


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

27 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/the-information-security-management-systems-in-e-business/316833

Related Content

THE EXPERT'S OPINION

Paul Cheney (1993). *Journal of Global Information Management* (pp. 45-48).
www.irma-international.org/article/expert-opinion/51238

Differential Effects on ERP Post-Adoption Stages across Scandinavian and Iberian SMEs

Pedro Ruivo, Tiago Oliveira, Björn Johansson and Miguel Neto (2013). *Journal of Global Information Management* (pp. 1-20).
www.irma-international.org/article/differential-effects-on-erp-post-adoption-stages-across-scandinavian-and-iberian-smes/83643

Networked Knowledge Management Dimensions in Distributed Projects

Ganesh Vaidyanathan (2008). *Global Information Technologies: Concepts, Methodologies, Tools, and Applications* (pp. 2574-2597).
www.irma-international.org/chapter/networked-knowledge-management-dimensions-distributed/19132

Optimal Kernel Selection Based on GPR for Adaptive Learning of Mean Throughput Rates in LTE Networks

Joseph Isabona and Agbotiname Lucky Imoize (2021). *Journal of Technological Advancements* (pp. 1-21).
www.irma-international.org/article/optimal-kernel-selection-based-on-gpr-for-adaptive-learning-of-mean-throughput-rates-in-lte-networks/290350

The Effects of Communication Patterns on the Success of Open Source Software Projects: An Empirical Analysis from Social Network Perspectives

Jing Wu, Khim-Yong Goh, He Li, Chuan Luo and Haichao Zheng (2016). *Journal of Global Information Management* (pp. 22-44).
www.irma-international.org/article/the-effects-of-communication-patterns-on-the-success-of-open-source-software-projects/170530