findings by audit type

	4	6	7	8	9	10	A06	A07	A08	A09	A10	A11	A12	A13	A14	A15	A16	A17	A18
1 IA			1		1		2		1									1	1

2 PA	2	5	5	3	7		1	2	8	8		4	17	6	4	1	6	5	15
3 RA	1	9	4	2	1	1	3	2	8	6	1	7	12	3	2	1	1	9	5
4 Oth	2		1		2				2				1						2
Total	5	14	11	5	11	1	6	4	19	14	1	11	30	9	6	2	7	15	23

Let's consider the number of performed audits based on the type of audit. We can see that there were seven initial audits during the entire year. Therefore, it makes no sense to evaluate this category because of a very small data sample. The situation is similar in the case of other types of audit. As the analysis shows, these audits focused on specific security areas and this is why auditors found irregularities.

For our analysis it makes sense to evaluate two categories – PA – periodical audit and RA – recertification audit. In the case of periodical audits, the most frequently identified irregularities were in the following areas:

- **"**A12" – Operations Security **–** Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring, Control of operational software, Technical vulnerability management, Information system audit and consideration.
- Category "A18" – Compliance **–** Compliance with legal and contractual requirements, Information security review.

The following two areas are also worth noticing:

- Category "A08" – Asset Management **–** Responsibility for Assets, Information Classification, Media Handling.
- Category "A09" – Access Control **–** Business requirements on access control, User access management, User responsibilities, System and application access control.

The most frequent irregularities in recertification audits included the following areas:

- **"**A12" – Operations Security – Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring, Control of operational software, Technical vulnerability management, Information system audit and consideration.

Other areas identified by the analysis include:

- Category "6" – Planning – Action to address risks and opportunities, information security objectives and planning to achieve them.
- Category "A17" – Information security aspects of business continuity management – Information security continuity shall be embedded in the organization´s business continuity management system.
- Category "A08" – Asset Management – Responsibility for Assets, Information Classification, Media Handling.

4. Conclusions

Based on the analysis of 152 findings of information security audits in Czech and Slovak companies in 2019, we reached the following answers to our research questions:

RQ1: What are the main identified problematic areas (according to the ISO / IEC 27001: 2013 standard) in information security in 2019 based on the size of the audited company?

Final answer:

Tab. 5 Identified problematic areas in information security by audited company size

Company size	Major problematic area	Other areas
Small	**"A12"** – Operations Security – Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring, Control of operational software, Technical vulnerability management, Information system audit and consideration.	"A18"
Medium	**"A17"** – Information security aspects of business continuity management – Information security continuity shall be embedded in the organization´s business continuity management system. **"A18"** – Compliance – Compliance with legal and contractual requirements, Information security review.	"A08", "A09"
Large	**"A12"** – Operations Security – Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring, Control of operational software, Technical vulnerability management, Information system audit and consideration.	6, "A11", "A18"

RQ2: What are the main identified problematic areas (according to the ISO / IEC 27001 standard) in information security in 2019 based on the type of audit?

Final answer:

Tab. 6 Identified problematic areas in information security by audit type

Company size	Major problematic area	Other areas
IA/initial audit	Data sample too small to make a conclusion	
PA/periodical audit	"A12" – Operations Security – Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring, Control of operational software, Technical vulnerability management, Information system audit and consideration.	"A08", "A09"
RA/recertification audit	"A12" – Operations Security – Operational procedures, responsibility, Protection form malware, Back up, Logging and monitoring, Control of operational software, Technical vulnerability management, Information system audit and consideration.	6, "A17", "A08"
Oth/Other	Data sample too small to make a conclusion	

The good thing is that no irregularities of type CAT1 or CAT2 were identified during the 2019 audits. It means that security management systems showed no major irregularities or showed irregularities of medium gravity that have no impact on the quality and reliability of the information security management system in the company. OBS – observation, OFI – opportunity is used mainly for continuous improvement and further development of the security management system in companies.

5. Acknowledgement

Paper was processed with contribution of the Czech Science Foundation project GAČR 17-02509S and with support from institutional-support fund for long-term conceptual development of science and research at the Faculty of Informatics and Statistics of the University of Economics, Prague (IP400040).

6. References

Basl, J., & Doucek, P. (2019). A Metamodel for Evaluating Enterprise Readiness in the Context of Industry 4.0. Information, 10(3). DOI: http://dx.doi.org/10.3390/info10030089

Basl, J., & Doucek, P. (2018). Metamodel of Indexes and Maturity Models for Industry 4.0 Readiness in Enterprises. 26th Interdisciplinary Information Management Talks – IDIMT 2018 Strategic Modeling in Management, Economy and Society. Linz: Trauner Verlag Universität, pp. 33–40.

ČSN EN ISO 19011:2019 Směrnice pro auditování systémů managementu. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak: 01 0330

Eling, M., & Schneell, W. (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance. 17 (5), pp. 474 - 491.

GDPR, (2016). GDPR Key Changes. Available at: http://www.eugdpr.org/key-changes.html, Retrieved: 2020_04_04.

Hanclova, J., Doucek, P., Fischer, J., & Vltavska, K. (2015). Does ICT capital affect economic growth in the EU-15 and EU-12 countries? Journal of Business Economics and Management, 16(2), pp. 387-406. DOI: 10.3846/16111699.2012.754375

Hoy, Z., Foley, A. (2015). A structured approach to integrating audits to create organizational efficiencies: ISO 9001 and ISO 27001 audits. Total Quality Management & Business Excellence, 26(5-6), pp. 690–702, DOI: 10.1080/14783363.2013.876181

Industry 4.0 (2016). Building the digital enterprise, Global Industry 4.0 survey, Price Waterhouse Coopers.

ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management system – Requirements. International Organization for Standardization.

Kaziliunas, A. (2008). Problems of Auditing Using Quality Management Systems for Sustainable Development of Organizations. Technological and Economic Development of Economy, 14(1), pp. 64-75. DOI: 10.3846/2029-0187.2008.14.64-75

Kuncova, M., Doucek, P., & Novotný, O. (2018). Penetrace ekonomických ICT služeb do ekonomiky – srovnání zemí V4. Scientific Papers of the University of Pardubice [online]. 2018, 44(3), pp. 151–162.

Kuncova, M., & Sekničkova, J. (2019). Electricity Consumption Cost for Households in the Czech Republic Based on the High and Low Tariff Rates Ratio – Optimization Model. 37th International Conference on Mathematical Methods in Economics 2019. České Budějovice: Ekonomická fakulta, Jihočeská univerzita v Českých Budějovicích, pp. 547–553.

Kuncova, M., & Sekničkova, J. (2018). Multicriteria Evaluation of the Czech Regions from the Selected Economic Activity Aspects Point of View. In: Quantitative Methods in Economic, Multiple Criteria Decision Making XIX. Bratislava: Letra Edu, 2018, pp. 193–200.

Lin, T. W., & Chiang Ch. (2011). The Impacts of Country Characteristics upon the Value of Information Technology as Measured by Productive Efficiency. International Journal of Production Economics, 132 (1), 13-33.

Manďák, J. & Nedomova, L. (2014). Measuring Performance of European ICT Sectors Using Output-Oriented DEA Models. 22th Interdisciplinary Information Management Talks – IDIMT 2014 Networking Societies – Cooperation and Conflict. Linz: Trauner Verlag universitat, pp. 79–86.

Mangir, F., & Erdogan, S. (2011). Comparison of Economic Perforamnce among Six Countries in Global Financial Crisis: The Application of Fuzzy TOPSIS Method. Economics, Management and Financial Markets, 6 (2), 122-136.

Novák, L., & Doucek, P. (2017). Regulation of Cyber Security in the Banking Sector. In IDIMT-2017 Digitalization in Management, Society and Economy, Linz: Trauner Verlag Universität, pp. 49-54.

Purcarea A.-A., Tiganoaia, B., & Petrea G. (2011). Considerations Regarding the Implementation and Certification Within an Organization of an Information Security Management System. 5th International Conference of Management and Industrial Engineering (ICMIE 2011). Editura Niculescu, Bucuresti, pp. 106-114.

Svecova, L. & Veber, J. (2018). Novelty Digitalization, Revolution, Transformation RR Innovation? 26th Interdisciplinary Information Management Talks – IDIMT 2018 Strategic Modeling in Management, Economy and Society. Linz: Trauner Verlag Universität, pp. 435–445.

Zákon č. 101/2000 Sb. ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů, In: Sbírka zákonů České republiky 2000, částka 32, 1521-1532. Available at: http://aplikace.mvcr.cz/sbirka-zakonu/ SearchResult.aspx?q=101/2000&typeLaw=zakon&what=Cislo_zakona_smlouvy

Zákon č. 110/2019 Sb., Zákon o zpracování osobních údajů. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110