Webology (ISSN: 1735-188X)
Volume 19, Number 2, 2022

Factors Causing Information Security Gaps

Sándor Dombora[1] , Pál Michelberger[2]

[1]Doctoral School of Safety and Security Sciences, Óbuda University, Budapest, Hungary.

[2]Donát Bánki Faculty of Mechanical and Safety Engineering, Óbuda University, Budapest, Hungary.

Abstract

Cyberattacks and an increasingly stringent legislative environment require organizations to effectively implement information security. Standards and legislation set the requirements, i.e., 'WHAT should be met?' to achieve the expected level of information security, but do not adequately address the question 'HOW to comply?' It is often the case that the information security management system (ISMS) meets the requirements of laws and standards, but it' rules and procedures cannot be enforced and implemented in practice. Therefore, it does not provide the necessary level of protection for the information handled by the organization. So, it became increasingly important to identify the factors that make impossible for information security to be implemented effectively in organizations.

Keywords: Information Security, Management Systems, Information Security Gaps, Information Security Problems, Problem Groups

Introduction

Authentic and up-to-date information is critical element of business processes, so security of information and information systems is playing a central role in ensuring reliable operation of business and administrative processes (Dombora & Michelberger, Információbiztonság szerepe az üzleti folyamatokban, 2016). Implementation of information security in organizations should consider all possible occurrence of information and implement a complex set of security measures that cover all employees, partners, assets, and processes, whether they are supported by an IT service or not.

Many definitions of information security exist, but the most adopted is the definition of the ISO/IEC 27001 standard (ISO, 2013). The definition is incorporated in the ISO/IEC 27000 standard, which is a common overview document for the information security management standards family, listing more than 40 standards. In my paper I adopt this definition, as all organizations subject to my research.

Information security: "preservation of confidentiality (3.10), integrity (3.36) and availability (3.7) of information" (ISO, 2018, p.: 4); **Confidentiality**: "property that information is not made available or disclosed to unauthorized individuals, entities, or processes (3.54)" (ISO, 2018, p.: 2) **Integrity**: "property of accuracy and completeness" (ISO, 2018, p.: 5); **Availability**: "property of being accessible and usable on demand by an authorized entity" (ISO, 2018, p.: 2).

Information security is often confused with IT security, which only applies to data stored in electronic information systems. Haig emphasizes the importance of information technology and IT security in military operations, including network and Internet of Things (IoT) assets (Haig, 2018). This area became important as IoT devices play an increasingly important role not only in warfare but also in industry (Smit et al., 2016) and private sector too.

Another concept that overlaps with information security is cybersecurity. Organizations are using this concept, but its meaning is not clearly defined. Kovács defines the concept of cybersecurity, in a way that it includes information security (Kovács, 2018). From my point of view, information security is a broader concept as it covers all occurrences and manifestation of information, though when we are talking about information security, we cover the cybersecurity too. Looking at the challenges of information security we see that cyberattacks are a common way of hacker groups to penetrate corporate networks and steal electronically stored confidential or secret information. One way to improve cybersecurity and through it the information security is addressing the vulnerabilities of information systems (Sharkasi, 2015).

Nowadays, impersonation is a common source of threat. Before committing impersonation perpetrators steal or buy personal data from black hat hackers. To steal personal data hackers are targeting organizations and achieve easy success mainly in organizations which have information and IT security gaps. Therefore, the security of personal data is increasingly emphasized both by global and local legislation, and so an organization which does not do everything in its power to protect personal data can be subject to large fines (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016). To support data protection ENISA published a study on building IT security based on design (Danezis et al., 2014).

It is clear, therefore, that it is not enough to develop a legislation and standards compliant ISMS, but its requirements must be feasible and enforceable in practice.

Although the continuous improvement of standards and legislation are helping organizations planning their information security and implementing security controls, more and more information security incidents are revealed which affect thousands or even millions of data records causing damage to organizations, partners, and customers. This led to the conclusion that the ISMS developed by organizations and the implemented information security are inefficient.

Background

International organizations in the domain of information security regularly conduct surveys and publish their results. These surveys usually focus on the compliance of ISMS with the standards and legislation. A good example of this is the ISACA Budapest Chapter's regular survey entitled "Information Security Situation" (ISACA Budapest Chapter, 2011; 2012; 2015; 2017; 2019) which gathers information and builds statistics on the compliance with the regulatory, organizational, and general requirements of the information security standards. The European Agency for Cybersecurity also publishes a threat landscape (ENISA, 2021), which covers mainly technology-based risks. On the other hand, well known information security consulting firms conduct their own surveys, covering special IT security topics (Symantec, 2019; SOPHOS, 2020; CISCO, 2021) such as malware protection, intrusion detection, network segmentation, remote access, cyber intelligence etc. If we look at these surveys and we try to combine them, they are assessing information security policies and procedures and cover different focused areas which are critical regarding information security independently. They do not cover adequately the implementation, operation, interaction, and effectiveness of controls required by ISMS policies. On the other hand, we know that information security is as strong as its weakest point is. It is enough to have one weak point to become vulnerable to attacks and misuse. Therefore, even if we combine the result of these surveys it might lead to partial result and does not reflect the state of information security leading to false security awareness. To get a real picture of the state of information security, it is not enough to examine only the existence of policies and individual measures, but it is also worth asking about their feasibility operation, interaction, effectiveness. Because the answers to these questions reveal the real state of information security, organizations might not respond or give evasive answers. To learn about the information security status of an organization we must assess the main issues on information security:

- What prevents organizations complying with information security policies?
- To what extent do information security policies help or hinder work in your organization?
- What changes are needed to prevent employees from circumventing information security policies to speed up work?

To achieve the level of information security required by the needs and legal environment the ISMS - policies and procedures - must adhere to the infrastructure and economic capabilities of the organizations. The requirements and processes must be feasible, their implementation must lead to security measures that facilitate the smooth operation of business and operation processes while providing the required level of information security.

Methodology

Disclosure of the security level achieved by the implemented security measures may impact the judgement of organizations. Information security surveys and statistics are often inaccurate because organizations do not answer all the questions or provide unreliable answers. The most common causes of inadequate or unreliable answers are that organizations seek to demonstrate

that their implemented information security measures protect the data professionally. On the other hand, depending on the size of sampling the organizations can be identified even if their parameters are anonymized.

To be able to appropriately examine the implemented information security and the impact of ISMS on the organization, it is necessary to learn its structure and operation.

The only possible way to learn more about the effectiveness of the information security implementation in the examined organization, is to select a methodology that provides detailed information about the developed solutions and their quality. This can be achieved through active participation in information security related projects. Action research (Reason & Bradbury, 2001) is a method, which provides a good framework for joint application of different qualitative research techniques and aims to contribute positively to both people's real problems in an immediate problematic situation and social science within a mutually acceptable ethical framework (Lewin, 1946). Information collected and analyzed during the project execution, results in a case study, i.e., a description of a unique, interesting, or special thing (Yin, 1984). The data obtained and case studies developed during the research projects on the implementation and problems of information security is sensitive. To protect the interests of organizations and maintain confidentiality, work can only be done according to non-disclosure agreements. Therefore, I exclude the use of statistical methods performed on a large sample. In the case studies I prepared for the organizations participating in the research I analyzed the impact of ISMS on the business and operation processes, examined the factors obstructing the achievement of the necessary information security level. I used my theoretic results in my research projects on analysis and implementation of information security (Dombora, 2015) to assess the quality and level of information security achieved. I developed generic problems using Grounded Theory research method developed by Glaser and Strauss (Glaser & Strauss, 1967), in which I incorporated the knowledge mapping (Dörfler & Velencei, 1999) and concept mapping techniques (Baracskai et al., 2008). I explored the reasons for their occurrence based on the information collected in the interviews and incorporated into the case studies.

To protect the interests of the participating organizations, sensitive information obtained and incorporated in case studies of the research projects remain confidential and cannot be disclosed. When I mention the projects, I use generic acronyms for organizations. The only link to their identity is the size, which is not enough to identify them. I enrolled the organizations into three categories: small with less than 100 employees, medium with 101-500 employees and large with more than 501 employees. When I give the context of the research projects, I mention the economic sectors covered without linking to the organizations, just to show that the same information security problems are affecting them. When I present the occurrence of generic problems, only the acronym and size of the organization is listed.

I assessed the information security of nine organizations in twelve projects of which seven were Information Security Management System development and review projects (ISMSP) and five related to Information System Security Requirement development and review projects (ISSRP). The organizations involved in the projects are active in the fields of public administration, services, manufacturing, and finance.

The execution of ISMS projects started with an assessment of the current state of information security. In the ISMS projects compliance with ISO/IEC 27001 standard (ISO, 2013), data protection (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016) and information security (2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 2013) legislation had to be achieved, with incorporation of sector-specific information security requirements. This covered the entire regulatory map and relevant standards. Subsequently, I prepared a case study presenting the in detail the status of the legal compliance at the beginning of the project. The presentation of the compliance assessment covered the requirements missing from the policies and standards of the organization, and the protection measures which were included, but were not implemented in practice.

In case of Information System Security Requirement projects security requirements specification for an IT system had to be developed or evaluated against the ISMS and in its absence to the applicable laws and standards. In these cases, I reviewed and analyzed the business requirements and high-level design of the IT system, the ISMS and legal background of the target system, to which the security requirements had to be adjusted or checked.

The research projects are summarized in Table 1. Because the information is sensitive, the table contains the generic acronyms of the organizations, the size of the organization, the project type, the key information security requirements, and the realization of the ISMS requirements at the time the project was launched. Table column headers are: Organization: generic acronym of the organization; Size: size of the organization: small, medium, large; Project: type of project; LC: compliance with information security legislation is required, ISO 27001: operation in accordance with the standard is required, GDPR: compliance with data protection laws including GDPR is required; ISMS: whether the organization has an ISMS at the beginning of the project; IS Realized: the existing ISMS requirements are met or not.

Organization	Org. Size	Project	LC	ISO 27001	GDPR	ISMS	IS Realized
O1	medium	ISMSP	Yes	No	Yes	Yes	No
O2	medium	ISMSP	Yes	Yes	Yes	Yes	No
O3	medium	ISMSP	Yes	No	Yes	No	No
O4	small	ISMSP	Yes	No	No	Yes	No
O5	large	ISMSP	Yes	No	Yes	Yes	No
O6	large	ISMSP	No	Yes	Yes	Yes	Yes
O7	large	ISMSP	No	Yes	Yes	Yes	No
O8	small	ISSRP	Yes	No	No	No	No
O9	medium	ISSRP	Yes	No	No	Yes	No
O4	small	ISSRP	Yes	No	No	Yes	No
O7	large	ISSRP	No	Yes	Yes	Yes	No
O3	medium	ISSRP	Yes	No	Yes	No	No

1. Table Information security projects (self-editing)

Results

Analyzing the case studies prepared for the organizations in these projects, I collected the problems and gaps related to ISMS, which I summarized in Table 2. I did not list separately the recurring problems and shortcomings in the different projects. So, the numbers in the first column do not indicate a priority order, they only reflect the number of deficiencies collected. Definitions of generic information security problems are summarized in Table 2.

#	Security problems and gaps
1.	References to non-existing policies, standards and procedures.
2.	References to higher level policies and standards are missing.
3.	Correlation between policies, standards and procedures is missing.
4.	The Information Security Policy (ISP) which should contain only general rules for all employees, contains additional rules related to only certain roles, unauthorized access of which raises security issues.
5.	The ISP contains several rules that are irrelevant to all employees.
6.	Security rules and procedures are not assigned to organization roles.
7.	It is not clear which rules apply to which role.
8.	The ISP contains general methodology (development, operation, risk analysis, etc.) descriptions instead of referring to them.
9.	The ISP is too long, consisting of hundreds of pages, with irrelevant content incorporated.
10.	ISMS does not have a documented structure, the references between policies, standards and procedures is inconsistent.
11.	Missing glossary.
12.	The concepts are redefined in each document, in certain cases with completely different description.
13.	Wording of the ISMS policies, standards and procedures is incomprehensible to most of the employees.
14.	Some policies are too long, take a long time to read, and those involved do not remember their contents.
15.	ISMS policies use abbreviations and professional terminology that are incomprehensible to those involved.
16.	ISMS policies use many undefined foreign terms.
17.	ISMS policies are not consistent with the organization's operational and legal environment.
18.	The ISMS based on legislation is too general.
19.	Policies, standards, and procedures of the ISMS are modified versions of applicable laws or standards. They remain theoretical and are not implemented in organizational workflows. They state but do not provide the necessary protection.

#	Security problems and gaps
20.	It is difficult to link ISMS rules and requirements to the related points of the laws or standards.
21.	The ISMS contains contradictory rules and requirements.
22.	If employees adhere to the rules of ISMS, it hinders them in performing their daily tasks.
23.	The conditions for the implementation of the ISMS (environmental, technical, economic, etc.) are not met.
24.	ISMS is not appropriate for the operating environment: the rules are too strong, incomplete, or irrelevant.
25.	ISMS based on legal environment is too general. It contains high level requirements. Stakeholders do not recognize the tasks they have to perform.
26.	ISMS rules conflict with business process execution rules.
27.	The ISMS includes an IT and information security risk analysis policy that overlaps with the organization's risk analysis policy.
28.	The ISMS contains the Information Security Incident Management Policy, which overlaps with the IT Incident Management Policy.

2. Table Discovered ISMS problems (own editing)

Going from project to project during the research, I explored the factors hindering the successful implementation of the information security system. Table 2 illustrates that I discovered several similar or related problems and deficiencies. I collected, analyzed, and generalized the problems that occurred in organizations. In each project, I examined the occurrence of the previously identified and defined general problems, which are listed in Table 3.

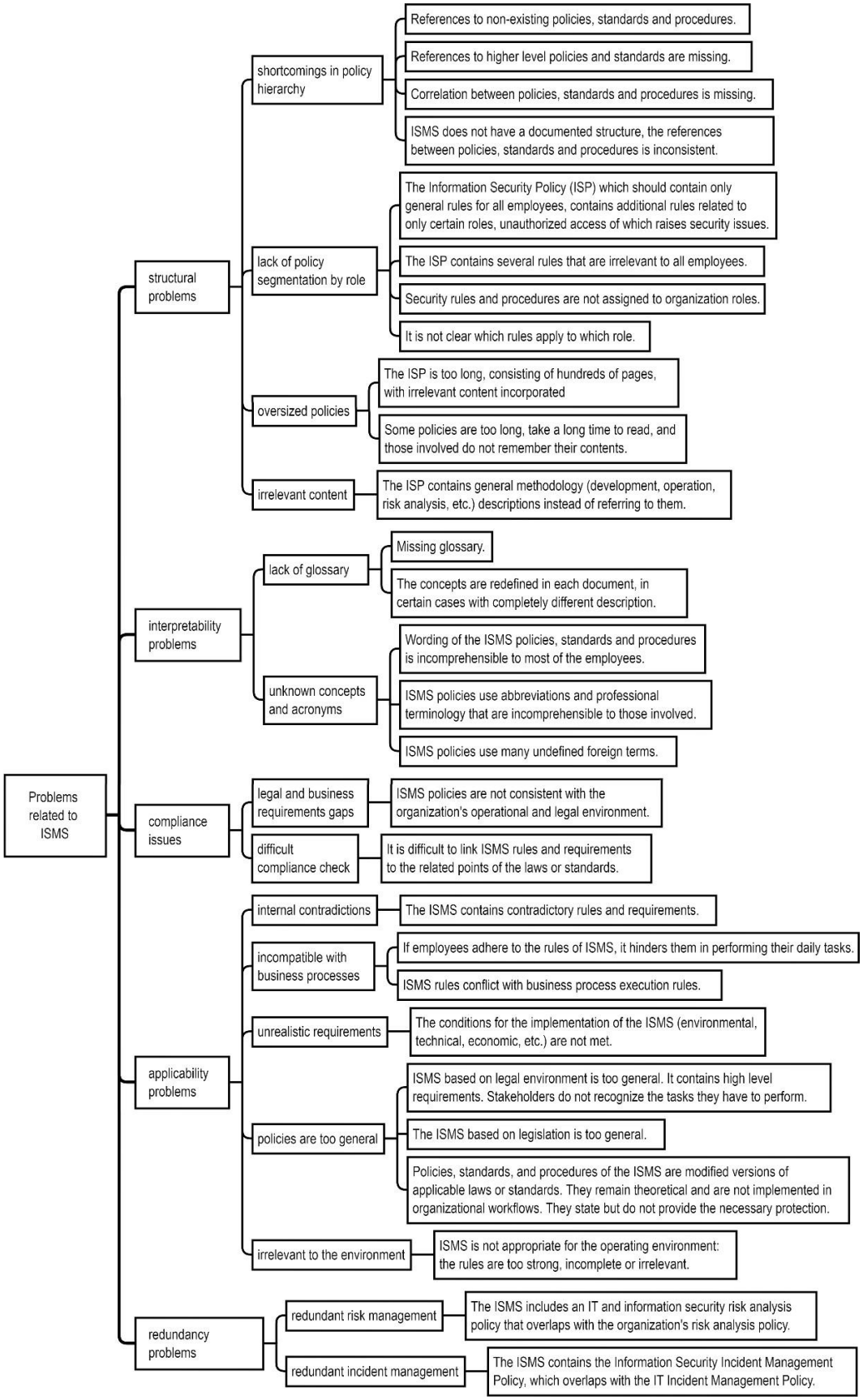
During my research, I constantly reviewed and clarified the definitions of generic problems. I linked the newly discovered problems to the generic ones trying to saturate them (Kucsera, 2008).

#	Generic problem	Generic problem definition
1.	shortcomings in policy hierarchy	ISMS has no documented structure. The system of contexts and interdependence of regulations is not defined.
2.	lack of policy segmentation by role	The scope of policies and standards do not adhere to the organization roles.
3.	oversized policies	The ISMS policies and standards are too long, consisting of hundreds of pages.
4.	irrelevant content	The ISMS contains general methodology (development, operation, risk analysis, etc.) descriptions instead of referring to them.

#	Generic problem	Generic problem definition
5.	lack of glossary	Lack of a standardized concepts and acronyms spanning across the entire ISMS.
6.	unknown concepts and acronyms	ISMS is difficult to read due to use of technical concepts, foreign terms, and acronyms.
7.	oversized regulations	Some regulations are too long, take a long time to read, and affected employees do not remember their contents.
8.	legal and business requirements gaps	ISMS policies and standards do not adhere to the business expectations and legal environment of the organization.
9.	difficult compliance check	The ISMS rules and requirements do not refer to law and standard requirements.
10.	internal contradictions	The ISMS policies, standards and procedures contain conflicting rules.
11.	incompatible with business processes	ISMS rules and requirements conflict with business process execution. Adherence to certain requirements of the ISMS prevents or makes it impossible to work.
12.	unrealistic requirements	The conditions for the implementation of ISMS (environmental, technical, economic, etc.) are not available in the organization, typically the organizational culture and financial resources.
13.	policies are too general	ISMS based on legal environment is too general. It contains high level requirements. Stakeholders do not recognize the tasks they have to perform.
14.	irrelevant to the environment	ISMS is not appropriate for the operating environment: the rules are too strong, incomplete, or irrelevant.
15.	redundant risk management	The ISMS includes an IT and information security risk analysis policy that overlaps with the organization's risk analysis policy.
16.	redundant incident management	The ISMS contains the Information Security Incident Management Policy, which overlaps with the IT Incident Management Policy.

3. Table Generic problems

In the research projects, I also examined the causes of the problems, which helped me to group the defined generic problems. I defined a three-layer hierarchy. At the lowest level are the problems and security gaps identified, which I assigned to the generic problems at the second level. Then the general problems were categorized into groups at the third level according to their characteristics and causes of occurrence. The complete hierarchy is presented in Figure 1.



1. Figure Problems, generic problems, problem groups and their relationship (own editing)

The definition of the problem groups is listed in Table 4.

Problem group	Definition
structural problems	I define the structural problem as any shortcomings in the structure and design of ISMS. This includes deficiencies in the hierarchy, context, assignment of policies, standards and procedures to roles, reference of policies, as well as irrelevant content and oversizing.
interpretability problems	I refer to any factor that affects the understanding of the regulations as a problem of interpretability. In summary, this means that the target audience does not understand the requirements set out in the regulations. These include unknown abbreviations and terms, jargon, and incomprehensible large circular sentences.
compliance issues	Problems in meeting the requirements of legislation and standard requirements relevant to the organization.
applicability problems	Problems regarding compliance, enforcement, and implementation of policy requirements. These include internal inconsistencies in ISMS, incompatibility with business rules, hindering workflow executions, problems in assigning tasks to responsible, unrealistic expectations regarding security measures.
redundancy problems	ISMS requires definition and implementation of workflows which already have an alternative implementation that is required by other organizational-level policies.

4. Table Problem groups (own editing)

Meanwhile I generalized the problems and deficiencies identified; I tracked their occurrence in the affected organizations. The occurrence of generic problems in the studied organizations is presented in Table 4.

Generic Problem	O1	O2	O3	O4	O5	O6	O7	O8	O9
Structural problems									
shortcomings in policy hierarchy	Yes	No	N/A	Yes	Yes	Yes	Yes	N/A	Yes
lack of policy segmentation by role	No	Yes	N/A	Yes	Yes	No	Yes	N/A	Yes
oversized policies	No	No	N/A	No	Yes	No	No	N/A	No
irrelevant content	No	No	N/A	No	Yes	No	No	N/A	No
Interpretability problems									
lack of glossary	No	No	N/A	Yes	Yes	No	Yes	N/A	Yes
unknown concepts and acronyms	Yes	Yes	N/A	No	Yes	Yes	No	N/A	Yes
Compliance issues									
legal and business requirements gaps	Yes	Yes	N/A	Yes	Yes	No	Yes	N/A	Yes
difficult compliance check	Yes	No	N/A	Yes	Yes	Yes	Yes	N/A	Yes

Generic Problem	O1	O2	O3	O4	O5	O6	O7	O8	O9
Applicability problems									
internal contradictions	Yes	No	N/A	No	Yes	No	No	N/A	No
incompatible with business processes	Yes	Yes	N/A	Yes	Yes	Yes	Yes	N/A	Yes
unrealistic requirements	Yes	Yes	N/A	No	Yes	No	No	N/A	Yes
policies are too general	No	Yes	N/A	Yes	Yes	No	Yes	N/A	Yes
irrelevant to the environment	No	No	N/A	No	Yes	No	No	N/A	Yes
Redundancy problems									
redundant risk management	Yes	Yes	N/A	Yes	Yes	Yes	Yes	N/A	Yes
redundant incident management	Yes	Yes	N/A	Yes	Yes	Yes	Yes	N/A	Yes

5. Table Incidence of generic information security problems in the examined organizations (own editing)

In Table 6 I summarized the occurrence of the generic problems and problem groups by organization size. Only organizations with ISMS implemented (seven out of nine) at the start of the project are included in the table.

Problem group / Generic Problem	Small	Medium	Large	Total
Structural problems	***1***	***3***	***3***	***7***
shortcomings in policy hierarchy	*1*	*2*	*3*	*6*
lack of policy segmentation by role	*1*	*2*	*2*	*5*
oversized policies	0	0	1	1
irrelevant content	0	0	1	1
Interpretability problems	***1***	***3***	***3***	***7***
lack of glossary	1	1	2	4
unknown concepts and acronyms	*0*	*3*	*2*	*5*
Compliance issues	***1***	***3***	***3***	***7***
legal and business requirements gaps	*1*	*3*	*2*	*6*
difficult compliance check	*1*	*2*	*3*	*6*
Applicability problems	***1***	***3***	***3***	***7***
internal contradictions	0	1	1	2
incompatible with business processes	*1*	*3*	*3*	*7*
unrealistic requirements	0	3	1	4
policies are too general	*1*	*2*	*2*	*5*
irrelevant to the environment	0	1	1	2
Redundancy problems	***1***	***3***	***3***	***7***
redundant risk management	*1*	*3*	*3*	*7*
redundant incident management	*1*	*3*	*3*	*7*

6. Table Statistics of generic ISMS problem incidence organization size (own editing)

The statistics provide information on the distribution of the occurrence of generic problems and problem group in the examined small, medium, and large organizations. I noted that all generic problems of each problem group occur in at least in one of the small, medium, and large organizations. Furthermore, I concluded that all problem groups occur in each organization examined, so I can state that all problem groups affect all organizations involved in research projects indifferent of their size and area of interests.

I marked with italics the lines in the table, which cover generic problems which affect at least five of the seven organizations examined. These are shortcomings in policy hierarchy, lack of policy segmentation by role, unknown concepts and acronyms, legal and business requirements gaps, difficult compliance check, incompatible with business processes, policies are too general and redundant incident and risk management problems, which affect all examined organizations with the exceptions of one or two.

Discussion

During the research of information security problems, I became aware that development of a compliant ISMS with the legislation and relevant standards, and its implementation to achieve information security are two different things. Organizations follow laws and standards to create a compliant ISMS with the regulatory environment, but usually there are significant gaps in its implementation. Identifying the problems of information security provides an opportunity to address them. However, to find an effective way to eliminate the identified problems, I had to go deeper and gather information on their root causes. I started the research with exploring the theoretical background of information security risk management and development of ISMS. Assessing and managing information security risks plays an important role in achieving the needed security level. Jakus and Tick emphasize that when discussing security awareness and corporate IT responsibility which play key role in reducing IT risks such that information risks (Jakus & Tick, 2017). I tried to look-up publications that present studies of effective ISMS. I found articles on development (Calder, 2009; Dey, 2007), but only a few discussed the quality of ISMS too. Nassar not only identifies the shortcomings of ISMS, but also examines the level of maturity of the ISMS according to ISO/IEC 27001 standard based on the COBIT maturity model (Nassar, 2017). The presented gap analysis looks at the implementation of information security from a regulatory point of view, unfortunately it does not cover the examination of the implementation of controls and the quality of implementation in practice. I consider this important because the result of my research shows that most of the problems are caused by common mistakes committed during the development of the ISMS. These problems do not affect the compliance with the legislation, but rather the quality of policies, standards and procedures which cause problems during the implementation phase or in the execution of required information security measures.

Conclusion

I identified and generalized the information security deficiencies in the examined organizations. I found that these problems can be classified into structural, interpretability, compliance,

applicability, and redundancy groups. At first sight, these are related to the implementation in practice of the security measures required by ISMS and seem to be applicability issues. The statistics on the occurrence of information security problems shows that all problems groups are present in all examined organizations regardless of their size and activity. Examining their root causes leaded to the conclusion that these are symptoms caused by mistakes made during the development of the ISMS. This raises the question whether solving these problems can be done by building an ISMS development methodology.

References

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. (2013).

Baracskai, Z., Dörfler, V., & Velencei, J. (2008). Concept Mapping and Expert Systems: Exploring Synergies., 3, pp. 70-74.

Calder, A. (2009). Implementing Information Security Based on ISO 27001/ISO 27002 (2 ed.). Zaltbommer, Netherlands: Van Haren Publishing.

CISCO. (2021). Securing Outcome. CISCO. Retrieved 12 17, 2021, from https://www.cisco.com/c/dam/en/us/products/collateral/security/security-outcomes-study-vol-2-report.pdf?ccid=cc000160&oid=rptsc027923&dtid=odicdc001478

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R., & Schiffner, S. (2014). Privacy and Data Protection by Design. ENISA. doi:DOI 10.2824/38623

Dey, M. (2007). Information Security Management – A Practical Approach. Proceedings of AFRICON (p. 6). IEEE. doi:10.1109/AFRCON.2007.4401528

Dombora, S. (2015). Szervezetek információbiztonságának elemzése és fejlesztése. In Z. Rajnai, B. Fregan, Z. Marosné Kuna, & J. Ozsváth (Eds.), Tanulmánykötet a 6. Báthory-Brassai nemzetközi konferencia előadásaiból (Vol. 1, pp. 365-382). Budapest: Óbudai Egyetem.

Dombora, S., & Michelberger, P. (2016). Információbiztonság szerepe az üzleti folyamatokban. International Journal of Engineering and Management Sciences, 1(1), 1-13. doi:10.21791/IJEMS.2016.1.17

Dörfler, V., & Velencei, J. (1999). Tudásrendezés. Gazdaság vállalkozás, vezetés: A szervezési és vezetési tudományos társaság lapja, 3(4), 64-73.

ENISA. (2021). ENISA Threat Landscape 2021. ENISA. doi:10.2824/324797

Glaser, B. G., & Strauss, A. L. (1967). The Discovery of Grounded Theory: Strategies for Qualitative Research. Chicago: Aldine.

Haig, Z. (2018). Információs műveletek a kibertérben. Budapest: Dialóg Campus Kiadó.

ISACA Budapest Chapter. (2011). Információbiztonsági helyzetkép 2011. Budapest. Retrieved 06 20, 2015, from https://higherlogicdownload.s3.amazonaws.com/ISACA/a33a1b3f-fd2b-4dc7-a080-308f6288e925/UploadedImages/Informaciobiztonsagi_helyzetkep/ISACA_Infobizt_helyzetkep_2011.pdf

ISACA Budapest Chapter. (2012). Információbiztonsági helyzetkép 2012. Budapest. Retrieved 06 20, 2015, from https://higherlogicdownload.s3.amazonaws.com/ISACA/a33a1b3f-fd2b-4dc7-a080-308f6288e925/UploadedImages/Informaciobiztonsagi_helyzetkep/ISACA_Infobizt_helyzetkep_2012.pdf

ISACA Budapest Chapter. (2015). Információbiztonsági helyzetkép 2015. Budapest. Retrieved 01 25, 2016, from https://higherlogicdownload.s3.amazonaws.com/ISACA/a33a1b3f-fd2b-4dc7-a080-308f6288e925/UploadedImages/Informaciobiztonsagi_helyzetkep/ISACA_Infobizt_helyzetkep_2015.pdf

ISACA Budapest Chapter. (2017). Információbiztonsági helyzetkép 2017. Budapest. Retrieved 03 16, 2018, from https://higherlogicdownload.s3.amazonaws.com/ISACA/a33a1b3f-fd2b-4dc7-a080-308f6288e925/UploadedImages/Informaciobiztonsagi_helyzetkep/ISACA_Infobizt_helyzetkep_2017.pdf

ISACA Budapest Chapter. (2019). Információbiztonsági helyzetkép 2019. Budapest. Retrieved 12 28, 2019, from https://higherlogicdownload.s3.amazonaws.com/ISACA/a33a1b3f-fd2b-4dc7-a080-308f6288e925/UploadedImages/Informaciobiztonsagi_helyzetkep/ISACA_Infobizt_helyzetkep_2019.pdf

ISO. (2013). ISO/IEC 27001:2013, Information technology Security techniques - Information security management systems – Requirements. ISO.

ISO. (2018). ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary (5 ed.). Switzerland: ISO.

Jakus, A., & Tick, A. (2017). IT biztonsági kockázatok és kockázatkezelés. Hadmérnök, 1(XII. évfolyam 1.), 182-202. Retrieved 10 15, 2017, from http://hadmernok.hu/171_15_jakus.pdf

Joint Task Force Transformation Initiative. (2015). NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations (2 ed.). Gaithersburg, MD: NIST. doi:10.6028/NIST.SP.800-53r4

Kovács, L. (2018). A kibertér védelme. Dialóg Campus Kiadó.

Kucsera, C. (2008). Megalapozott elmélet: Egy módszertan fejlődéstörténete. Szociológiai Szemle, 3, 92-18. Retrieved 07 20, 2018, from https://szociologia.hu/dynamic/SzocSzemle_2008_3_092_108_KucsereCs.pdf

Lewin, K. (1946). Action Research and Minority Problems. Journal of Social Issues, 2(4), 34-46. doi:10.1111/j.1540-4560.1946.tb02295.x

Nassar, A. A. (2017, December). Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen. International Journal of Scientific Research in Multidisciplinary Studies, 3(11), 4-13. doi:10.26438/ijsrms/v3i11.413

Reason, P., & Bradbury, H. (2001). Handbook of Action Research. Thousand Oaks, CA.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. (2016).

Sharkasi, O. Y. (2015). Addressing Cybersecurity Vulnerabilities. ISACA Journal, 5, 1-11. Retrieved 10 39, 2015, from https://www.isaca.org/resources/isaca-journal/issues/2015/volume-5/addressing-cybersecurity-vulnerabilities

Smit, J., Kreutzer, S., Moeller, C., & Carlberg, M. (2016). Industry 4.0. European Parliament Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Brussels.

SOPHOS. (2020). SOPHOS 2021 Threat Report. SOPHOS. Retrieved 05 01, 2021, from https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf

Symantec. (2019). Internet Security Threat Report. Symantec. Retrieved 05 13, 2020, from https://docs.broadcom.com/doc/internet-security-threat-report-volume-24-en

Yin, R. K. (1984). Case study research. Beverly Hills, California: Sage Publications.