


The Information Security Management Systems in E-Business

Vladimír Bolek, University of Economics in Bratislava, Slovakia*

 <https://orcid.org/0000-0003-1144-278X>

Anita Romanová, University of Economics in Bratislava, Slovakia

František Korček, University of Economics in Bratislava, Slovakia

ABSTRACT

Enterprises trading on the electronic markets are exposed to security risks due to the active use of ICT in several transformation process activities. Realized risks cause particular damage to the enterprises that lack ISMS (information security management systems) or a basic process approach to IS management. In this article, the authors identify similarities and differences in information security management models from various aspects. The scientific article compares the presented models, their essence, goal, focus, and starting points. Based on advantages and disadvantages, the authors evaluate the possibilities of applying models in electronic business, which determines which models can be applied to all processes or only to specific processes of e-business. The representative data set was obtained from a sample of e-commerce enterprises using the Slovak electronic market. Research hypotheses based on scientific assumptions and statistical analysis are verified. The research conclusions provide an insight into practice of ISMS and an information security management system in e-commerce.

KEYWORDS

E-Business, E-Commerce, Information Security, Information Security Management Systems, IT Management

INTRODUCTION

Every year, the use of the internet increases substantially. The accessibility of affordable mobile devices and the expansion of the internet have become key factors (Yazdanifard, Edres & Seyedi, 2011). E-business is growing proportionately with the expansion of the internet, and new electronic markets emerge wherever the internet is available. E-business and e-commerce are connected to the online world and online transactions. In their study, Hazarika and Mousavi (2022) emphasize that all online transactions are closely related to the risk of a cyber attack. That E-business is on the rise is also supported by data from the European Union's statistical office, Eurostat, and the reports from countries such as China and the USA, whose turnovers from electronic sales of goods and services increase annually. Considering that e-commerce offers many benefits, the ratio of e-commerce sales

DOI: 10.4018/JGIM.316833

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

to the total sales is likely to continue to increase in the coming years (Ahluwalia & Merhi, 2020). Development in Slovakia attests to this upward trend, and in the next few years is expected to reach a total turnover of 1 billion euros from electronic sales of goods and services. The gradual informatization of the society (e.g., e-government, e-health) and the annual increase in the numbers of e-commerce indicate that the development of e-business in Slovakia will continue. The interactivity and openness of Internet-based e-commerce technology in inter organization data transmission have a very important impact on enterprise management practice (Sun & Wang, 2021).

However, such advancement will not be possible unless enterprises adhere to the basic dimensions of information security (IS) and create a safe environment for their information assets. The main reason for a potential bankruptcy is a customer because they are sensitive to security incidents involving e-shops. Every untreated and executed risk leads to the immediate loss of a large number of customers and possibly to existential problems. In the current era of countless security threats and offensive methods and techniques, businesses cannot afford to ignore internet security. Every company should have a clear idea what and why to solve in the field of security. This knowledge enables the organization to focus its security activities and resources where they are needed. It means, the organization is able to invest in areas that are really critical and does not waste funds and efforts by solving marginal problems. In this regard, importance of risk analysis, which is often considered a formality required by some standards or legislation, seems to be often underestimated. However, just the risk analysis is an important tool for the organization to be able to determine and separate critical areas (processes, systems) from areas to which it does not need to pay too much attention at that moment. Taking into account the value of assets, criticality of risks, costs of implementing the measure and its time-consuming nature, the organization can decide how to deal with an identified risk (remove the risk, reduce the risk to an acceptable level or accept the risk) and can create a realistic plan for the implementation of security measures in a certain time period. By this means the organization can determine exactly what and why wants to achieve it. It is possible to eliminate (often occurring in practice) spending of funds and resources for non-systemic measures. In the field of information security, there are several standards that contain recommendations and description of good practice, how to manage information security and what security measures to implement in the organization. We claim that the right path for businesses is to apply a procedural approach to information security management systems (ISMS) that guarantees adequate information security of e-businesses by minimizing consequences of risk with appropriate security measures at an acceptable cost. Any data leakage and breach of information security could damage the organization's reputation. Whereas clients, customers come and leave based on how much they trust a particular seller, business can fall apart if customers decide not to do trade with it. To prevent this, for enterprises it is necessary to ensure security and integrity of customer and company information. This is recommended for both: small and large enterprises. Setting up ISMS is a must.

ISMS of e-commerce is a necessary process that determines health and sustainability of an enterprise (Ji & Zou, 2016). Increasing cybercrime, its simplification, and accessibility to incompetent ICT users actively attack information assets of e-commerce businesses. However, it also forces them to apply proactive and reactive technical and organizational measures that ultimately lead to ISMS implementation.

E-commerce has connected buyers and sellers around the world more than ever before; online trading can be quite convenient, easy to manage and productive, but it creates conditions for security risks. For e-business and commerce it is very important to have adequate security measures to protect a business activity, because cyber attacks can occur where and when the business management least expects it and this situation can affect buyers. Consequences for the company can be liquidating. The market for hardware and software products offers a wide range of security options and their sophistication is increasing, but cyber-attacks are also becoming more sophisticated.

This scientific paper consists of several consecutive parts. The theoretical background provides an overview of the current state of e-commerce, focusing on e-commerce security, information

security management, and compares selected models of information security management. The main goal of this scientific article is to identify the impact of costs spent on information security on the level of information security perceived by enterprises based on examination of the level of information security enterprises' management with electronic commerce and determination of the costs spent on ensuring information security. The main goal is supported by several partial goals: to analyze, compare and create a synthesis of theoretical starting points of information security management with a focus on electronic business in domestic and foreign environment; analyze and compare selected information security management models; identify and evaluate the current status of information security management level of e-commerce enterprises based on available knowledge, research studies and own survey. The originality and novelty lie in a research problem choice. So far, no similar research focused on the information security of electronic commerce, has been carried out in the Slovak Republic, because enterprises do not like to provide such sensitive data. Therefore, implementation of the research required extensive efforts of authors and was time-consuming. There is also the originality in the issue and examination of relationship between costs spent on information security and perception of information security by enterprises. Some businesses are not even aware of this relationship and its importance. The Data and Methodology sections present the research model, research assumptions and hypotheses, the research tools, and the data set format. The central part, Results, consists of realized research outcomes and the verification of research hypotheses and main findings. The research results and conclusions provide new findings not only for academics, but also for business practice and management of e-commerce businesses. The Discussion section presents the research's main findings in line with the theoretical background and studies carried out by other authors. At the end of discussion, he also points out that from a global perspective, it is necessary to educate employees in companies setting of management processes and application of ISMS process approach. Employees and their behavior are often the weakest element of IT security. Applying IT security management system in companies is one of ways how to increase IT security level of companies with e-commerce. The research limits are also listed in this segment.

THEORETICAL BACKGROUND

The hierarchically highest level for business ventures utilizing ICT is the electronic business (e-business), whose activities are connected with business and production activities and the activities that support, integrate, and manage both groups to provide services to customers. Electronic business refers to "intra-company and inter-company processes and transactions between suppliers, customers, companies and business teams with a minimum number of intermediate links and with business, work processes and business interactions carried out electronically. It is a basic prerequisite for a successful enterprise in a newly emerging, globally interconnected and efficient business environment on the internet." According to Rous (2014), it is a conduct of business processes on the internet. These electronic processes include buying and selling goods and services, servicing customers, processing payments, managing production control, collaborating with business partners, sharing information, running automated employee services, recruiting. Authors Laudon and Traver (2014) claim that e-business digitally enables transactions and processes within the enterprise, including information systems under the enterprises' control.

E-business is conducted in the electronic market space, an internet business platform for buyers and sellers exchanging goods and services (Cheng, Chan & Lin, 2006). Due to the high level of competition in traditional markets, many start-ups as well as established businesses enter the electronic environment and reach new markets through online sales activities, ultimately increasing their sales (Wiradinata, 2017). The e-market is an online environment that opens up additional business opportunities for entrepreneurs (such as better target audience, more effective marketing, more customers) and allows the business to expand from the local to the national or global level.

Electronic commerce (e-commerce) is part of electronic business. It involves the electronic exchange of digital content between several entities resulting in a monetary exchange (Chen, 2005). E-commerce refers to any business processes and transactions carried out either in whole or in part by electronic means of communication, in particular the internet. E-commerce uses information and communication technologies to increase the effectiveness of relations between enterprises and individual users. We agree with the definition (Laudon & Traver, 2014) that e-commerce uses the internet, websites, and applications for business transactions, that is digitally enabled transactions between organizations and individuals.

The lowest level of e-business and also a part of e-commerce is an e-shop, which provides e-commerce with a communication interface through web applications.

E-business is characterized by many advantageous features for enterprises and their customers, especially in times of technology convergence. Most important for e-business are (Laudon & Traver, 2014): ubiquity, global reach, wealth, interactivity, universal standards, information density, personalization, social networking technology.

If businesses want to benefit from these features, they need to create and implement an appropriate e-business process. It consists of solving several areas, such as choosing a technical solution, providing marketing, logistics, creating business and complaint conditions, compliance with applicable laws, selecting the target group, purchasing and servicing products. In e-commerce environment, in addition to individual technical and software security, trust between involved parties plays an important role. The trust is a priority in the setting of each e-commerce (Mou, Cui & Kurcz, 2020). Simultaneously, the e-business process should be in alignment with other business processes.

The Enterprise Size Specifics on e-Business Security

Alongside the benefits that ICT brings to the e-market businesses (e.g., market expansion, a higher number of orders and sales, higher availability of information, effective marketing, lower costs, prices), it also brings many risks (Revathi, Shanthi & Saranya, 2015). that represent a threat to enterprises and service providers, but also end-users. With the rapid development of e-commerce and e-business, security issues are arising from people's attention. The security of the transaction is the core and key issues of the development of e-commerce and e-business (Wen, Zhou, Ma & Liu, 2008). From the perspective of enterprises, the risks are directed towards the vulnerability of information assets. It is necessary to protect personal information and other classified information, such as passwords and stored credit card information. Information security in e-business represents the protection of the information assets of enterprises operating in the electronic market against unauthorized use, alteration, destruction, and access to these assets (Niranjaramurthy & Dharmendra, 2013). According to the ISO/IEC 27005 (2012) standard, in regard to e-business, we divide information assets into primary assets (information, business processes, activities, reputation, personal data, knowledge, contacts, source codes), which are difficult to replace, even irreplaceable, and support assets (data, hardware, software, network, personnel, and location), which can be replaced to some extent.

The first stage in asset protection is technological solutions in specialized hardware, software, and security devices. Policies and procedures in the enterprise are other levels of asset protection. This area includes all organizational measures, including security policies, plans, declarations, SLAs, training, procedures, etc. Laws and standards complement the strategic level of a secure e-business environment. Compliance with relevant laws, standards, and best practices indicates information security at an appropriate level for the enterprise and internal or external stakeholders (staff, suppliers, customers, organizations concerned, public authorities, institutions).

Achieving a safe environment requires much effort and additional business resources. We consider this a necessity because as soon as the end-user (customer) loses full confidence in the e-business or has any doubts about the business' security or personal data, he will not carry out a monetary transaction. The customer is sensitive to the information security of e-commerce. Due to the increase in warnings by the media from security and privacy breaches like identity theft and

financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e-commerce has not been able to achieve its full potential. Many customers refuse to perform online transactions and relate that to the lack of trust or fear for their personal information (Yazdanifard, Edres & Seyedi, 2011). The e-commerce security must comply with the following six dimensions (Vasiu, Warren, & Mackay, 2003); Laudon & Traver, 2014; Patro, Padhy & Panigrahi, 2016; bt Mohd & Zaaba, 2019) that warrant adequate information security: integrity, non-repudiation, authenticity, confidentiality, privacy, accessibility. The author Varghese (2022) characterizes the security of electronic commerce precisely through four basic dimensions. E-Commerce security is the guideline that ensures safe transactions through the internet. It consists of protocols that safeguard people who engage in online selling and buying goods and services. You need to gain your customers' trust by putting in place eCommerce security basics. Such basics include: privacy, integrity, authentication, non-repudiation.

According to Muthaiyah et al. (2004), in addition to usability and interface, specialists designing the e-commerce need to incorporate solutions to reduce consumers' security and privacy concerns rooted in trust (Mandić, 2009). Customer confidence is one of the main factors stalling the development of e-commerce (Wu, Zhou & Yuan, 2012). and purchasing decisions (Al Rawabdeh, Zeglat & Alzawahreh, 2012). By applying six dimensions, the company becomes secure from the viewpoint of all stakeholders, which increases the credibility of e-business.

Handling information security in electronic business differs according to individual business size categories. From the viewpoint of IS management and implementation, micro-enterprises, and SMEs create a specific environment compared to large enterprises. The smaller the enterprise, the greater the differences between them, concerning the following areas (Dekýš, 2010):

- SMEs and micro-enterprises have minimal or no security team.
- The IT department performs information security management.
- The security budget is either part of the IT budget or does not exist.
- SMEs and micro-enterprises have a lower range of financial, time, and human resources allocated to information security.
- SMEs and micro-enterprises generally use open-source projects to minimize costs.

Unlike micro-enterprises and SMEs, the larger enterprises allocate resources more comfortably to create a separate IT security department because of the potentially more considerable consequences of security incidents. They are interesting for ISMS professional consulting firms, as they establish cooperation more easily. They are also more aware of the legal requirements for protecting confidential information (SHREDIT, 2017), focusing on more sophisticated security solutions that usually require a more substantial budget compared to SMEs and micro-enterprises. Larger enterprises active in e-business, implement more processes, have a more extensive IT infrastructure and organizational structure, therefore need to provide more information assets compared to SME and micro-enterprises.

Information Security Management Models

Information is a critical part of any enterprise. Acquisition, processing, storage, and confidentiality of information are among the most important activities of the enterprise's life (Kokles & Korček, 2015). To carry out such activities, it is necessary to take care of the technical equipment used to access information, set up an appropriate system for handling information carriers, and adhere to organizational principles for protection against damage. Information protection is necessary concerning any involved party, such as customers, employees, business partners, suppliers. Security deficiencies stem from a lack of appreciation of the importance of information security management (Stehlíková & Horovčák, 2012). With the development of ICT and competition, it is essential to place increasing importance on protecting confidential information, as ICTs have become a tool or the subject of cybercrime.

According to Ernst & Young (2014a), there are five main reasons why enterprises should focus on information security:

- **Change:** The fast movement of enterprises in the post-economic crisis is caused by the emergence of new products, new mergers, acquisitions, market expansion, and new technologies. These changes are complicated, with many negative consequences for enterprise's information security.
- **Ecosystem:** We live in an ecosystem of digitally connected entities, people, and data. The likelihood of exposure to cybercrime applies to both work and home environments.
- **Infrastructure:** Internet access is currently available also for traditionally closed operational technologies, so information security threats are reaching critical infrastructures, such as transportation systems, automation systems, power distribution and household environments.
- **Cloud:** Services based on the principle of data management and storage by a third party create unknown risks that did not exist before.
- **Mobility and customer orientation:** The widely adopted use of mobile computing technologies causes the weakening of corporate boundaries and delivering IT closer to the user and further from the enterprises. The widespread use of the internet, smartphones, and tablets combined with enterprises' positive approach to BYOD has resulted in almost unlimited corporate data access.

Informatization of society encourages enterprises to quickly adopt the issue of quality security of information assets and sensitive data, regardless of their size or focus. Historically, bigger enterprises were the first to deal with information security because they daily processed large amounts of data. Larger and richer enterprises had sufficient resources to invest in securing assets. SMEs mistakenly thought that cyber threats were only directed at large enterprises. More and more, attackers target SMEs because they do not adequately protect their sensitive data (Král, 2011). Enterprises are increasingly exposed to the risk of IS breaches, but many do not even have time to react when a security incident occurs (Huo, Meng & Chen, 2015). As a result of the expansion of computer networks and the internet, businesses are more vulnerable to attacks on confidential information, data, information systems (Bolek, Korček & Beňová, 2015), ICT, and employees.

It is possible to protect enterprises' information assets from information security threats by applying a systems approach. Information security management deals with the issue in detail. Below are definitions from various sources:

- ISO/IEC 27001 (2014) defines information security management as an information security management system (ISMS) that "protects the confidentiality, availability, and integrity of information by implementing a risk management process and providing confidence to stakeholders that risks are well-managed."
- ESET (2014) considers ISMS to be the basis for security risk management to establish, implement, operate, monitor, revise, maintain and improve information security in an organization.
- According to the EU Network and Information Security Agency ENISA (2015), information security management is a system that allows us to achieve the required qualitative characteristics of services offered by organizations (e.g., availability of services, confidentiality, and data integrity, etc.).
- Singh et al. (2013) argue that ISMS is a system of the balanced intersection of technical, managerial, and human aspects of information security in an organization.
- Ondrák et al. (2013) perceive ISMS as an effective documented information asset management system to eliminate their possible loss or damage.

According to the above definitions, we claim that ISMS is a comprehensive system within the organization's overall management system, which protects information from risks. At the same time,

safety management is not just about implementing technical measures, but mostly about management, as confirmed by ENISA (2015) in the following best rules for ISMS:

- IS, and ICT security administrators spend about two-thirds of their working time developing policies, procedures, security controls, risk analysis, and raising security awareness. They spend only a third of their time dealing with technical issues.
- Security relies more on people than on technology.
- Employees represent a much more significant threat than outsiders.
- The strength of security is defined by its weakest link.
- The level of security depends on three factors - a willingness to take the risk, system functions and costs incurred.
- Security is not a state but an ongoing process.

The implementation, maintenance, and constant updating of the ISMS indicate a system approach by enterprises to identify, assess, and manage information security risks (2015). The information security management system brings business continuity, competitiveness, profitability, prestige, elimination of threats and losses resulting from realized risks.

Enterprises manage many activities to make their operations efficient. To mitigate the risks of data breaches and security incidents, companies ensure adequate controls of their information systems by developing different auditing techniques for the physical and virtual systems (Juma'h & Alnsour, 2021). Existing models allow them to identify those significant system activities on which they need to concentrate available resources to achieve continuous system operation. By implementing selected models of information security management, organizations can continuously manage their information assets' security and also, can continuously improve process activities. By comparing selected ISMS models, we get a comprehensive overview of the possibilities of their application in electronic business.

To obtain a comprehensive overview, we identify similarities and differences in information security management models from various aspects. Table 1 compares the presented models, their essence, goal, focus, and starting points. As a dimension of comparison, we have selected specific requirements for implementing and improving ISMS according to ISO/IEC 27001 (context in the organization, leadership, planning, support, operation, performance evaluation, and improvement), which reveal differences strengths, and possible shortcomings of models. Based on the advantages and disadvantages, we evaluate the possibilities of applying models in electronic business, which determines which models can be applied to all processes or only to specific processes of electronic business.

From the comparison results in Table 1, we observe the similarities and several differences of the researched models. Most models are process-oriented and generally applicable within organizations. PDCA models and Cyber Security Framework models can be used universally, for example, for specific activities or processes inside and outside the organization and completely different environments and conditions. Because each model is based on independent research, environment, standard, or framework, it has a different goal of achieving information security. However, they agree that achieving an adequate ISMS level in the organization is necessary.

The model that includes all the information security management standard requirements is the PDCA. On the other hand, some models focus on incorporating only a specific set of requirements (ISSRM, Activate - Adapt - Anticipate, Confidentiality - Integrity - Availability). Other models highlight one or more areas of ISMS requirements while focusing more on some conditions and less on others. We consider it necessary to include the models' shortcomings, for example, concerning the organization's context. Also, the TQISM and BMIS models do not incorporate stakeholder's requirements, and the Cyber Security Framework Process Map does not address the ISMS scope.

Table 1. Comparison of selected models in Information security management

Model	PDCA	Activate Adapt Anticipate	Confidentiality Integrity Availability	TQISM	Domain Model ISSRM	General Model of Influence Factors	BMIS	Process map SRIB	Model according to Cybernetic Security Framework
Entity	Process	Process	Description	Process	Entity and relation	Analysis	Conception	Set of processes	Process
Aim	Continuous improvement	Building a system	Matching of characteristics IS	High quality level IS	Iterative risk management process	Holistic, systemic approach to IS	Alignment, a holistic approach to IS	IS process control	High cyber security level
Focus	Universal	Organizations	Organizations	Organizations	Organizations	Enterprises	Enterprises	Organizations	Universal
Starting point	Shewhart and Deminga's research	Own research EY	IS characteristics	Total Quality Management	Risk management	COBIT 5	Business activity	ISO/IEC 27001, 27002	NIST – Cybernetic Security Framework
Context in the organization	Complete incorporation	Not applied	Not applied	The need to supplement	Not applied	Complete incorporation	The need to supplement	Missing scope determination	Missing scope determination
Leadership position	Complete incorporation	Not applied	Not applied	Partial incorporation	Not applied	Complete incorporation	Partial incorporation	Partial incorporation	Partial incorporation
Planning	Complete incorporation	The need to supplement aims	Partial incorporation	Complete incorporation	Partial incorporation	Missing risk assessment	Missing aims risk assessment	Complete incorporation	The need to supplement aims
Support	Complete incorporation	Not applied	Not applied	Partial incorporation	Not applied	Partial incorporation	Complete incorporation	Complete incorporation	Partial incorporation
Operation	Complete incorporation	Complete incorporation	Complete incorporation	Complete incorporation	Complete incorporation	Missing risk assessment	Missing risk assessment	Complete incorporation	Complete incorporation
Performance evaluation	Complete incorporation	Not applied	Not applied	Complete incorporation	Not applied	Complete incorporation	Not applied	Complete incorporation	Partial incorporation
Improvement	Complete incorporation	Partial incorporation	Not applied	Complete incorporation	Not applied	Complete incorporation	The need to supplement	Complete incorporation	Complete incorporation
Application in electronic business	All processes without restrictions	Cyberspace protection only	IS risk management, some ISMS processes	ISMS as a whole	IS risk management, some ISMS processes	All processes without restrictions	Strategic management, ISMS as a whole	ISMS as a whole	ISMS as a whole

Source: own processing

With Partial Incorporation and where the requirements are not applied, we do not consider it necessary to supplement the models and their recommendations because they do not corrupt the set goals. However, if we identified that a particular part of the requirements is missing, we recommend supplementing or developing the models to obtain an adequate level of ISMS in enterprises.

In terms of application, we claim that, to a certain extent, the enterprises active in e-business can implement all models into their environment. However, not all models apply in the same way and for all processes. We evaluate the General model of impact factors and PDCA as the most complex models we can utilize to manage information security and electronic businesses' operations without restrictions. The other models are applicable either to the ISMS as a whole (TQISM, BMIS, SRIB Process Map, Cyber Security Framework Model) or specific ISMS processes such as cybersecurity (Activate- Adapt- Anticipate) and information risk management (ISSRM, Confidentiality – Integrity – Availability). The available information shows that the BMIS model should also be used in the enterprise's strategic management.

DATA AND METHODOLOGY

Enterprises trading on the electronic markets are exposed to security risk due to the active use of ICT in several transformation process activities. Realized risks cause particular damage to the enterprises

that lack ISMS or a basic process approach to IS management. These negative aspects characterize enterprises that do not have sufficient resources to secure confidential information. These are primarily human resources, but also financial and material. The high costs and complexity of implementing modern tools, techniques, methods, or recommended standards and legislation force enterprises to consider IS only on a superficial level. Due to cost minimization, it is necessary to use open-source (Dekýš, 2010). However, the importance of doing business in the electronic market forces enterprises towards better security and caution in handling information.

Research Model

As a part of the implementation procedures we have established a research model (Figure 1).

Research Assumption and Hypotheses

We determined the following assumptions to formulate hypotheses from the theoretical background analysis and the current state of knowledge on the issue.

RA1: The research assumption is built on the conclusions of scientific studies (Gordon & Loeb, 2002; Gordon & Loeb, 2002; Stehlíková & Horovčák, 2012; Singh et al., 2013; Černý, 2014). We assume that the amount of funds spent on information security correlates with the level of IS set by e-commerce enterprises. When the enterprise is spending more financial resources, it perceives a higher level of IS. Alternatively, if enterprises perceive a high level of IS, their IS expenses are higher.

The hypothesis, which we verify by correlation analysis of the variables the Proportion of IS spending in total expenses and the Level of IS in the enterprise, is set as follows:

- H1₀:** There is no statistically significant, moderate strength correlation between the expenses for information security and the level of information security as set by enterprises, indicated by the correlation coefficient ($r > 0.3$)
- H1₁:** There is a statistically significant, moderate strength correlation between the costs of information security and the level of information security set by enterprises, indicated by the correlation coefficient ($r > 0.3$)

Figure 1. Research model (Source: Own processing)

I. Phase	RESEARCH INITIATION AND CONCEPT			
II. Phase	THEORETICAL BACKGROUND			
	Research Assumption (RA1, RA2), Research Hypotheses (RH1, RH2)			
	Surveyed variables within information security management systems			
	SY01	The need to address ISMS within e-business	SY07	Sufficient financial resources on IS
	SY02	The possibility of protection of e-business without ISMS	SY08	Regularity of IS risk assessment
	SY03	The ability to improve e-business results	SY09	Regularity of IS policy updates
	SY04	The need of ISMS in the respondent's e-business	SY10	Satisfaction with level IS in the enterprise
	SY05	Practicing of ISMS in the enterprise	SY11	The level of IS in the enterprise
	SY06	The proportion of IS expenses in total costs		
III. Phase	SURVEY in Slovakia			
IV. Phase	RESULTS			
	data analysis, verification and falsification of hypotheses			
V. Phase	CONCLUSION			
	formulation of the most significant findings			

RA2: Simultaneously, based on the results of scientific studies (Singh et al., 2013; Černý, 2014; PWC, 2015), we assume that enterprises with a higher budget for information security are implementing and utilizing measures of information security risk management more. On the other hand, those enterprises that do not allocate funding to protect information do not manage information security risks.

Hypothesis 2 examines whether there are statistically significant differences between enterprises with more financial resources for information security and enterprises with fewer resources for information security available.

H2₀: Enterprises with a higher volume (1 standard deviation above average) of information security funds do not differ statistically significantly in managing information security risks from those with a lower volume (1 standard deviation below average) of information security funds.

H2₁: Enterprises with a higher volume (1 standard deviation above average) of information security funds differ statistically significantly in managing information security risks from those with a lower volume (1 standard deviation below average) of information security funds.

The analysis of theoretical starting points shows that mentioned authors examined only selected parts of the research issue and partial factors from our research model in a simplified way. Such extensive research focused on The Information Security Management Systems in e-business has not been carried out in the V4 countries (Visegrad Group) and in Slovak Republic. So far the relationship between information security management and the financial budget of companies has not been investigated. The originality and novelty of the research also lies in its expansion by new investigated variables, where we also investigated the interaction among these new variables.

Our contribution to originality and novelty can be identified in following points: adding and investigating new variables that have not been investigated by other authors so far, investigating interactions each other (among variables), the greatest contribution of originality lies in investigating the impact of information management of security to performance (e-business performance), financial complexity of information security management, information security management and its relationship to financial budget of enterprises, influences of ISMS to the level of information security. Research findings significantly expand the field of knowledge and they are also consistent with recommendations and some topics for further investigation from scientific and academic staff and enterprises that have identified these research gaps.

Data Structure

The values of the variables (SY01-SY11), the data analysis subject, enter the research model. The variables are based on the evaluation from the current state of knowledge/research of the issue, the recommendations of ISO/IEC 27005 on IS risk assessment methods, ISO/IEC 27002 on ISMS good practice rules, and ISMS organizations and experts from business practice, experts from practice collaborating on research at our university.

The variables from the group of enterprise characteristics are either discrete (Number of employees) or categorical (Economic activity - SK NACE Rev. 2, Main customers of e-commerce), which we measure on nominal scales. SK NACE – Statistical Classification of Economic Activities is a categorization of homogeneous activities of economic entities. This means that economic entities are classified into categories according to the main activity they are engaged in. Individual categories are given by law and cannot be changed. On the basis of this categorization economic statistical data on workers, data on inputs and outputs, capital formation or data on financial transactions of individual categories of entities are created. Thanks to SK NACE it is possible evaluate better the economic development in Slovakia. The NACE categorization is introduced throughout the European Union

on the basis of Regulation of the European Parliament No. 1893/2006). The authors Paksiova and Lovciová (2019) also mention using this classification in Europe. We used a ratio scale for the variable Number of employees, and its purpose is to sort respondents according to the enterprise's size. All other variables of the SY groups, except SY08 and SY09, are continuous variables measured on a point scale from 0 - minimum to 100 points - maximum. SY08 and SY09 are categorical variables on the ordinal scale.

A representative data set was obtained from a sample of e-commerce enterprises using the Slovak electronic market. It is a sample of 91 enterprises of various sizes, legal forms, economic activity, focus, and location. Data collection was ensured through online questionnaires from 01/2021 to 03/2021. A questionnaire (conditions of validity and reliability met) was chosen as a research tool. The questionnaire was constructed to be ensured its validity, namely construct, content and criterion validity. The construct validity was assessed by scientific and research workers dealing with the methodology of scientific work and research methods, experts from business practice, experts from practice collaborating on research at our university. At the same time, we compared our research tool and its reporting ability to similar research tools. By content validity we determined whether the research tool would have sufficient explanatory power. A group of experts participated in evaluation and refinement of the research tool to reach sufficient content validity by questionnaire which had been constructed by us. In addition to the above, we also paid attention to criterion validity, and verified how close the relationship between results obtained by given tool and the certain criterion is. The measuring construct empirically shows such relationships with other variables as assumed by theory. Individual questions and variables were formulated based on induction, deduction and to a certain degree abstraction. After obtaining the data, we measured the internal consistency of the questionnaire.

Based on the Number of Employees variable representing the number of employees, we have listed enterprises by size. The largest categories are micro-enterprises (73.63%), followed by small and medium-sized enterprises (23.08%) and large enterprises (3.30%). The data file structure mirrors the order in which the enterprises are currently divided by size in the Slovak Republic. In general, most e-shops in the Slovak Republic are operated by micro-enterprises. For many of them, they make up 100% of net sales. On the other hand, there is a small number of large enterprises in Slovakia, and only a small part of them uses e-commerce, often only as a form of corporate presentation and additional sales. A positive aspect of the survey is that it included respondents from each region of Slovakia and some from the European Union (5.49%). These are entrepreneurs who use e-commerce in the Slovak Republic.

Table 2 lists the number of enterprises in the survey according to the variable Economic activity by SK NACE Rev 2. The most surveyed enterprises are listed in group G (50.55%), group S (21.98%), and group M (6.59%). Not all economic activities in the survey are represented. The results confirm that most e-shops are focused on retail and wholesale sales.

Respondents depending on the variable The main customers of the e-commerce enterprise are divided into three categories: B2C, B2B, and B2G. However, no respondent considers the state administration to be the Main Customer. As many as 89.01% of e-commerce enterprises provide goods and services primarily to individuals, 68.13% are micro-enterprises, 18.68% are SMEs, and 2.20% are large enterprises. 10.99% of the surveyed enterprises focus on enterprises and organizations, of which 5.49% are micro-enterprises, 4.40% are SMEs, and 3.30% are large enterprises. The results show the reality where most e-shops target the end consumer in the form of an individual.

The data set is diverse and adequately structured in terms of the enterprise's characteristics. All data of the variables, which are essential for further investigation, are obtained in the required quality. The reliability of questionnaire is verified by reliability analysis and the reliability of results of statistical processing of collected data by representative sample of data from sample set. Within the survey, we approached 490 compliant enterprises. The number of successfully completed questionnaires is 91, which we consider to be a sufficiently representative sample not only from the point of view

Table 2. Data set structure by economic activity SK NACE Rev. 2

Sector	Percentage of Respondents (%)
A Agriculture, forestry and fishing	5.49%
C Industrial production	2.20%
F Construction	2.20%
G Wholesale and retail trade; repair of motor vehicles and motorcykles	50.55%
H Transport and storage	1.10%
I Accomodation and food service activities	1.10%
J Information and communication	2.20%
K Financial and insurance activities	1.10%
M Professional, scientific and technical activities	6.59%
O Public administration and defence; compulsory social security	1.10%
P Education	2.20%
R Art, entertainment and recreation	2.20%
S Other activities	21.98%
Total	100.00%

Source: own processing

of statistical analysis, but also due to high sensitivity of information obtained from respondents. We guarantee the accuracy of data by choosing appropriate scales of variables. The questionnaire is anonymous and we secured data transmission by encrypted communication, so preserving confidentiality of information was provided. In the survey, we included respondents representing each region of the Slovak Republic and each category of enterprise's size. Most e-commerce enterprises are retailers or wholesalers with the main focus on individuals. Simultaneously, the most used legal forms of enterprises in the Slovak Republic are represented in sufficient numbers. The structure of sample corresponds to percentage distribution, representation of enterprises in individual branches of the national economy of Slovak Republic.

RESULTS

We determined the research assumption and two research hypotheses which we are testing empirically. In the following part of partial analysis and construction of conclusions to verify research hypotheses, we use descriptive statistics to examine individual variables, their correlation, test differences between variables and examined by linear regression analysis whether the values of the variable ISMS in the enterprise.

We analyzed the current state of information security management in e-commerce enterprises in the Slovak Republic through descriptive statistics. Descriptive statistics of the variables, except categorical variables, the Regularity of the IS risk assessment (SY08), and the Regularity of the IS policy updates (SY09) are shown in Table 3.

The variable the Need to address ISMS within e-business (SY01) determines whether it is necessary to deal with ISMS areas in electronic business. The results show that enterprises are inclined ($M = 64.89$, $SD = 30.02$) to argue that ISMS should be addressed in e-business. 50% of respondents stated the number of points more and less than 70, and at the same time, up to 25% of respondents rated the variable by more than 93 points. Enterprises with e-commerce are aware of the importance of ISMS. According to kurtosis, there are more extreme values (-0.73) in the set, and according to

Table 3. Descriptive statistics of variables SY

Variable	Min	Max	Var	Kurt	Skew	Modus	Median	M	SD
SY01	0	100	100	-0.73	-0.51	100	70	64.89	30.02
SY02	0	100	100	-1.03	0.23	50	49	45.02	30.23
SY03	0	100	100	-0.79	-0.09	50	50	51.75	29.38
SY04	1	100	99	-0.74	-0.41	100	60	61.26	29.33
SY05	0	100	100	-0.70	0.66	0	24	30.08	28.59
SY06	0	77	77	4.64	2.04	5	6	12.63	15.11
SY07	0	100	100	-1.03	0.48	–	29	36.95	32.15
SY10	1	100	99	-0.54	-0.61	50	70	66.63	27.09
SY11	1	100	99	-0.68	-0.52	80	70	62.93	27.68

Note: N = 91

Source: own processing

skewness, the values are closer to 100 (-0.51). It is a flatter, obliquely divided division on the right. Because the results of the Kolmogorov – Smirnov test at the significance level $\alpha = 0.05$ confirm that the data are distributed normally ($Z = 1.16$; $p = 0.120$), we can say that with 95% confidence, the interval for the mean value of the Need to address ISMS in e-business between 58.64 and 71.14 points.

Another variable is the Possibility of e-business protection without ISMS (SY02). We examined whether e-business can be protected from information risks without a comprehensive ISMS, where 0 points mean definitely fails and 100 points certainly can. The results show the indecision of the representative enterprises in this issue ($M = 45.02$; $SD = 30.23$; $Modus = 50$; $Median = 49$), although more respondents are inclined to smaller values according to the slope (0.23), i.e., to the Need of ISMS in electronic business. 10% of respondents stated more than 88 points. These respondents claim that protecting e-business is certainly possible without an ISMS. According to kurtosis (-1.03), the distribution is flatter. The data are distributed normally ($K - S$ test; $Z = 1.00$; $p = 0.269$), so we can determine a 95% confidence interval for the mean value of the normal distribution (38.73; 51.32).

Another variable, the Ability of ISMS to improve e-business results (SY03), examines whether the established IS management system can improve e-business performance from 0 (certainly not) to 100 points (certainly can). The results are again in this case inconclusive ($M = 51.75$; $SD = 29.38$; $Mode = 50$; $Median = 50$). Respondents are unable to assess whether the ISMS affects the enterprise's financial results or not. The data are flatter (-0.79), slightly skewed to smaller values (-0.09) and are normally distributed ($K - S$ test; $Z = 0.86$; $p = 0.465$). The 95% confidence interval for the base set mean value is between 45.63 and 57.87 points.

The fourth variable of the SY group, the Need for ISMS in the respondent's e-business (SY04), measures the need to create, implement, maintain and continuously improve ISMS in the surveyed e-commerce enterprise. We defined the scale from 0 (definitely not) to 100 points (definitely yes). 50% of respondents rated this need as more or less than 60 points. The most frequently mentioned value is 100 points, and these respondents are up to 15.38%. On average, survey participants favour the need to improve ISMS in their company ($M = 61.26$; $SD = 29.33$). 75% of respondents stated more than 46.50 points. The data are mostly flat-distributed (-0.74) and skewed on the right (-0.41). According to the results of the $K - S$ test at the significance level $\alpha = 0.05$, the data are normally distributed ($Z = 0.89$; $p = 0.407$); therefore, we can say that the mean value of the distribution is with 95% confidence between 55.16 and 67.37 points.

The variable (SY05), Practice of ISMS in the enterprise, examines whether enterprises create, implement, maintain, and improve ISMS in their environment. The variable is specific because we

categorized its values in the verbal description into four intervals, with which the respondents were familiar. The values are divided into categories from 0 to 25% (enterprises create ISMS), further up to 50% (create and implement ISMS), up to 75% (create, implement and maintain ISMS), and up to 100% (improve ISMS). 0% means that enterprises do not perform any ISMS activity. Most enterprises create only a basic form of information security management (41%), so it is only in ISMS's initial phase. However, up to 13% of enterprises do not carry out any activity in this area. It is interesting that 8% of enterprises already have ISMS in place and are improving this system. On average, enterprises achieve $M = 30.08$ points; $SD = 28.59$ points. The data are skewed to smaller values (0.66) and are rather flat (-0.70). As many as 25% of respondents stated a value less than or equal to 2, which means that these enterprises are not concerned with ISMS at all. The median is only 24 points. Up to 75% of the values fit up to 50 points. These data show that enterprises tend not to implement information security management and do not pay enough attention to the issue. Because the data are not distributed according to the normal distribution ($K - S$ test; $Z = 1.47$; $p = 0.018$), the 95% confidence interval of the mean value cannot be reliably determined.

The following variable (SY06) is the Proportion of IS expenses in total costs, which we measured as a percentage. On average, enterprises invest 12.63% of total costs in IS ($M = 12.63$; $SD = 15.11$). Small and medium-sized enterprises invest the most, up to 18.86% of total costs. It is followed by micro-enterprises (10.81%) and large enterprises (9.67%). We consider the proportion of expenses in all categories to be unnecessarily high. However, the results may be skewed by the low number of respondents in the categories SME and Large enterprises and several high values from the data set, determined by mode, median, kurtosis, and skewness. The mode value indicates that the largest number of enterprises use 5% of the cost of IS. Up to half of the values are less than 6%. As expected, the data are significantly skewed to low values (2.04), and according to the sharpness, most values are close to the average (4.64). Three-quarters of companies spend up to 20% of total costs on IS. Only 10% of enterprises invest more than 30% of their total costs in the issue. According to descriptive statistics, the data are not normally distributed. The $K - S$ test ($Z = 2.49$; $p < 0.001$) confirms that as well. According to statistics, several high values influence the relatively high average. The mode and median show a more realistic picture of the data distribution. Therefore, we claim that enterprises invest about 5% of the total costs in IS, which we consider an adequate amount of IS costs.

The variable Sufficient financial resources on IS (SY07) monitors, on a scale from 0 (definitely not) to 100 points (certainly yes), whether the enterprise has the financial resources that can be used to protect corporate information adequately. 50% of the values represented more or less than 29 points. Regarding the kurtosis, the data set contains more extreme values (-1.03), but more values are smaller in terms of the skewness (0.48). On average, the respondents determined that the surveyed enterprises do not have enough available financial resources for IS, only for $M = 36.95$ points; $SD = 32.15$ points. As assumed, large companies have the most available funds, on average 51.33 points. It is followed by micro-enterprises (37.33 points) and SMEs (33.67 points), which do not have such resources at their disposal. In our view, the ideal interval for evaluating sufficient funding is 75 points or more. However, only 19% of enterprises reported such values, and only 25% of enterprises have enough available resources, specifically over 59 points. As many as 10% of respondents set a value of 0 or 1. It means that about one-tenth of e-commerce enterprises do not have enough resources at all to secure business information. The 95% confidence interval is not determined because the data are not normally distributed, which is indicated by the statistics and the $K - S$ test ($Z = 1.33$; $p = 0.043$).

From the analysis of the variable Regularity of risk assessment IS (SY08), we found enterprises that do not assess risks at all form the largest group, as much as 35.16% of all of them. It is followed by enterprises that evaluate risks once a year (26.37%) and twice a year (14.29%). In general, the more often enterprises deal with risks, the more prepared they are for potential IS threats and incidents. In our opinion, enterprises should evaluate the risks of IS at least once a year. In the survey, this represents 54.95% of enterprises. Although this percentage is surprisingly high for the Slovak Republic conditions, it is still low compared to the IS's risks possible impacts. As many as 26.37% of micro-

enterprises, 7.69% of small and medium-sized enterprises, and 1.10% of large enterprises from the entire group do not evaluate IS risks. In this area, it is necessary to increase safety awareness and draw attention to the consequences of potentially executed risks of IS in the enterprise. Interestingly, the figure 21.98% represents micro-enterprises evaluating risks at least once a year, which we consider extremely good. In particular, we note that the survey revealed up to 18.69% of micro-enterprises, 7.70% of SMEs, and 2.20% of large enterprises in the entire set that deal with risks more than once a year. Although these percentages are unexpectedly high, they should increase significantly in the coming years to address the risks of IS in enterprises adequately.

In the variable Regularity of IS policy update (SY09), we examined whether enterprises have developed an information security policy and at what intervals it is renewed. As assumed, many enterprises do not have this policy developed, represented by 46.15%. On the other hand, 53.85% of enterprises have some form of IS policy, which they are updating more or less regularly. 18.68% of enterprises update their policy once a year, and up to 21.98% of enterprises more than once a year. 38.46% of micro-enterprises, 6.59% of SMEs, and 1.10% of large enterprises from the entire data set do not have an information security policy. These groups need to be targeted in the context of IS education. Enterprises should update their IS policy at least once a year. Because IS threats are constantly evolving, frequent updating is recommended. The ideal frequency of updating the IS policy depends on the conditions and needs of a particular enterprise. For example, large enterprises should improve their policy more than once a year.

The following variable, Satisfaction with IS level in the enterprise (SY10), determines the extent to which enterprises are satisfied with the security of their confidential and sensitive information. Respondents rated on a scale from 0 (definitely dissatisfied) to 100 points (definitely satisfied) how satisfied they are. On average, the business representatives are rather satisfied ($M = 66.63$; $SD = 27.09$); up to 50% of the values are above 70 points. The kurtosis is determined by relatively flat data (-0.54), which are skewed to the right (-0.61), i.e., they contain larger values. According to the $K - S$ test, these data are not normally distributed ($Z = 1.33$; $p = 0.043$). Although most respondents are indecisive (Modus = 50; 15.38% of enterprises), up to 25% of respondents rated the variable more than 90 points. In summary, most e-commerce enterprises are more satisfied with their information security level than not.

The variable Level of IS in the enterprise (SY11) is linked to the previous variable as it measures the perceived level of information protection in the enterprise. Respondents rated the level of information security in the enterprises on a scale from 0 (minimum) to 100 points (maximum). The average value is $M = 62.93$ points; standard deviation $SD = 27.68$ points. Information security in electronic business is at the level of 62.93%. Enterprises claim that their level is sufficient. Due to the current IS threats, the level should be even higher. Micro-enterprises have the highest detected IS level among other enterprises, averaging 67.58 points. The following are SMEs with 50.71 points. The IS level of large enterprises is rather insufficient (44.67 points). Presumably, large enterprises are more aware of the need to protect information than enterprises of other sizes, and they identify their shortcomings more. In addition, compared to smaller enterprises, larger enterprises need to secure more areas, systems, and processes. Respondents mostly rated the IS level with 80 points, and half rated the level with more or less than 70 points. Only 25% of enterprises have a level less than or equal to 47.50 points. The data are more flat than spiked (-0.68), skewed to the right (-0.61), and not normally distributed ($K - S$ test; $Z = 1.63$; $p = 0.006$). IS level values can be explained in two ways. Either the level of information security in enterprises is indeed at a sufficient level, and the results reflect the real situation, or enterprises lack sufficient education and security awareness. At the same time, respondents believe that enterprises' information security level is good.

According to the results of the analysis of the variables of the Information Security Management System (SY), we state that enterprises have a basic overview of IS and are prepared for information security threats only at a necessary, but sufficient level. However, many enterprises still need to improve information security management and implement a suitable system. We also examine our

statements in the following section, the analysis and results, which will further explain the real state of information security management in electronic business.

In the previous section, we used the Kolmogorov – Smirnov to identify that the interval variables (scales) SY01, SY02, SY03, and SY04 are normally distributed. The Pearson correlation coefficient verifies the correlation of the variables. The results are shown in Table 4.

The scale of Need to address ISMS within e-business (SY01) correlates with the scales of Possibility of e-business protection without ISMS (SY02), $r = 0.24$; $p = 0.020$, and the Ability of IS to improve e-business results (SY03), $r = 0.39$; $p < 0.001$, only weakly and thus the strength of the interdependence of these scales is weak. There is a moderately strong correlation between the variables Need to address IS within e-business (SY01) and Need for ISMS in the respondents' (SY04), $r = 0.42$; $p < 0.001$. It shows that the variables have a moderately strong relationship. There is no correlation between the SY02 and SY03 scales ($r = 0.00$; $p = 0.966$), which means that the possibility of protecting e-business without ISMS and improving the economic performance of e-business through ISMS are unrelated. Scales of variables SY02 and SY04, $r = -0.24$; $p = 0.022$, as well as the SY03 and SY04 scales, $r = 0.39$; $p < 0.001$, correlate weakly. Because, according to the results of the K – S test, the values of the interval variables SY05, SY06, SY07, SY10, and SY11 are not normally distributed and SY08 together with SY09 are ordinal variables, we use Spearman's rho and Kendall's tau – c to examine the correlation between them. The results are shown in Table 5, in which we highlighted the correlation values of variables with stronger than weak interdependence.

According to the Spearman correlation coefficient, the Practice of ISMS in the enterprise (SY05) correlates moderately strongly with the scale of the Proportion of IS expenses in total costs (SY06), $r = 0.42$, and the scale of Sufficient financial resources for IS (SY07), $r = 0.41$. In both cases, Kendall's tau-c does not support the moderate correlation strength. The variable SY05 correlates only weakly with SY06 ($\tau = 0.31$) and SY07 ($\tau = 0.30$). The standards for creating, implementing, maintaining, and improving ISMS in enterprises is little related to the costs incurred for information security in enterprises and the perceived sufficient financial resources for adequate protection of enterprise information.

Other combinations of interval variables, except the relationship of the variables Satisfaction with enterprise IS level (SY10) and Level of IS in the enterprise (SY11), have a weak correlation. Therefore, we will not examine them further. The variables SY10 and SY11 correlate moderately strongly, as evidenced by Spearman's rho ($r = 0.68$) and Kendall's tau – c ($\tau = 0.51$). Satisfaction with the Level of information security is moderately related to the set level of information security in the company.

Table 4. Correlation of the variables with normally distributed data

		SY01	SY02	SY03	SY04
SY01	Pearson Correlation	–	0.24	0.39	0.42
	Sig. (2-tailed)		0.020	0.000	0.000
SY02	Pearson Correlation	0.24	–	0.00	-0.24
	Sig. (2-tailed)	0.020		0.966	0.022
SY03	Pearson Correlation	0.39	0.00	–	0.39
	Sig. (2-tailed)	0.000	0.966		0.000
SY04	Pearson Correlation	0.42	-0.24	0.39	–
	Sig. (2-tailed)	0.000	0.022	0.000	

Note: N = 91

Source: own processing

Table 5. Result of Spearman's correlation and Kendall's tau-c

	Statistic	SY01	SY02	SY03	SY04	SY05	SY06	SY07	SY08	SY09	SY10	SY11
SY05	Kendall's tau-c	0.16	0.08	0.11	0.22	-	0.31	0.30	-0.29	-0.31	0.05	0.18
	Spearman Correlation	0.22	0.10	0.14	0.30		0.42	0.41	-0.38	-0.39	0.05	0.26
SY06	Kendall's tau-c	-0.06	-0.01	0.08	0.07	0.31	-	0.18	-0.15	-0.24	-0.09	0.06
	Spearman Correlation	-0.10	-0.01	0.11	0.11	0.42		0.24	-0.21	-0.34	-0.13	0.08
SY07	Kendall's tau-c	0.05	0.15	0.01	0.12	0.30	0.18	-	-0.19	-0.17	0.12	0.22
	Spearman Correlation	0.09	0.21	0.02	0.16	0.41	0.24		-0.25	-0.23	0.17	0.32
SY08	Kendall's tau-c	-0.08	-0.17	-0.12	-0.05	-0.29	-0.15	-0.19	-	-	0.12	-0.01
	Spearman Correlation	-0.11	-0.23	-0.15	-0.07	-0.38	-0.21	-0.25			0.15	-0.02
SY09	Kendall's tau-c	-0.01	-0.13	-0.10	0.00	-0.31	-0.24	-0.17	-	-	0.08	0.02
	Spearman Correlation	-0.01	-0.18	-0.13	0.01	-0.39	-0.34	-0.23			0.11	0.02
SY10	Kendall's tau-c	0.03	0.13	-0.04	-0.01	0.05	-0.09	0.12	0.12	0.08	-	0.51
	Spearman Correlation	0.04	0.18	-0.06	-0.04	0.05	-0.13	0.17	0.15	0.11		0.68
SY11	Kendall's tau-c	0.14	0.12	0.15	0.07	0.18	0.06	0.22	-0.01	0.02	0.51	-
	Spearman Correlation	0.20	0.18	0.24	0.11	0.26	0.08	0.32	-0.02	0.02	0.68	

Source: own processing

There are two ordinal variables in the group of SY variables: Regularity of IS risk assessment (SY08) and Regularity of IS policy updates (SY09). We used several nonparametric tests to determine the strength of their relationship. The results of the analysis are shown in Table 6.

The results of all statistics confirm a correlation of moderate strength between ordinal variables. As a representative sample, we choose Kendal tau-c with the lowest value results ($\tau = 0,55$). The Regularity of risk assessment of IS correlates with regularity of IS policy updates in the enterprise, where the strength of this linear correlation is moderate to strong. We conclude that enterprises that regularly identify and assess risks are automatically updating policies of IS of the enterprise. Both activities lead to the improvement of the whole management of information security in the enterprise.

In general, only some of the scales indicate moderate linear dependence (SY10 and SY11, SY08 and SY09, SY01 and SY04). Correlation between the rest of the scales of ISMS is weak or non-existent (e.g., SY02 and SY03).

Impact of Selected Factors on the Examined Variables of ISMS

The following section verifies the difference between the enterprises that assess the information security risks ($N = 59$) and those that do not assess these risks ($N = 32$). We also look at the difference between enterprises that devised IS policy ($N = 49$) and those who did not devise such policy ($N =$

Table 6. Correlation results of the ordinal variables SY08 a SY09

	Category	Statistic	Type	Value	Asymp. Std. Error	Approx. T	Approx. Sig.
Symmetric measures	Ordinal by Ordinal	Kendall's tau-c	–	0.55	0.06	9.18	–
		Gamma	–	0.74	0.07	9.18	–
		Spearman Correlation	–	0.70	0.06	9.24	–
Directional measures	Ordinal by Ordinal	Somers' d	Symmetric	0.63	–	9.18	0.000
			SY08 Dependent	0.65	0.07	9.18	0.000
			SY09 Dependent	0.61	0.07	9.18	0.000

Note: N = 91

Source: own processing

42). The groups are compared with values of variables (SY) of the information security management system to test if there is a statistically significant difference between them.

The tables below provide an overview of those variables that show the statistical significance of examined differences. Table 7 consists of Levene's test results that indicate that the uneven spread of groups ($F = 4,97$; $p = 0,028$) is statistically significant. Subsequently, the t-test confirms the statistically significant difference in the variable the Need for IB in respondent's e-business (SY04), $t(49, 70) = 2.23$; $p = 0.030$, between those who do assess the risks ($M = 66.64$; $SD = 25.13$) and those, who do not assess the risk of IS ($M = 51.06$; $SD = 34.05$).

The results of non-parametric tests in Table 8 show that enterprises concerned with IS risk assessment differ significantly in variables SY05, SY06 and SY07 ($p < 0,05$) from enterprises that are not. The differences of other examined variables are random ($p > 0,05$).

Table 7. Testing the differences of the variables SY04 depending on the risk assessment

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
	Equal variances	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
SY04	Assumed	4.97	0.028	2.44	89.00	0.017	15.30	6.27	2.84	27.76
	Not assumed	–	–	2.23	49.70	0.030	15.30	6.85	1.54	29.06

Source: own processing

Table 8. Testing the differences of the variables SY depending on risk assessment

Variable		Mann-Whitney U	Z	Asymp. Sig. (2-tailed)
SY05	Practice of ISMS in the enterprise	328.00	-5.13	0.000
SY06	Proportion of IS expenses in total costs	536.50	-3.40	0.001
SY07	Sufficient financial resources for IS	415.50	-4.40	0.000

Source: own processing

In terms of IS policy-making in e-commerce enterprises, the results of testing differences in the examined groups are shown in Table 9. Two-sample t-tests of variables with normally distributed data did not show statistical significance of differences. However, non-parametric testing confirmed the systematic differences in the variables SY05, SY06, and SY07 between enterprises with an IS policy developed and enterprises without an IS policy at the significance level $\alpha = 0.05$.

The results confirm that implementing information security policy influences ISMS practice in the enterprise, the amount of IS costs, and the volume of financial resources for IS. For the other variables of the SY group, the differences are not large enough to be statistically significant ($p > 0.05$).

Impact ISMS Practice on the Level of Information Security

By linear regression analysis, we examine the hypothesis whether the values of the variable ISMS practice in the e-commerce enterprise (SY05) significantly affect the Level of IS in the enterprise (SY11) as set by respondents. The relationship of the variables is shown in Figure 2, where the systematic linear dependence is not obvious but also not excluded.

The results of the analysis are described in Table 10. The correlation coefficient ($r = 0,33$) demonstrates the weak relationship of the variables. The coefficient of determination ($R^2 = 0.11$) explains 11% of the variation of the dependent variable SY11 affected by the independent variable SY05. The remaining 89% is influenced by other factors, such as investments in the

Table 9. Testing the differences of the variables SY depending on information security policy

Variable		Mann–Whitney U	Z	Asymp. Sig. (2-tailed)
SY05	Practice of ISMS in the enterprise	462.50	-4.52	0.000
SY06	Proportion of IS expenses in total costs	577.50	-3.61	0.000
SY07	Sufficient financial resources for IS	527.00	-4.00	0.000

Source: own processing

Figure 2. Correlation diagram of the variable SY05 a SY11 (Source: Own processing)

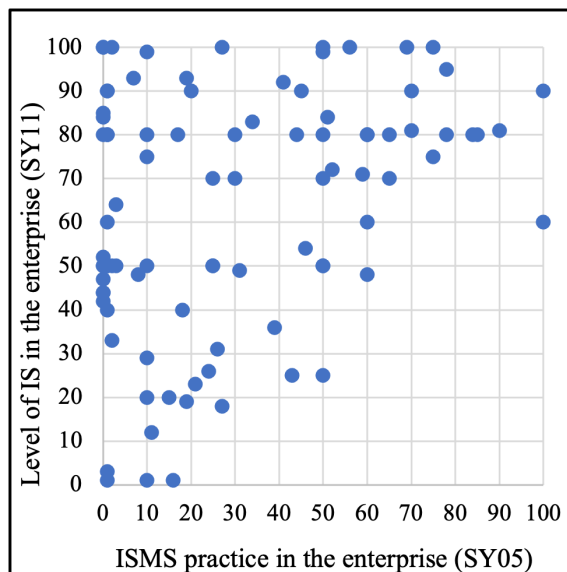


Table 10. Regression model of the dependent variable SY11 and the independent variable SY05

Explanatory Variable	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95% Confidence Interval for B	
	B	Std. Error	Beta			Lower Bound	Upper Bound
(Constant)	53.40	4.01	0.00	13.31	0.000	45.42	61.37
SY05	0.32	0.10	0.33	3.27	0.002	0.12	0.51
Adjust R ²	0.11						
F (1, 89)	10.70**						
N	90						

Note: *p = 0.05; **p = 0.01
Source: own processing

ISMS, security controls, security training, incorporation of IS requirements into business processes, or supply contracts.

Analysis of variance (ANOVA) confirms a statistically significant linear regression model with a good data description, $F(1, 89) = 10.70$; $p = 0.002$. The regression coefficient $b_1 = 0.32$ significantly contributes to the prediction of the SY11 variable ($p = 0.002$). From the results we conclude that Practice of ISMS in e-commerce enterprise significantly affects the Level of IS in the e-commerce enterprise at significance $\alpha = 0.05$.

Verification of Research Hypotheses

In phase II. of the research model, we have established two research assumptions from which we subsequently formulated research hypotheses.

The hypothesis H1 is verified by correlation analysis of the variable Proportion of IS expenses in total costs and Level of IS in the enterprise. The results of the K – S test for Proportion of IS expenses in total costs (SY06; $Z = 2.49$; $p < 0.001$) and for the IS level in the enterprise (SY11; $Z = 1.63$; $p = 0.006$) demonstrate that the variable data are not normally distributed. We selected Spearman’s correlation coefficient and Kendall tau – c to measure correlation, and the results are shown in Table 11.

Spearman’s correlation coefficient is $r = 0.08$, and Kendall’s tau – c is even lower, $\tau = 0.06$. Both values are very low and close to zero, describing the trivial force of the linear correlation of the surveyed variables; therefore, we accept the null hypothesis $H1_0$. The correlation between the costs of information security in e-commerce businesses and the level of information security set by businesses is minimal. There is no statistically significant correlation between the variables.

Table 11. Correlation results of variables SY06 a SY11

	Category	Statistic	Value	Asymp. Std. Error	Approx. T	Approx. Sig.
Symmetric measures	Ordinal by Ordinal	Kendall’s tau–c	0.06	0.07	0.78	–
		Spearman Correlation	0.08	0.11	0.72	–

Note: N=91
Source: own processing

The minimal correlation of the variables, Proportion of IS expenses in total costs, and Level of IS in the enterprise can be observed in Figure 3, where a systematic arrangement of points is not evident. The points are randomly distributed in the graph.

These findings can be explained in terms of security measures divided into two groups. While technical measures are financially costly, IS's organizational measures do not necessarily entail additional costs, although they also contribute to the increase of the perceived and real level of IS. For example, if the enterprise develops, publishes, and adheres to the IS policy that is not a technical measure but is essentially a documented set of rules, it will significantly increase the perceived level of IS, with minimal or no development costs of such a policy. Therefore, the amount of investment in IS investment does not affect the level of IS set by the respondents and perceived in the enterprise.

Hypothesis H2 examines whether there are statistically significant differences between enterprises with more financial resources and enterprises with less information security resources available.

Using the standard deviation method, we divided the variable Sufficient financial resources for IS (SY07) into two groups with extreme values. The average SY07 represents $M = 36.95$ points; $SD = 32.15$ points. One standard deviation above the average is the range of values from 69.10 points to 100 points. There are 18 values in this group. On the other hand, a value of 4.80 points represents one standard deviation below the mean. All units in the data set with this value or less represent the second extreme group. There are 20 values in the group.

The average of the variable Risk management of IS (OP01) at the group values of one SD above the average of SY07 is $M = 40.50$ points; $SD = 37.30$ points. The average of the variable OP01 at the group values of one below the average of SY07 represents $M = 9.95$ points; $SD = 18.36$ points. Already, we observe a significant difference at these values, but through statistical testing, we find out whether the differences are systematic or random.

Before selecting a suitable test, we subject the variable Risk management of IS (OP01) to K – S test that determines whether the values come from a normal distribution. The results show that the data are not normally distributed ($Z = 1.94$; $p = 0.001$), so we select the non-parametric Mann – Whitney U test. The test result shown in Table 12 is highly statistically significant for information security risk management ($U = 22.50$; $p < 0.001$). We reject hypothesis H2₀ and accept the alternative

Figure 3. Correlation diagram of variables SY06 a SY11 (Source: Own processing)

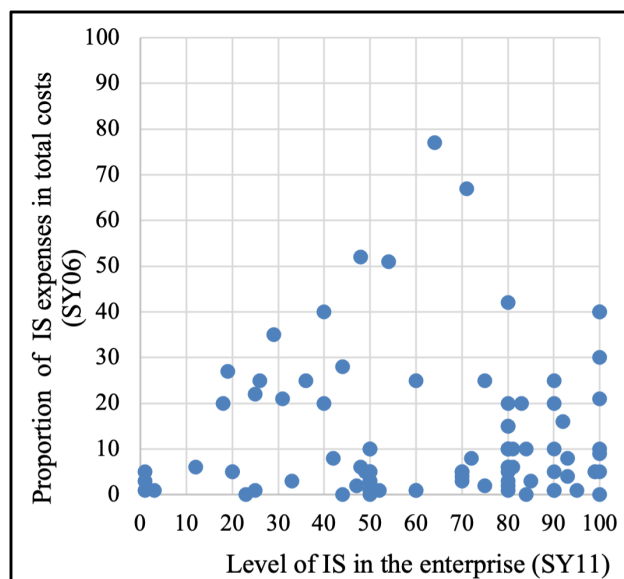


Table 12. Mann–Whitney U test applied on OP01

Ranks	N			Mean Rank		Sum of Ranks	
	1 SD ↓ M	1 SD ↑ M	Total	1 SD ↓ M	1 SD ↑ M	1 SD ↓ M	1 SD ↑ M
OP01	20.00	18.00	38.00	27.38	55.44	547.50	998.00
Test Statistics	Mann-Whitney U		Wilcoxon W	Z		Asymp. Sig. (2–tailed)	
OP01	22.50		998.00	-4.77		0.000	

Source: own processing

hypothesis H2₁. There is a statistically significant difference in information security management between enterprises with larger funds for information security and enterprises with smaller information security funds.

The effect size is determined as $r = -4.77/\sqrt{38} = -0.77$, indicating a strong effect for the data of the variable IS risk assessment. Considering statistical significance $p < 0.001$, a strong effect $r = -0.77$, and the identified systematic differences between the group averages, we state that companies with a higher volume of funds intended for IS make more use of IS risk management.

At the end of presentation of research results, we point out the validity of model, which was fulfilled. We tested for multicollinearity and autocorrelations using the Durbin–Watson statistic. Results of this Durb. Watts. = 2.1; $p = 0.89$ explain that assumption of validity of tested regression models was met.

DISCUSSION

The global nature of e-commerce (Benamati, Ozdemir & Smith, 2021) is complicating privacy issues because perceptions of privacy, trust, risk, and fair information practices vary across cultures, and differences in national regulation create challenges for global information management strategies. We defined Information security management as a comprehensive system within an organization that protects information from threats by implementing and improving information security risk management. By maintaining this system, the organization becomes credible to all stakeholders, such as employees, suppliers, or customers. Creating, implementing, monitoring, and improving of the ISMS consists of numerous activities performed at regular intervals. Some need to be done more frequently (security incident assessment, risk assessment, treatment), while others can be sufficiently performed once a year (e.g., compliance checks, internal or external audits, updating security policies). We consider risk assessment to be the most crucial part of ISMS as it entails creating a complete risk analysis of the organization. As a result of this analysis, it is possible to design appropriate ways of dealing with risks and select adequate security measures at an acceptable cost, thus achieving adequate security of the organization’s information assets.

The processes, recommendations, and goals of ISMS are generally applicable to any company or organization. In many instances, the ISMS needs to be suitably adapted to the organization’s conditions. Similarly, from the perspective of e-commerce enterprises, it is necessary to re-evaluate, modify the ISMS security requirements, or eliminate completely some requirements due to the non-existence of a specific process in the enterprise. Information security management is professionally handled by several organizations, companies, and institutions. They design, research, and assess ISMS strategies, frameworks, standards, recommendations, and measures. In this manner, they appeal to increase security awareness and improve the overall level of IS. In Slovakia, this area is growing, and in the last three years, an increased number of job offers focused on IS. Particularly active are private (ISACA, PwC, Ernst & Young, ESET, SECTEC, Slovak Association for Information Security)

and state organizations. In the near future, we expect a significant increase in engagements by the National Security Office, following from the Concept of Cyber Security of the Slovak Republic for 2015-2020 and the anticipated Act on Cyber Security.

ISO, The International Organization for Standardization, provides certifications according to the ISO/IEC 27001 standard to any organization that meets set requirements. However, the whole certification process can be perceived by businesses not only as an organizational and time burden but mainly as a financial one. Ultimately, although the organization's certification attests to excellent standards of ISMS, it often serves only as a source of prestige and marketing benefits. On the other hand, the results of the survey ISO (2017) on the distribution of the certificates according to ISO/IEC 27001 in 2015 show an increase up 20% compared to 2014. On the other hand, the results of the ISO survey (2017) on the distribution of certificates according to ISO / IEC 27001 in 2015 show an increase of 20% compared to 2014. A total of 27 536 organizations were certified in 2015. The countries with the most certified organizations are Japan (8 240), Great Britain (2 790), and India (2,490). Of the V4 countries, Poland has the most certificates (448), followed by the Czech Republic (381), Hungary (323), and finally Slovakia (232). Compared to 2014, Slovakia improved by 70 certified organizations, while in the Czech Republic, more organizations underwent the certification process, a total of 105. From the last survey (ISO, 2019) in 2019 on the distribution of certificates according to ISO/IEC 27001, it can be deduced that 36 362 certificates. The top 5 (most certificates issued) were in China (8 356), Japan (5 245), the United Kingdom (2 818), India (2 309), and Italy (1 390). Slovakia recorded 219 certificates issued.

The increase in overall interest may mean that organizations are no longer perceiving certificates only as prestige but are beginning to give weight to IS. It is likely caused by the media's cybercrime coverage and the promotional activities of organizations active in IS. However, it is unnecessary to go through the certification process because an adequate level of ISMS can be implemented without certification at a reasonable cost. Besides, the overall increase in awareness of IS through the organizations' activities is already an improvement in information security. The study (Wenqing, Kun & Chia-Huei, 2022) shows that financial performance becomes better as ISO 27001 implementing experience accumulated. This will assist managers to gain confidence in using information security certification.

In our research, formed on theoretical background and current state of knowledge on the issue, we assume that enterprises in the Slovak electronic market lack (Král, 2011; Netolická, 2012b) a comprehensive information security management system. We examined this assumption through the variable Practice of ISMS in the enterprise. The results indicate ($M = 30.08$; $SD = 28.59$) that this statement also applies to our data sample. As many as 25% of enterprises do not address the ISMS at all. 75% of enterprises perform ISMS only at up to 50 points out of 100 points. It is clear from the data that enterprises tend not to implement ISMS. The theoretical basis analysis has already shown that the right way for enterprises is to apply a process approach through ISMS, guaranteeing an adequate IS of e-business. Only 8% of the surveyed enterprises focus on IS system management at this advanced level. The remaining enterprises lack a comprehensive information security management system. However, according to the values of the variable Need to address ISMS in e-business, enterprises are aware of ISMS's importance and at the level of 64.89% are inclined to agree that ISMS should be addressed in e-business ($M = 64.89$; $SD = 30.02$). Besides, the analysis of the data of the variable ISMS Need in the respondent's e-business shows that, on average, businesses agree with the need to improve ISMS in their company ($M = 61.26$; $SD = 29.33$). As many as 15.38% of enterprises are sure that they need an information security management system.

Other findings determined from the current state of knowledge of information security management in e-business can be summarized by stating that e-commerce enterprises do not have sufficient financial resources to adequately secure information assets (Gordon & Loeb, 2002; Gordon & Loeb, 2002; Stehlíková & Horovčák, 2012; Singh et al., 2013; Černý, 2014). As a result of the data analysis, we found that the surveyed enterprises use, on average, 12.63% of the total cost of IS

($M = 12.63$; $SD = 15.11$). However, this figure is skewed by several very high values. Mode (5%) and median (6%) demonstrate a better picture of data distribution. They explain that most enterprises invest around 5% of the total cost in IS. Only 10% of companies invest more than 30% in IS. On average, small and medium-sized enterprises use IS the most, up to 18.86% of the total costs. These are followed by micro-enterprises (10.81%) and large enterprises (9.67%). Simultaneously, the results confirm that enterprises that trade on the Slovak electronic market indeed utilize a certain part of the IS's costs and deal with the security of information assets at least passively. Based on the results of other Information Security Management System (SY) variables, we state that these costs are used by enterprises primarily only for necessary security measures (e.g., antivirus system, application firewall, TLS protocol, backup). We conclude that enterprises have enough available funds for IS at the level of only 36.95 points out of 100 points ($M = 36.95$; $SD = 32.15$). Large enterprises (up to 51.33 points) have the most of these resources, followed by micro-enterprises (37.33 points) and SMEs (33.67 points). 50% of the values represented less than 29 points. As many as 10% of enterprises set a value of 0 or 1 point. These enterprises do not have sufficient resources to secure corporate information assets. The results of the research largely reflect the established assumption. Most enterprises that trade on the Slovak electronic market lack sufficient financial resources to protect information assets. The verification of the research hypotheses showed no statistically significant, moderate or stronger, correlation between Costs of IS and Level of IS set by the enterprises. Contrary to claims (Stehlíková & Horovčák, 2012; Singh et al., 2013; Černý, 2014), we did not confirm the correlation between Cost of IS and Level of IS in the e-business enterprise. In the research, we also found that the examined groups of enterprises differ statistically significantly in IS risk management measures. With a statistical significance of $p < 0.001$ and a strong effect of $r = -0.77$, we can confirm that enterprises with higher budgets for information protection utilize IS risk management more. Our findings are in line with the results of a study by PwC (2015), which states that 24% of enterprises that have increased their IS budgets are more capable of managing IS's risks. From conclusions of the research, the comparison of theoretical starting points and studies carried out, it is possible to formulate realistic applicability: The processes, recommendations, and goals of ISMS are generally applicable to any company or organization. In many instances, the ISMS needs to be suitably adapted to the organization's conditions. Similarly, from the perspective of e-commerce enterprises, it is necessary to re-evaluate, modify the ISMS security requirements, or eliminate completely some requirements due to the non-existence of a specific process in the enterprise. We found out that surveyed organizations pay more and more attention to certification in the field of information security. This increase in overall interest can mean that organizations no longer perceive certificates as prestige only, but they start to attach importance to IS. It is likely caused by the media's cybercrime coverage and the promotional activities of organizations active in IS. The Slovak electronic market lacks a comprehensive information security management system, companies tend not to implement ISMS. It is interesting that companies are aware of the need to implement ISMS. In the scientific article, we point out the applicability of ISMS process approach in comparison with theoretical starting points. One of problems of ISMS implementation and protection of information assets is a lack of financial resources, financial resources are used only for necessary security measures. We point to the percentage of expenditure spent by companies on information security, we appeal to increase this percentage, because security incidents and infiltration can cause irreversible damage to company's information assets. A significant contribution to the novelty and originality of research was examining of IS costs and the level of IS, while this relationship was not confirmed in the e-business enterprise. We recommend companies to increase their budget in IS also because of that we found out a statistical significance (strong effect) between the financial budget on information protection and IS risk management. Enterprises with a higher budget for this area can manage information security risks better.

In addition to implementing ISMS, following principles of e-commerce security, it is necessary also remember the idea of authors (Yadiati & Meiryani, 2019): In many cases, an e-commerce company

can survive not only on the strength of the product, but with a reliable management team, timely delivery, good service, good business organization structure, network infrastructure and security, website design good, several factors include: providing competitive prices, providing responsive, fast and friendly purchasing services, provide the complete and clear information about product and service, provide many bonuses such as coupons, special offers, and discounts, give special attention such as the proposed purchase, providing a sense of community for discussion, input from customers, and others, facilitate trading activities. There is a constant need to pay extra attention to e-commerce security. Increasingly sophisticated cyberattacks threaten customer privacy and transaction safety (Umar, Yudhana & Faiz, 2018; Chen, Cai & Wen, 2021).

The research issue is also reflected in global perspectives and its importance is strengthened at a global level. Legislators in the European Union and individual member states have to also reflect on increasing digitization and those connected growing number of cyber threats. New directives and regulations (DORA, NIS2, CER) will be transposed soon into laws of individual member countries. All enterprises will have to respond to these changes. In case they want to secure themselves against cyber threats, they have an ideal opportunity to do it thanks to possible external financing. The European Union also announces financial aid schemes. It is needed to be prepared thoroughly and take advantage of opportunities to finance digital development and security before it's too late. The upcoming NIS2 directive allowed EU member states relatively wide space for open implementation of security measures (e.g. also in the field of reporting cyber security incidents). At states level this fact could reduce the quality of correct implementation of security measures and overall security in framework of cross-border cooperation with different levels of cyber resilience along with different mitigation and remedial measures. It is the integrity, availability and confidentiality of processed information in networks and information systems (including those included in critical infrastructure) that are threatened by increasing number, frequency, scope and sophistication of cyber security incidents. The conducted study emphasizes that the integrity, availability and confidentiality of processed information in networks and information systems are threatened by increasing number, frequency, scope and sophistication of cyber security incidents. The conclusions of research show that the right way for companies is to apply a procedural approach to IT security management systems. It guarantees adequate IT security of electronic business by minimizing consequences of risks with appropriate security measures at acceptable costs. The results of research showed that the application and compliance with IT security norms and standards is the only „safe and correct“ way. However these standards need to be adjusted and regularly updated to take into account current trends, the situation and the state of e-business cyber security. Certification plays an important role. An independent view of the organization from outside, as well as inside, is one of the biggest advantages of certification because it enables a view of IT security settings from a different point and in a wider context. It ensures that any deficiencies will be identified and addressed before they are misused.

CONCLUSION

The value of high-quality information to the enterprise is substantial. Based on accurate, complete, confidential, and available information, the enterprise can make decisions that make it more stable, competitive, faster growing, and adaptable to the market environment. Especially in e-business, entrepreneurs cannot directly or appropriately target a product or service without quality customer information. On the other hand, without detailed, complete, and reliable information, the customer can hardly buy the product or service. Information and information assets that capture, process, store, create, transform into knowledge, or otherwise work with information are essential in the electronic environment. Enterprises cannot continue to operate without many information assets of high to critical importance. Whenever the enterprise loses, impairs, discloses any crucial information asset, or if the asset is inaccessible, the loss of credibility will cost the enterprise customers, reputation, competitive advantage, and stability.

Conducting business in the electronic marketplace requires the protection of all information assets to achieve an adequate level of information security, ideally through the implementation of information security management. We define ISMS as a comprehensive system within the organization's management, which protects information and information assets from information security risks.

Results and conclusions of this conducted research provide new findings not only for academics, but also for business practice. Creating of a comparison matrix of selected information security models provides an overview of their applicability and a clear picture for scientific and professional public. Conclusions from investigation and verification of hypotheses identify new connections in relationship between information security, investments and costs for information security, which provides important information for management of electronic trading businesses.

Information security risks are caused by various threats directed towards the vulnerabilities of enterprises' information assets. Information security threats exploit information assets in security incidents, which are a source of consequences of various sizes for the enterprise and its operations. In e-business, these threats are all the more likely because the whole transformation process is secured by information and communication technologies and computer networks. Appropriate selection of security measures and process management of information security risks allows eliminating and reducing individual risks to an acceptable level. The ISMS integrates the risk management process and enhances it with a range of activities that lead to continuous, systemically, and procedurally achieved confidentiality, availability, and integrity of information at an acceptable level from stakeholders' perspective. The ISMS processes, recommendations, and goals are generally applicable to any business or organization. In many instances, the ISMS needs to be adapted to the organization's conditions. From the viewpoint of enterprise with e-commerce, it is necessary to re-evaluate, adjust the ISMS security requirements, or eliminate some requirements due to the non-existence of a specific process in the enterprise.

The realized research has certain limitations. The questionnaire survey was conducted by a random selection of enterprises in the Slovak Republic. The research sample is limited in its regional scope. The measuring instrument can also be considered a limitation of the research since the respondents answered the individual questions through self-assessment, while their answers could be influenced by various factors (lack of time, imminent event when filling the questionnaire). Already during the realization of the research, some enterprises noted that the character of the disclosed information is highly sensitive. The degree of generalization of the research findings and conclusions is therefore limited.

ACKNOWLEDGMENT

The paper was elaborated within VEGA No. 1/0388/20 „IT Management in Enterprises in Slovakia: International Standards and Norms Versus Individual Business Processes“ – proportion 100%.

REFERENCES

- Ahluwalia, P., & Merhi, M. I. (2020). Understanding country level adoption of e-commerce: A theoretical model including technological, institutional, and cultural factors. *Journal of Global Information Management*, 28(1), 1–22. doi:10.4018/JGIM.2020010101
- Al Rawabdeh, W., Zeglat, D., & Alzawahreh, A. (2012). The Importance of Trust and Security Issues in E-Commerce Adoption in the Arab World. *European Journal of Economics, Finance and Administrative Sciences*, 2012(52), 176.
- Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2021). Information Privacy, Cultural Values, and Regulatory Preferences. *Journal of Global Information Management*, 29(3), 131–164. doi:10.4018/JGIM.2021050106
- Bolek, V., Korček, F., & Beňová, M. (2015). Information security risk management in Slovak enterprises. In *CER Comparative European Research 2015: Proceedings of the 4th biannual CER conference*. Sciemcee Publishing.
- bt Mohd, N. A., & Zaaba, Z. F. (2019). A review of usability and security evaluation model of ecommerce website. *Procedia Computer Science*, 161, 1199–1205.
- Černý, M. (2014). *Prístup k informačnej bezpečnosti v malých a stredných podnikoch*. Retrieved February 19, 2021, from <http://www.itnews.sk/2014-06-24/c163829-pristup-k-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch>
- Chen, C. M., Cai, Z. X., & Wen, D. W. M. (2021). Designing and Evaluating an Automatic Forensic Model for Fast Response of Cross-Border E-Commerce Security Incidents. *Journal of Global Information Management*, 30(2), 1–19. doi:10.4018/JGIM.20220301.oa5
- Chen, S. (2005). *Strategic Management of E-business* (2nd ed.). John Wiley & Sons.
- Cheng, C. B., Chan, C. C. H., & Lin, K. C. (2006). Intelligent agents for e-marketplace: Negotiation with issue trade-offs by fuzzy inference systems. *Decision Support Systems*, 40(2), 626–638. doi:10.1016/j.dss.2005.02.009
- Dekýš, P. (2010). *Správa informačnej bezpečnosti v malej a stredne veľkej spoločnosti*. Retrieved February 27, 2021, from <https://www.eset.com/sk/firmy/services/clanky/sprava-informacnej-bezpecnosti/>
- ENISA. (2015a). *The ISMS Framework*. Retrieved February 20, 2021, from <<https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/framework>>
- ESET. (2014). *Systém riadenia informačnej bezpečnosti*. Retrieved February 15, 2021, from <http://static1.esetstatic.com/uploads/media/System_riadenia_informacnej_bezpecnosti.pdf>
- EY. (2014a). *Cyber Threat Intelligence – how to get ahead of cybercrime*. Retrieved February 20, 2021, from [https://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/\\$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf](https://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf)
- Gordon, L. A., & Loeb, M. P. (2002). Return on information security investments: Myths vs. realities. *Strategic Finance*, 84(5), 26.
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438–457. doi:10.1145/581271.581274
- Hazarika, B. B., & Mousavi, R. (2021). Review of cross-border e-commerce and directions for future research. *Journal of Global Information Management*, 30(2), 1–18. doi:10.4018/JGIM.20220301.oa1
- Huo, C., Meng, L., & Chen, K. (2015). Research on the University Network Information Security Risk Management Model Based on the Fuzzy Sets. In *International Conference on Automation, Mechanical Control and Computational Engineering AMCEE*. Atlantis Press. doi:10.2991/amcee-15.2015.17
- ISO. (2017). *The ISO Survey of Management System Standard Certifications (2006-2015)*. Retrieved February 20, 2021, from https://www.iso.org/iso/iso_27001_iso_survey2015.xls
- ISO. (2019). *The ISO Survey of Management System Standard Certifications 2019*. Retrieved February 20, 2021, from <https://www.iso.org/the-iso-survey.html>

Ji, H., & Zou, S. (2016). Electronic Commerce in China Information Security Management System Strategy Research. *2nd International Conference on Humanities and Social Research (ICHSSR 2016)*. doi:10.2991/ichssr-16.2016.111

Juma'h, A. H., & Alnsour, Y. (2021). How Do Investors Perceive the Materiality of Data Security Incidents. *Journal of Global Information Management*, 29(6), 1–32. doi:10.4018/JGIM.20211101.oa4

Kokles, M. & Korček, F. (2015). Analýza rizík informačnej bezpečnosti v malých a stredných podnikoch. *Ekonomika a manažment*, 12(1), 38.

Král, D. (2011). Information Security in Small and Medium-Sized Companies. *ACTA VŠFS*, 5(1), 62.

Laudon, K. C., & Traver, C. G. (2014). *E-commerce: business, technology, society* (10th ed.). Pearson.

Mandić, M. (2009). Privacy and security in e-commerce. *Market-Tržište*, 21(2), 255.

Mou, J., Cui, Y., & Kurcz, K. (2020). Trust, risk and alternative website quality in B-buyer acceptance of cross-border E-commerce. *Journal of Global Information Management*, 28(1), 167–188. doi:10.4018/JGIM.2020010109

Muthaiyah, S., Ernest, J. A. J., & Wai, C. K. (2004). Review Of E-commerce Issues: Consumers' Perception On Security And Privacy. *International Business & Economics Research Journal*, 3(9), 77.

Netolická, B. (2012b). *5 zásad pre riadenie a presadzovanie informačnej bezpečnosti v organizácii*. Retrieved February 21, 2021, from <https://www.eset.com/sk/firmy/services/clanky/5-zasad-informacnej-bezpecnosti/>

Niranjaramurthy, M., & Dharmendra, Ch. (2013). The study of E-Commerce Security Issues and Solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, 2(3).

Ondrák, V., Sedlák, P. & Mazálek, V. (2013). *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM.

Paksiova, R., & Lovciová, K. (2019). Reporting on CSR and Ethical and Sustainable Management in Food Industry in Slovakia as an EU Member. In *Ethical and Sustainable Supply Chain Management in a Global Context* (pp. 199–219). IGI Global. doi:10.4018/978-1-5225-8970-9.ch013

Patro, S. P., Padhy, N., & Panigrahi, R. (2016). Security issues over E-commerce and their solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, 5(12), 81–85. doi:10.17148/IJARCCCE.2016.51216

PWC. (2015). *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016*. Retrieved February 20, 2021, from <https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html>

Revathi, C., Shanthi, K., & Saranya, A. R. (2015). A Study on E-Commerce Security Issues. *International Journal of Innovative Research in Computer and Communication Engineering*, 3(12), 12896.

Rouse, M. (2014). *E-business (electronic business)*. Techtarget.

SHREDIT. (2017). *Security Tracker – Australia*. Retrieved February 20, 2021, from https://www.shredit.com.au/getmedia/a4a2f8e5-6f4c-4368-bffe-4e1e557267cd/Shred-it_Security_Tracker_AUS.aspx?ext=.pdf

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ism) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*, 14(4), 226. doi:10.1007/s40171-013-0047-4

Stehlíková, B., & Horovčák, P. (2012). Manažment informačnej bezpečnosti v malých a stredných podnikoch. *Security Revue*. Retrieved February 18, 2021, from <<http://www.securityrevue.com/article/2012/06/manazment-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch/>>

STN ISO/IEC 27001: 2014. (2014). Information technology - Security methods - Information security management systems – Requirements.

STN ISO/IEC 27005: 2012. (2012). *Information technology - Security methods - Information security risk management*.

- Sun, Y., & Wang, P. (2021). The E-Commerce Investment and Enterprise Performance Based on Customer Relationship Management. *Journal of Global Information Management*, 30(3), 1–15.
- Umar, R., Yudhana, A., & Faiz, M. N. (2018). Experimental Analysis of Web Browser Sessions using Live Forensics Method. *Iranian Journal of Electrical and Computer Engineering*, 8(5), 2951–2958. doi:10.11591/ijece.v8i5.pp2951-2958
- Varghese, J. (2022). *Ecommerce Security: Importance, Issues & Protection Measures*. Retrieved July 15, 2022, from <https://www.getastra.com/blog/knowledge-base/ecommerce-security/>
- Vasiu, L., Warren, M., & Mackay, D. (2003). Three strategic dimensions of information security in ecommerce: a literature review based conceptual model. In: *Surfing the waves: management challenges, management solutions: Proceedings of the 17th ANZAM conference*. School of Management, ECU.
- Wen, Y., Zhou, C., Ma, J., & Liu, K. (2008). Research on e-commerce security issues. In *2008 International Seminar on Business and Information Management* (vol. 1). IEEE.
- Wiradinata, T. (2017). Nascent entrepreneurs in e-marketplace: The effect of founders' self-efficacy and personality. *International Journal of Electronic Business*, 13(2/3), 164. doi:10.1504/IJEB.2017.083294
- Wu, W., Shi, K., Wu, C. H., & Liu, J. (2021). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. *Journal of Global Information Management*, 30(3), 1–16.
- Wu, X. F., Zhou, J., & Yuan, X. (2012). The Research of Factors which Effect B2C E-commerce Trust – Based on the Mechanism of Process. *Advanced Materials Research*, 2012(591-593), 2583–2586. doi:10.4028/www.scientific.net/AMR.591-593.2583
- Yadiati, W., & Meiryani, M. (2019). The Role Of Information Technology In ECommerce. *International Journal of Scientific & Technology Research*, 8(1), 173–176.
- Yazdanifard, R., Edres, N. A. H., & Seyedi, A. P. (2011). Security and Privacy Issues as a Potential Risk for Further Ecommerce Development. *International Proceedings of Computer Science and Information Technology*, 2011(16), 1–5.

Vladimír Bolek, PhD, is Associate Professor in Department of Information Management Faculty of Business Management, University of Economics in Bratislava, Bratislava, Slovak Republic. He is a member of the scientific committee of the scientific international conference Competition organized by College Polytechnics Jihlava, Czech republic. He is a member of the Conference Committees of International Business Information Management Association, USA. He acted as "Association Editors" at the ECIS 2018 conference "Beyond Digitization - Facets Of Socio-Technical Change", 23-28. June, 2018, at the University of Portsmouth, UK, for the 26th European Conference on Information Systems. He also works as a reviewer of several scientific journals and international scientific conferences. His research interests include information technology, information systems management, IT management, information security, ambient intelligence, and information literacy.

Anita Romanová, PhD, is Associate Professor in the Department of Information Management. She is a member of the scientific committee of Faculty of Business Management and of University of Economics in Bratislava. Her research interests include information technology, e-commerce, especially Enterprise Resource Planning (ERP) systems, IT governance, information systems management, IT management, and information systems effectiveness.

František Korček is a PhD graduate of PhD studies at the University of Economics in Bratislava, Faculty of Business Management, Department of Information Management. He worked as an assistant professor at the Department of Information Management. He currently works in business practice and is an external collaborator of the Department of Information Management. His research areas are information management, information security, electronic business, electronic commerce and data analytics.