

RISK MANAGEMENT IN E-COMMERCE: A LITERATURE REVIEW

Marta WARSEWICZ

Poznań University of Economics and Business; marta.warsewicz@gmail.com, ORCID: 0009-0001-3689-5905

Purpose: The aim of the article is to provide a structured insight into risk management and explore various types of risk in e-commerce sector, ultimately indicating recommendations, literature gaps and future research directions.

Design/methodology/approach: The approach of this paper is analytical and interpretative, focusing on a systematic review of literature related to risk management in e-commerce, while the theoretical scope includes frameworks that address risk factors and recommendations.

Findings: The analysis highlights the shift towards leveraging technology for operational efficiency and data security, alongside emphasizing the importance of consumer trust and experience. A comprehensive approach combining technological advancements, robust information management, and strategic consumer engagement is recommended to manage these varied risks.

Research limitations/implications: The study's include conceptual ambiguities due to the broad mix of risk categories analyzed. Moreover, including a topic of perceived risks might bias the research towards subjective assessments of risk, which can vary between different user demographics and market segments. Indicating an area for future research direction, a significant gap exists in addressing supply chain and operational risks from a company perspective.

Practical implications: An effective e-commerce risk management strategy involves identifying potential risks, assessing their probability and impact, and implementing measures to mitigate them. Proactive risk management not only supports the security and operational efficiency of e-commerce entities, but also enhances consumer trust and long-term business loyalty.

Originality/value: This paper offers a comprehensive synthesis of the e-commerce risk management literature by categorizing various risks - such as supply chain, privacy and perceived risk - while highlighting the interplay between them, thus providing valuable insights for researchers and practitioners alike. The findings are particularly relevant for e-commerce companies, policymakers and researchers who want to develop targeted strategies to effectively manage risk in an increasingly complex digital landscape.

Keywords: Risk management, e-commerce, perceived risk, online shopping, electronic shopping.

Category of the paper: literature review.

1. Introduction

In today's world, e-commerce has become ubiquitous. The convenience of online shopping is highly favored by consumers, allowing them to purchase a wide range of products with minimal effort. The prevalence of smartphones and internet connectivity has further enhanced the shopping experience, making it more available (Vipin et. al., 2021). Recently, the COVID-19 pandemic has accelerated the trend towards online shopping, as consumers searched for comfort and security while buying goods from home.

However, alongside this growth and turnover potential, there appear inherent risks that must be acknowledged and effectively managed (Ruch, Sackmann, 2009). In this dynamic landscape, where transactions are facilitated through the Internet's network, understanding, and effectively managing risk factors have become essential for businesses and consumers. Risk management is crucial not only for businesses to secure their operations and assets but also for encouraging consumer trust.

There are numerous studies on risk management within management science. However, they often remain general or focus on specific types of risks without proper categorization. This lack of systematic classification limits the understanding of various risks that can arise in e-commerce settings. Furthermore, while perceived risk is an important concept that is frequently discussed in relation to consumer behavior, there is a significant gap in research that integrates this category into the broader concept of risk management in e-commerce. Addressing this research gap is essential for several reasons. First, a structured approach to categorizing risks in e-commerce can help businesses identify and mitigate potential challenges more effectively, leading to increased consumer trust and satisfaction. Second, incorporating perceived risk into a comprehensive risk management framework can enhance the understanding of consumer behavior in digital transactions. This research will contribute valuable knowledge to the field of e-commerce, particularly in the context of risk management.

By conducting a literature review, the main objective of this paper is to provide a structured insight into risk management and explore various types of risk in e-commerce sector, ultimately indicating recommendations, literature gaps and future research directions. The current state of literature on risk management in e-commerce provides a comprehensive analysis including among others: supply chain risks, data and privacy concerns, and customer's point of view. However, researchers primarily concentrate on the customer perceived risks, including psychological, social, or functional risks. When it comes to mitigation strategies, there is a strong emphasis on leveraging technological solutions to prevent fraud and enhance security. Financial and logistics (ex. inventory, demand planning) dimensions are explored primarily through quantitative studies that develop specific mathematical models for managing these risks. Providing trust and ensuring quality are crucial for addressing perceived risks effectively.

2. Research methodology

Twenty articles focusing on risk management in the e-commerce sector were collected. Top journal articles published since 2000 were selected, with the majority published after 2017, as this period was characterized by the rise in e-commerce popularity and a development of technologies. A set of keywords was identified for database searches. The keywords included terms such as: risk management, perceived risk, online shopping, electronic shopping, e-commerce. To assess the popularity and validity of the study topic, the results of these searches were recorded in Table 1, detailing the dates of the searches, the search engines used, and the number of results obtained.

Table 1.

Search terms results and data sources

Search terms	Google Scholar	Science Direct	Emerald
“e-commerce risk management”	1 180 000	42 790	14 000
“electronic commerce risk management”	1 880 000	20 235	19 000
“online shopping risk management”	2 130 000	32 362	18 000
“perceived risk management e-commerce”	573 000	17 613	10 000
“perceived risk management online shopping”	1 730 000	17 400	14 000

Note. Data collected by author on the 29th of October 2024.

Source: Google Scholar, Emerald, Science Direct.

The number of results depends on the database. Google Scholar included the most searches, however significantly less under the search term “perceived risk management e-commerce”. ScienceDirect reached the highest number of results for “e-commerce risk management” and “online shopping risk management” with fewer results for terms including “perceived risk”. Emerald provided the most searches for the term “electronic commerce risk management” the lowest count under “perceived risk management e-commerce”. The significant number of articles and their different ratio of keywords in the databases indicate the popularity and importance of the topic, and also proves that it is worth having sources from different databases.

In the review, all aspects related to risk management in e-commerce are considered. While thinking of risks in a particular industry, various categories can be identified, such as supply chain, payments, data security, threats related to conducting business (the seller’s point of view), and the customer perceived risk. The search was divided into two main components: looking for primary articles in renowned international journals such as Emerald Insight or ScienceDirect and conducting a broader search across less known but reliable sources. The primary data sources were Google Scholar, Emerald Insight and ScienceDirect. Google Scholar enabled to trace articles that may not have been accessible through direct databases. Moreover, AI tools such as ResearchRabbit and scite.ai were used to support the search or link and find articles accurate for the literature review. Then, the 20 articles were collected and searched for similarities and dependencies within the concept of risk management in e-commerce. The definitions and aspects of risk management discussed in the selected literature were

examined. The categories were organized into a table, which was divided into: supply chain, financial/legal and customer perceived risk. Relevant quotes from the articles were assigned to the appropriate columns. Additionally, recommendations to identified risk were also highlighted in the last column of the table.

3. Literature review

With the rise of products' and services' complexity, risk exposure has also grown (Faisal, 2016). Recent supply chain disruptions have significantly impacted company performance of companies. Notably, a fire at a Phillips semiconductor plant in 2000 led to a \$400 million loss for Ericsson (Walker, Wilson, 2017). In 2011, a major earthquake and tsunami in Japan reduced Toyota's production by 40,000 vehicles, resulting in a daily loss of \$72 million in profits (Pettit et al., 2013). Recently, the COVID-19 pandemic has further intensified supply chain vulnerabilities, causing global widespread disruptions that have affected production and delivery timelines, leading to significant financial and social losses. These events highlight the importance of robust supply chain risk management in mitigating such negative impacts. Risk situations can be caused by external factors (economic, environmental, social, political and technological aspects) or internal factors (infrastructure, human resources, process and technology used by a company). Nevertheless, in many situations, risk can be predicted and managed (Verbano, Venturini, 2013). Risk management (RM) has emerged as a crucial strategy for businesses to secure their sustainability and navigate uncertainties in pursuit of their objectives. RM plays a significant role in enhancing competitiveness and supporting business growth by facilitating the formulation of strategies to minimize risks and take advantage of emerging prospects.

E-commerce transactions are subjected to various and additional uncertainties, for instance incomplete information or worries about privacy (Chatterjee, Datta, 2008). As businesses expand their digital presence, the complexity of managing these risks increases. Additionally, researchers are delving into the complex aspects of perceived risk and consumer behavior in online transactions, with a focus on trust, marketing, or quality. Among these factors, perceived risk is a key element, indicating the level of uncertainty individuals link to a product or service, especially in terms of results of their purchase. Perceived risk includes various dimensions, including psychological, social, or time risk. On the other hand, e-commerce involves various logistical operations, including the technical resources such as online platforms, digital stores, and electronic payment systems, as well as the coordination of order processing, storage, shipping, or handling returns (Yu et al., 2016). Having conducted a literature review, table 2 provides a summary of risks divided by categories and recommendations. After indicating article in the first column, the next section of the table relates to supply chain aspects, focusing

on operational tasks primarily from the seller's viewpoint. Legal concerns, such as data privacy and financial fraud, have become increasingly significant within the evolution of e-commerce (Dutta et al., 2019), thus constituting the third column. The fourth segment addresses customer perspectives and perceived risks. Moreover, it is beneficial to provide recommendations for addressing specific risks and outlining potential outlooks, hence the last category within the table.

Table 2.

Summary of risks divided by categories and recommendations

Authors	Supply chain	Financial/ legal	Customer perceived risk	Recommendations
(Tolleuuly et al., 2020)	Financial risk; entrepreneurial risk; risks associated with information security.	Risks associated with the protection of personal data of buyers.		Enhancing technologies; digital signatures; encryption technology; digital envelopes.
(Glover, Benbasat, 2010)	Late or non-delivery; order and pay functional inefficiency risk; receive functional inefficiency risk; exchange or return functional inefficiency risk; maintenance functional inefficiency risk.	Financial information misuse; personal information misuse.	Unmet needs; search and choice functional inefficiency risk.	Software to simplify the ordering procedure functions by saving the customer's information on the retailer's systems.
(Warren, Hutchinson, 2003)		Security risks within information systems		Viable system model (VSM) and baseline security approach
(Park et al., 2004)			Psychological risk; financial risk; functional risk; physical risk; time risk (non-monetary); social risk.	A robust mechanism, which utilize state-of-art Internet technologies; enable consumers to place full trust on the privacy, security, integrity and availability of vendor information; build trust with consumers by giving them complete confidence on the product; reliability; responsiveness' assurance; empathy.
(Ruch, Sackmann, 2012)		Payment risks; transaction risk.		Value-oriented model: retailers to choose only payment methods with a valuable risk-turnover combination per customer and transaction evaluation of unknown customers with little or no data available.

Cont. Table 2.

(Vanneschi et al., 2018)		Payment risks/credit		Credit scoring model to replace the pre-risk check of the e-commerce risk management system Risk Solution Services (RSS).
(Nascimento et al., 2019)		Fraud; privacy concerns.		Acoustic indexes and business intelligence towards fraud detection using buyer-placed information combined with the sound analysis from a confirmation purchase call.
(Chong, 2000)	Operational risk; staff leaving; recruitment procedures.			No solutions proposed. "Risk management is crucial"
(Rosillo-Díaz et al., 2020)			Financial risk; psychological risk; social risk; privacy risk; time risk; performance risk.	Minimize any likelihood of uncertainty or mistrust and ensure that consumers feel comfortable when making any type of transaction; adjusted marketing; provide quality.
(Guru et al., 2020)			Performance risk; financial risk; time-loss risk; social risk; psychological risk; physical risk; source risk.	Companies should understand and tackle various perceived risks at the earliest in appropriate manner.
(Kharsun et al., 2022)	Military risk; infrastructural economic and financial risk; social; reputational.			Strengthening the SCM systems of e-commerce enterprises by analyzing the risks of military conflicts and developing a system of preventive measures; comprehensive application of the methods: equalization, preservation, reduction, and transfer.
(Tang, 2006)	Operational risk; disruption risk; supply chain risks.			Strategic and tactical – supply network design, supplier selection, demand, product variety, postponement information – visibility; sharing management
(Shi et al., 2020)	Inventory risk; tax risk.			Statistical model using machine learning techniques to solve the inventory decisions.
(Ho et al., 2015)			Company's performance, financial risk; psychological and social risk.	Ensure quality, reduce uncertainty about creditworthiness and the ability of a business to deliver reliable goods and services.

Cont. Table 2.

(Tzavlopoulos et al., 2019)			Financial risk; product risk; security risk; time risk; social risk; psychological risk.	To understand the factors of perceived risk that influence consumer online purchase intentions because it provides useful information to the online retailers in e-commerce activities.
(Lăzăroiu et al., 2020)			Social risk; Psychological risk; financial risk.	Trust, social commerce adoption, and product evaluation factors are essential in shaping repurchase intention; competitive price and website reputation.
(Pelaez et al., 2019)			Financial risk; physical risk; psychological risk; social risk; convenience risk; economic risk; personal risk; seller performance risk; privacy risk.	Trust is the essential component of consumer purchase intention; higher perceived risks are associated with lower purchase intentions.
(Dutta et al., 2019)	Supply interruption risks; demand and supply planning and integration risks; demand fluctuation; reverse logistics.	Regulatory and compliance risks; information privacy and security risks; contract compliance and legal risks; employee and third-party fraud risks.		Real time information sharing; flexible supplier/seller base; RFID and GPS technologies; various data backup and recovery mechanisms; insurance and liability contracts; suitable network Infrastructure; product screening by returns.
(Raptis et al., 2002)		Security (Information and communication technology ICT systems)		CORAS method for model-based risk analysis

Source: Own compilation.

4. Analysis and results

An analysis of the table provides a detailed overview of the types of risks encountered in the e-commerce sector, along with various mitigation strategies proposed. The outcomes within the three categories are relatively equally divided. Risks that appear within supply chain were

observed in seven articles. These include mostly supply and demand planning interruptions, inventory (Shi et al., 2020), financial risks, reverse logistics (Dutta et al., 2019), human resources (Chong, 2000), operations and in one case military risks (Kharsun et al., 2022). They focus on operational side. In most cases the entrepreneur has to deal with those risks in order to provide his service. Subsequently, risks that relate to fraud or privacy concerns occur in seven articles. These are mostly risks associated with the personal data (Toleuly et al., 2020), unauthorized access, information (Raptis et al., 2002) and financial misuse, payment risks (Vanneschi et al., 2018) and legal concerns (Dutta et al., 2019). Finally, there are nine articles relating to customer perceived risks (Guru et al., 2020) including psychological, social, and functional inefficiencies that impact consumers' trust and their willingness to engage with e-commerce platforms. These risk categories highlight the complex landscape of challenges that e-commerce entities must face to ensure operational efficiency and maintain consumer satisfaction.

Suggestions for reducing risks are outlined in articles, although some of them relate to the present situation and offer general guidance and direction rather than specific solutions. To mitigate the risks associated with e-commerce, several strategic approaches were recommended. Technological innovations play a critical role, with the implementation of advanced technologies such as RFID, GPS, Internet of Things (IoT), digital signatures, encryption, and robust internet technologies designed to enhance security and operational efficiency. Information management is equally important, emphasizing the need for real-time information sharing, data backup, and recovery mechanisms to ensure data integrity and availability. Organizational policies are also vital. These include training teams on e-commerce risks, sharing organizational policies among customers, ensuring compliance with standards, and implementing robust recruitment procedures. Finally, maintaining consumer trust and confidence is crucial and can be achieved through strategies that ensure transparency, quality assurance, adjusted marketing strategies, and the provision of a personalized, secure shopping experience. These combined strategies help safeguard against the multifaceted risks inherent in e-commerce and enhance consumer engagement and trust.

Several key insights and trends have emerged from the literature review of risk management in e-commerce. There is a notable shift towards integrating technology, leveraging it not only to enhance operational efficiency but also as a fundamental component in securing transactions and protecting consumer data. Over time, there has also been a significant shift in focus from internal risks, such as supply chain and financial risks, to include those risks that directly affect consumer perception and trust. This underscores the growing importance of the consumer experience in risk management strategies. Furthermore, the complex range of risks identified in e-commerce requires a holistic approach to risk management. This approach combines technology, legal compliance, and strategic consumer engagement practices to effectively address the multifaceted challenges faced by e-commerce platforms. These trends highlight the

evolving landscape of e-commerce risk management, emphasizing the need for adaptive and consumer-focused strategies.

The studies collectively acknowledge that managing risks in e-commerce is not only about addressing potential financial and operational losses but also about enhancing the consumer experience and trust, which are critical for the long-term success of e-commerce platforms. This integrated approach highlights the complexity of e-commerce ecosystems and the need for ongoing innovation and adaptation in risk management practices.

Conducting the literature review there is a significant gap in how supply chain and operational risks are approached from a corporate perspective, which is an area for future research directions. This gap consists of the need to develop strategies that target these risks directly at the organizational level. Moreover, while current approaches focus on building consumer trust, there is a lack of comprehensive strategies that holistically integrate both the customer and company perspectives.

5. Conclusions, research gaps and future implications

Risk management in e-commerce is a critical area of focus as businesses increasingly shift towards digital platforms. The digital marketplace, while offering vast opportunities for growth and customer reach, also exposes businesses to a wide range of potential risks. These risks can vary from operational disruptions, such as those caused by supply chain failures or technological breakdowns, to cybersecurity threats including data breaches and financial fraud. An effective risk management strategy in e-commerce involves identifying potential risks, assessing their likelihood and impact, and implementing measures to mitigate them. A proactive risk management supports not only the security and operational efficiency of e-commerce entities but also enhances consumer trust and long-term business loyalty.

This literature review on risk management in e-commerce identifies various types of risks that affect both operations and consumer point of view. Key challenges include supply chain and operational risks such as supply interruptions and logistics inefficiencies, financial and transactional risks like fraud and credit issues, as well as security and privacy risks involving data theft and unauthorized access. Consumer perceived risks impacting trust and engagement are also significant. To mitigate these risks, strategies recommended include implementing advanced technologies such as RFID and encryption, enhancing information management practices, adopting robust organizational policies, and focusing on building consumer trust through transparency and personalized service. On the other hand, providing trust and quality to customers is significant to deal with perceived risk. The review also highlights notable trends such as the increasing integration of technology to secure transactions and protect data, a shift in focus from internal risks to those affecting consumer trust, and the necessity for a holistic

approach to risk management that combines technological, legal, and consumer engagement strategies. These insights emphasize the evolving nature of e-commerce risk management and highlight the importance of adapting strategies to enhance both operational efficiency and consumer trust in the digital marketplace. There is a significant research gap in addressing supply chain and operational risks from an organizational perspective, suggesting a critical need for future research to develop strategies tailored to the company level. Additionally, while existing methods emphasize consumer trust, there is a lack of comprehensive strategies that effectively integrate both customer and company perspectives.

Concerning a broad mix of risk categories such as supply chain, privacy, and perceived risks in a single literature review introduces complexities that can bias specific insights. The overlap of different risk types can lead to conceptual ambiguities. This approach might result in a generalized analysis that misses the details for developing targeted risk management strategies. Moreover, including a topic of perceived risks might bias the research towards subjective assessments of risk, which can vary between different user demographics and market segments.

Indicating an area for future research direction, a significant gap exists in addressing supply chain and operational risks from a company perspective. This gap highlights the need for developing strategies that target these risks directly at the organizational level. Additionally, while the current approaches focus on building consumer trust, there is a lack of comprehensive strategies that holistically integrate both customer and company perspectives. This oversight indicates another critical area for further exploration and development in upcoming studies.

References

1. Chatterjee, S., Datta, P. (2008). Examining Inefficiencies and Consumer Uncertainty in E-Commerce. *Communications of the Association for Information Systems*, 22. <https://doi.org/10.17705/1cais.02229>
2. Dutta, P., Suryawanshi, P., Gujarathi, P., Dutta, A. (2019). Managing risk for e-commerce supply chains: An empirical study. *IFAC-PapersOnLine*, 52(13), 349-354. <https://doi.org/10.1016/j.ifacol.2019.11.143>
3. Faisal, M.N. (2016). Assessment of supply chain risks susceptibility in SMEs using digraph and matrix methods. *International Journal of Industrial and Systems Engineering*, 441-468. <https://doi.org/10.1504/IJISE.2016.080288>
4. Glover, S., Benbasat, I. (2010). A comprehensive model of perceived risk of E-commerce transactions. *International Journal of Electronic Commerce*, 15(2), 47-78. <https://doi.org/10.2753/JEC1086-4415150202>

5. Guru, S., Nenavani, J., Patel, V., Bhatt, N. (2020). Ranking of perceived risks in online shopping. *Decision*, 47(2), 137-152. <https://doi.org/10.1007/s40622-020-00241-x>
6. Ho, W., Zheng, T., Yildiz, H., Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research*, vol. 53, iss. 16, pp. 5031-5069). Taylor and Francis Ltd. <https://doi.org/10.1080/00207543.2015.1030467>
7. Jain Vipin, Malviya Bindoo, Arya Satyendra (2021). An Overview of Electronic Commerce (e-Commerce). *Journal of Contemporary Issues in Business and Government*, 27(3). <https://doi.org/10.47750/cibg.2021.27.03.090>
8. Kharsun, L., Kavun-Moshkovska, O., Kotova, M., Nechyporuk, A. (2022). Adaptation of risk management in the supply chains of e-commerce enterprises under the conditions of political instability. *Eastern-European Journal of Enterprise Technologies*, 5(13-119), 6-20. <https://doi.org/10.15587/1729-4061.2022.265649>
9. Lăzăroiu, G., Neguriță, O., Grecu, I., Grecu, G., Mitran, P.C. (2020). Consumers' Decision-Making Process on Social Commerce Platforms: Online Trust, Perceived Risk, and Purchase Intentions. *Frontiers in Psychology*, Vol. 11. Frontiers Media S.A. <https://doi.org/10.3389/fpsyg.2020.00890>
10. Nascimento, D.C., Barbosa, B., Perez, A.M., Caires, D.O., Hiramã, E., Ramos, P.L., Louzada, F. (2019). Risk management in e-commerce-a fraud study case using acoustic analysis through its complexity. *Entropy*, 21(11). <https://doi.org/10.3390/e21111087>
11. Park, J., Lee, D., Ahn, J. (2004). Risk-focused e-commerce adoption model: A cross-country study. *Journal of Global Information Technology Management*, 7(2), 6-30. <https://doi.org/10.1080/1097198X.2004.10856370>
12. Pelaez, A., Chen, C.W., Chen, Y.X. (2019). Effects of Perceived Risk on Intention to Purchase: A Meta-Analysis. *Journal of Computer Information Systems*, 59(1), 73-84. <https://doi.org/10.1080/08874417.2017.1300514>
13. Pettit, T.J., Croxton, K.L., Fiksel, J. (2013). Ensuring supply chain resilience: Development and implementation of an assessment tool. *Journal of Business Logistics*, 34(1), 46-76. <https://doi.org/10.1111/jbl.12009>
14. Raptis, D., Dimitrakos, T., Gran, B.A., Stølen, K. (2002). The Coras Approach for Model-Based Risk Management Applied to E-Commerce Domain, pp. 169-181. https://doi.org/10.1007/978-0-387-35612-9_13
15. Rosillo-Díaz, E., Blanco-Encomienda, F.J., Crespo-Almendros, E. (2020). A cross-cultural analysis of perceived product quality, perceived risk and purchase intention in e-commerce platforms. *Journal of Enterprise Information Management*, 33(1), 139-160. <https://doi.org/10.1108/JEIM-06-2019-0150>
16. Ruch, M., Sackmann, S. (2009). Customer-Specific Transaction Risk Management in E-Commerce. Berlin/Heidelberg: Springer, pp. 68-79. https://doi.org/10.1007/978-3-642-03132-8_6

17. Ruch, M., Sackmann, S. (2012). Integrating management of customer value and risk in e-commerce. *Information Systems and E-Business Management*, 10(1), 101-116. <https://doi.org/10.1007/s10257-010-0152-2>
18. Shi, Y., Wang, T., Alwan, L.C. (2020). Analytics for Cross-Border E-Commerce: Inventory Risk Management of an Online Fashion Retailer. *Decision Sciences*, 51(6), 1347-1376. <https://doi.org/10.1111/dec.12429>
19. Tang, C.S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics*, Vol. 103, Iss. 2, pp. 451-488. <https://doi.org/10.1016/j.ijpe.2005.12.006>
20. Toleuuly, A., Buketov Karaganda, A.Y., Khussainova, Z., Zhanseitov, A., Jumabaeva, S. (2020). Features of e-commerce risk management in modern conditions. *Academy of Strategic Management Journal*, Vol. 19, Iss. 1.
21. Tzavlopoulos, I., Gotzamani, K., Andronikidis, A., Vassiliadis, C. (2019). Determining the impact of e-commerce quality on customers' perceived risk, satisfaction, value and loyalty. *International Journal of Quality and Service Sciences*, 11(4), 576-587. <https://doi.org/10.1108/IJQSS-03-2019-0047>
22. Vanneschi, L., Horn, D.M., Castelli, M., Popovič, A. (2018). An artificial intelligence system for predicting customer default in e-commerce. *Expert Systems with Applications*, 104, 1-21. <https://doi.org/10.1016/j.eswa.2018.03.025>
23. Verbano, C., Venturini, K. (2013). Managing Risks in SMEs: A Literature Review and Research Agenda. *J. Technol. Manag. Innov.*, Vol. 8, Iss. 3. <http://www.jotmi.org>
24. Warren, M., Hutchinson, W. (2003). A security risk management approach for e-commerce. *Information Management and Computer Security*, 11(5), 238-242. <https://doi.org/10.1108/09685220310509028>
25. Yen Yee Chong (2000). Bringing risk management up to date in an e-commerce world. *Balance Sheet*, 8(5), 22-28. <https://doi.org/https://doi.org/10.1108/EUM0000000005379>
26. Yu, Y., Wang, X., Zhong, R.Y., Huang, G.Q. (2016). E-commerce Logistics in Supply Chain Management: Practice Perspective. *Procedia CIRP*, 52, 179-185. <https://doi.org/10.1016/j.procir.2016.08.002>