Journal of Engineering Science and Technology
Vol. XX, No. Y (Year) PPP - QQQ


# RESEARCH FRAMEWORK OF KNOWLEDGE SHARING IN COLLABORATIVE E-COMMERCE

SYARIFAH B. RAHAYU[1,2,*], SITI F. ASLAH[3], TENGKU M. T. SEMBOK[2], MOHD R. M. ISA[2]

[1]Cyber Security and Digital Industrial Revolution Centre, National Defence University of Malaysia 5700 Kuala Lumpur, Malaysia
[2]Faculty of Defence Science & Technology, National Defence University of Malaysia 5700 Kuala Lumpur, Malaysia
[3]Destination Transport (M) Sdn. Bhd., Corporate member of Chartered Institute of Logistics Malaysia
*Corresponding Author: syarifahbahiyah@upnm.edu.my

**Abstract**

The Internet has been a massive contribution to the growing number of collaborative e-commerce. The collaboration and interaction between businesses have resulted in intensive information sharing. However, collaborative e-commerce causes other issues such as trust, partnership, intellectual property protection, and more. Thus, these issues require significant measures to minimize the impact on businesses, customers, and society. This paper reviews the elements related to knowledge sharing in collaborative e-commerce in order to identify the relationship between trade secret partnerships and organizational trust in collaborative e-commerce. The research has conducted an exhaustive review and analysis of the literature to identify the issues and challenges faced by e-commerce collaborators in sharing knowledge. From the literature gathered, a proposed model of research framework consisting of interrelated constructs is illustrated that can be used for details studies on Knowledge Sharing in collaborative E-commerce. Future work is to adopt blockchain technology in securing digital assets exchange among the collaborators of e-commerce.

Keywords: e-business, relationship trust, technological trust, IR 4.0, blockchain

## 1. Introduction

Majority of businesses in most markets are small and medium enterprises (SMEs). With 28 million SMEs in the United States and 5.2 million SMEs in the United Kingdom, SMEs represent almost the entire (99.7%) marketplace [1]. Due to the enormous market size and value of e-commerce, cybercriminals can attack and threaten the online business platform from a far wider range of angles. The financial and legal ramifications of data breach occurrences on e-commerce are getting worse, according to empirical studies on the subject [2]. Consumer data accounts of commercial retailers account for the majority (80%) of the data breach [3].

Technological advances in the global Industry Revolution 4.0 have changed the e-commerce model. Today, there is no communication boundary between business-to-business e-commerce and customers [4-6]. Even though the new generation of collaborative e-commerce enhances and improves the process of today's e-commerce business, careful attention is also required to reduce the number of cyber-attacks in the e-commerce industry [7]. Security adaptation is of critical importance to protect businesses and customers. Additionally, the deployment of security measures significantly contributes to boosting consumer confidence in e-commerce companies. To address the dangers and difficulties of the e-commerce industry, several risk management frameworks and standards can be used, enhancing security [8]. In order to determine the relationship between trade secret partnership and organizational trust in collaborative e-commerce, this article examines the knowledge-sharing components in collaborative e-commerce.

## 2. E-Commerce

Present, consumers frequently buy goods and services online, which has helped fuel the growth of the e-commerce industry [9]. According to earlier scholars [10–17], e-commerce, also known as electronic commerce, is essentially the transaction of all business activities through network technologies. The transactions to buy, sell, transport, or trade data, goods, or services are included in these business activities. The affordability of technology and the Internet's capacity to establish a bidirectional network are the two key drivers of business interactions. [18, 19]. There are four categories of e-commerce as proposed by Chaffey [18], Manzoor [20], Turban [21].

B2B transaction makes up 85% of the e-commerce [21] and is the primary type of e-commerce business to business relationship in the marketplace; the percentage of B2B transaction is greater [19]. Several scholars agreed on the benefits of e-commerce in the digital economy that is evident by the increasing use of this kind of business in the marketplace. According to [22], among the benefits are timesaving [21], cost reduction [23], and quality improvement [24]. The adoption of e-commerce comes at a high cost [25, 26] compared to its advantages [27], and there are problems with data security and the interchange of data between customers and sellers [25].

Beyond Web 2.0 and the digitalization of corporate operations, a new revolution dubbed as IR 4.0 has been brought about by the convergence of all ICT. Despite the fact that IR 4.0 has many different meanings, Schwab [28] describes it as the

interconnectedness of diverse innovations and technologies across the physical, digital, and biological worlds. Due to the current paradigm shift in IR 4.0, network integration is now possible with customer social networks as well as business-to-business e-commerce.

The contact between businesses in collaborative e-commerce is information-intensive [29]. The network increases with greater openness in data exchange and information sharing between firms because there is no restriction on geographic location. It becomes possible to switch between explicit and implicit forms of information. Additionally, information exchange has become bilateral and requires stricter regulation by the participating entities [30]. In some instances, this interaction involves crucially important, commercially sensitive data (CBI) in e-commerce. According to Arrasvuori, Liting, and Kuusisto [31], CBI needs to be secured in order to give organizations some measure of control over the information that is shared between them. A few examples of e-commerce-driven mergers are given by Scott [32], such as the merger of a pharmacy supplier with a health insurance provider, which has provided new insight into the B2B network. To reach more customers and improve customer happiness, businesses must network.

An empirical study of [33] has revealed factors that are critical in the success of B2B, which promote a harmonious relationship between the parties involved. Hitpass [26] state that interaction at the global level scale have a big influence on how corporations connect with one another. Businesses and organizations must attain best practices in business process integration in order to compete globally. Therefore, in order to encourage the exchange of information and expertise, corporate collaboration requires a high level of trust [33, 34].

Collaboration in e-commerce is successful when there is a good interpersonal working connection. A case study [35] shows that relationship trust is a critical factor in the realization of the value of a B2B, especially in e-commerce partnerships. The findings of this study suggest that there are three factors influencing relationship trust, namely goodwill, predictability, and competency. Moreover, relationship trust is another factor reinforcing the trust relationship between all parties. For instance, having a shared objective is a key component of trust in business relationships. According to Chen, Lin, and Yen [36], in order to build strong relationships with their partners, increase trust, and promote additional information sharing between the businesses, there must be clear shared goals between the firms. Chang [37] highlights the successes that occurred when all partners embraced the shared objective of cost and knowledge sharing. The researchers show that the downstream and upstream partners of a textile factory follow the decision of the textile factory to shift to using a digital and integrated business platform. The adoption of an integrated business platform saves time and costs and increases economic gain. Therefore, organizations that wish to cooperate have to align their goals and objectives.

From a technological standpoint, the first obstacle to trust in an e-commerce joint endeavor is technological. Having a technology infrastructure and control mechanism that can deliver an authentic, legitimate, and secure e-commerce transaction is the most crucial component of a cooperation [38] since the first contact point in B2B e-commerce is the use of the partner's technology or platform.

Ratnasingam [35] states that economic benefit will improve after familiarization is established, thus facilitating the cooperation between the employees from both organizations.

In contrast, several papers, including those by [33, 34, 39, 40] raise the issues concerning the SMEs e-commerce adoption. Among the concerns are usability, reach and cost of integration. The dichotomy between partners' efforts to improve economic competitiveness and knowledge preservation is another reason for concern. An understanding of the dimensions involved in inter-organizational knowledge sharing, including the type of knowledge, manner of knowledge sharing, and dynamic of knowledge sharing, has been made possible by a serious discussion on this issue [30]. The advantages and disadvantages of information sharing in e-commerce collaboration have been demonstrated in earlier studies [34, 35, 41]. Technology and interpersonal relations are the two main problems in information sharing.

The economic impact of an organization's competitive advantage on its rivals is also increased by the adoption of a measured strategy to operational risk in the domain of information exchange [42]. The rise of international competition is one illustration of operational risk, which may compel firms to work together inside and across industries. Internal knowledge sharing is concerned primarily with confidential business information (CBI) such as technological knowledge. CBI is a critical intangible asset of a company, and therefore must remain confidential [31]. Falkenreck and Wagner [33] urge further investigation into the long-term social and economic advantages of business-to-business relationships between firms. Another critical success factor (CSF) for effective risk management is trust. According to Seyed M, Seyed H and Siamak N [43], the CSF for risk management is dependent on the level of trust and confidence between the parties involved. Hence, trust and confidence must be present when deciding a suitable risk management structure for knowledge sharing in cyber security.

## 3. Cybersecurity

Nearly every company needs to use the Internet to remain current and get an advantage over its competition. The Internet of Things (IoT) and the proliferation of ICT infrastructure present new problems for managing cyber security [44]. Therefore, it is crucial to comprehend the precise meaning of information security, information and communication technology security, and cyber security—terms that are frequently and indiscriminately used to define information technology governance. According to Whitman and Mattord [45], information security is the protection of critical characteristics of the information asset, namely the Confidentiality, Integrity and Availability (CIA) triad. Information security governance assures the safety of an organization's information asset and that articulated strategies are communicated across the organization and aligned with the organization's business strategy [46]. Von and Van [47] define information and communication technology (ICT) security as technology protection for storing or transmitting information. Thus, cyber security [48] is the ontology for protecting information assets, including the processes, tools, guidelines for storing assets, and transmission in the cyber environment.

The overall security goal is to ensure that the CIA triad—three crucial aspects of information—remains intact and is safeguarded. This CIA triad is essential in the security model for the security requirement. Over time, the expanding boundary in information exchange requires better security protection. Cyber security plays a critical role in knowledge sharing, including protecting sharing information. Information security governance, according to Humphreys [49], ought to cover risk management, including but not restricted to IT risk, human risk, and operational risk. A severe issue with the human risk is a trust violation that leads to the misuse of information, including identity theft, fraud, and IT sabotage. To address these problems and reduce, if not completely eliminate, the risks, a cyber security risk framework is required. [50].

Several risk management frameworks [51 – 52] are available for ensuring cyber security in knowledge sharing. For example, Cherdantseva and Hilton [53] propose the Reference Model of Information Assurance and Security (RMIAS) for incorporating the Information Security (InfoSec) and Information Assurance (IA). According to the RMIAS model, risk analysis is carried out to determine the security goal [54]. The confidentiality of information assets within businesses and the ease and security with which information security knowledge can be communicated should be the main areas of future study.

Additionally, the widespread usage of ICT in modern society needs to be safeguarded [47]. The interchange of information in an electronic setting is subject to a number of risk considerations, including threats, vulnerabilities, and consequences. Ustundag and Cevikcan [55] contend that a large number of connected devices increases data intensity, which encourages theft and unlawful access. The worldwide economy loses $400 billion annually as a result of cybercrime, and this figure has been rising exponentially [56]. Cyber espionage has a similar high economic cost as cybercrime. The partnership between Compaq and CISCO is an example of the two essential components of trust in the cyber security of information sharing [35]. Compaq is a client of Cisco. It is a large company with 300 employees, and its main business activity is purchasing software and hardware products. Cisco is a small-medium supplier of software and hardware products with 20 employees. With the application of best practices through policy and standard procedures, both organizations demonstrate a high level of mutual trust.

Thus, RMIAS is a suitable and relevant model for addressing the cyber security issues in knowledge sharing because its dimensions cover information and security, including goals, comprehensive countermeasure, and development lifecycle. It builds a strong trust and confidence between the parties in e-commerce. Each party knows what, when, with whom and how to share their information. Therefore, knowledge sharing is safe within the boundaries guarded by cyber security.

## 4. Trade Secret

Trade secrets are becoming more and more well-liked as a kind of intellectual property in the modern, global economy, as highlighted by Kumar et al. (2012) [57]. Due to its increased value as an intangible asset in the information economy, trade secrets have an edge over other forms of intellectual property like patents, trademarks, and copyrights [58]. According to Soares and Kauffman [59], the nature

of data sharing in the Internet of Things (IoT) environment presents a challenge to data protection. They back up this claim. Trade secrets, according to Bone (1998), are the final and most important category of intellectual property (IP) [60]. Thus, a trade secret is a secret tool, piece of knowledge, or method employed by a business in the creation of its goods or delivery of services [61]. A trade secret, according to Kumar, R.C. Tripathi, and M.D. Tiwari [57], is a piece of knowledge that is unique to a specific firm and has a legitimate value that aids the organization in gaining a competitive advantage over rivals.

A trade secret is defined according to three criteria: it must be an exclusive property, have a value deriving from it, and be subject to a reasonable attempt to preserve it. A trade secret can be a formula, pattern, technique, or process. Lemley [62] disputes this concept and claims that it is permissible to define trade secrets as legally binding information similar to one's intellectual property rights. However, requiring evidence of secrecy to ensure its protection is another approach to revoke the trade secret's initial public rights. Technical trade secrets and business trade secrets, as well as the information's patentability, have been classified as trade secrets by researchers [34, 57]. The contact between businesses in a collaborative e-commerce environment is information-intensive, and there is a chance that the shared data contains CBI and trade secrets. In order for the commercial connection outlined by Falkenreck and Wagner [33] to succeed, the two essential criteria must be met. Additionally, the shared CBI might be a trade secret in fields of innovation and knowledge generation like research and development (R&D). For instance, in a case study of an innovation ecosystem in the aerospace and defense (A&D) and information and communications technology (ICT) sectors, sharing knowledge is a key mechanism for creating value [63]. This procedure is appropriate provided that the risk is reduced through a written agreement (for A&D) and product differentiation (ICT).

Additionally, the kind of data interchange determines the type of information protection. The problem in data protection, according to Loebbecke and Van Fenema [30], is striking a balance between the need for information exchange and maintaining an organization's competitive advantage. The two frequently become interchangeable, which could have unfavorable effects. To resolve the hazy distinction between trade secrets and confidential business information (CBI), empirical study was conducted. Trade secrets, according to the author, are a subset of CBI [31], and [34] support this opinion. Hence the treatment and protection given to a CBI can be extended to a trade secret. Arrasvuori, Liting and Kuusisto [31] identify two areas for improvement in managing and protecting CBI and trade secret, namely better employee training concerning the handling of CBI and trade secret and changing the company's culture about CBI and trade secret protection. Based on the different opinions and findings discussed above, it is apparent that trade secret can be a subset of CBI. To maintain a competitive advantage, trade secrets must therefore be protected in some way.

The number of trade secret litigation cases has significantly increased during the past 50 years. Current or former employees (59%) and business partners (31%) were the two main sources of trade secret misappropriation in 2008 [34]. Five years later, permanent employees were responsible for 80% of the information misappropriation

[64]. The analysis's findings indicate that an unacceptably high proportion of instances of misappropriation include a close relative of the trade secret owner as the source. The act of misappropriation results from the adoption of a different ideology and a drive of credit; it is made possible by exploiting the flaws in an organization's security policy and management. Bone [60] identifies three instances that facilitate the tendency for trade secret misappropriation. The defendants either violate a contract (i.e., breach of duty), break the law (i.e., theft, fraud or trespass), or misappropriate commercial ethics. These acts may be carried out by the current employees or former employees. However, the number of cases involving the third party has significantly decreased to 7% of the total reported incidents. This decrease may be due to the enhanced awareness of data protection and the countermeasures implemented by organizations to protect trade secrets.

According to the findings of a survey, a significant portion of ICT-based companies (70.9%) see trade secrets as a crucial technique for safeguarding their internal company knowledge [65]. The number of patent applications filed at the European Patent Office increased significantly (by 54%) between 2014 and 2017, according to Maskus [66], and the top five petitioners are ICT businesses, including Samsung Group. In contrast, the high cost of patent registration has influenced organizations to leave their information unpatented [67]. Instead, the owners of the trade secrets have taken several measures which constitute reasonable trade secret protection. Among the implemented measures are protecting the IP rights of documents and publication [31]; computer and physical-based measures [53]; confidentiality agreement with employees and third party [59]; education and policy awareness campaign, and comprehensive protection measures [66].

## 5. Industrial Espionage

The worldwide IR 4.0 helps e-commerce partners gain a stronger competitive edge. [38]. Verbano and Venturini [42] concur with this and state that businesses have to take the operational risk in sharing knowledge to achieve a higher competitive advantage. However, all organizations must balance between protecting information and sharing knowledge to increase their competitive advantage while also avoiding adverse consequences [30, 37, 62, 63]. Giachetti and Lanzolla [68] posit that a negative outcome from competitive advantage is product imitation and suggest that the innovative products introduced by market leaders are often imitated more quickly than the diffused products. Market leaders must therefore be ready to take all necessary precautions to safeguard their transient market edge from corporate espionage.

Threats from business intelligence and industrial espionage are included in the protection of competitive advantage. The distinction between them is vague [69]. Harvey anf Evans [39] concur that the offensive action is including cyber espionage. A crucial defensive strategy for combating cyberespionage is information assurance [53]. The CNEX versus Huawei case [70] is a recent illustration of industrial espionage.

## 6. Overview of Issues and Challenges of Knowledge Sharing in Collaborative E-Commerce

The paper is focusing on e-commerce for knowledge sharing. The knowledge sharing has a direct relationship to impact on human & society. Furthermore, the successful of knowledge sharing depends on Partner, who to share with, and Trade Secret (IP). The IP may include Patent and Copyright, however, these IP insufficient to protect CBI of e-commerce. In order to protect CBI and trade secret, few measurements have been introduced by previous works [31, 53, 59, 66, 71, 72]. All of the above measures and cybersecurity can be utilized to develop a theoretical framework for the trust tactics between e-commerce partners and trade secret protection [73, 74, 75]. Cybersecurity is focusing on managing risks such as human risk, IT risk and operational risk. These risks would assist e-commerce businesses [76] in selecting a suitable risk management framework, for example, RMIAS, NIST SP 800-30, COBIT 5, OCTAVE and ISF. They also may develop its own risk management framework [77] and focus on physical network of commercial information [78].

The relationship trust includes interpersonal relationship. Interpersonal relationship measures consist of staff training on do's and don'ts involving sharing of information related to CBI and trade secret within organization as well as external parties. In shared goals, organizations must put in place a confidentiality agreement that are best fit to the parties involved. They must adequately 'sharing' cost and knowledge via digital and integrated platform. Other contribution factors are goodwill, predictability, and competency. In technological trust perspective, alignment of technology platform used increase level of ease and trust with collaborating partner. And to ensure both parties adhere to the rules of the game, a standard policy are needed which will be a determining factor in the continuity of the relationship in the future. Contribution factors of technological trust are technological infrastructure and control mechanism. For example, e-commerce collaborators may have a ground understanding on a secure e-commerce transaction. Thus, a reputation of e-commerce [79] can be strengthen. Figure 1 shows a proposed model of research framework.

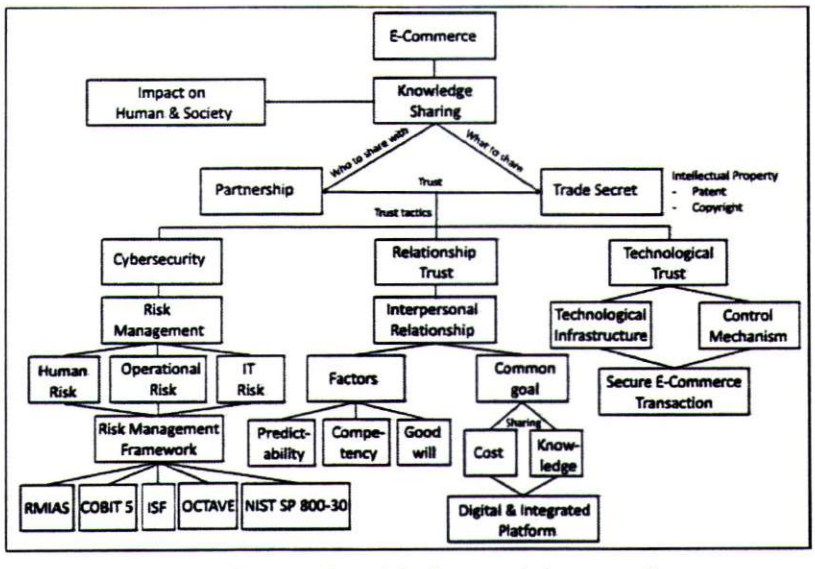


**Fig. 1. Proposed model of research framework**

## 7. Discussion

A review of the literature shows e-commerce must deal with knowledge sharing extensively. Under knowledge sharing, the two main parts are dealing with partnership and types of intellectual property to be shared. The research reveals trust is the major factor in knowledge sharing. This will include relationship trust, technological trust and cybersecurity.

Relationship trust is focusing on interpersonal relationship among the e-commerce partners. There are three main factors to establish a strong interpersonal relationship such as predictability, competency and good will. The partnership must have a common goal either sharing cost or knowledge to digitalization an integrated platform.

Technological trust is emphasizing on the technological infrastructure and control mechanism in order to ensure a secure e-commerce transaction. Secure e-commerce transaction will strengthen the relationship among partners and also customers. Companies which dealing with online payment transaction including Secure Electronic Transaction (SET), Secure Sockets Layer (SSL) and blockchain. For example, SET is a system and electronic protocol to ensure the integrity and security of transactions, while blockchain is a digital ledger to secure a chain of transactions conducted over the internet.

Knowledge sharing somehow must be protected from malicious activities either internal and/or external threats. Companies must look into risk management in terms of human, operational and IT risks. They may start with existing Risk Management Framework such as RMIAS, COBIT 5, ISF, OCTAVE and NIST SP 800-30.

As a result, the proposed model of research framework has cover the important factors in sharing information and knowledge among e-commerce partnership. Those factors may reduce the negative effects of industrial espionage on people and society by utilizing both relationship and technology trust as well as cybersecurity.

## 8. Conclusion

This study has covered in great detail the difficulties and problems associated with knowledge sharing in collaborative e-commerce, as well as how to build and maintain trust among e-commerce collaborators to safeguard knowledge sharing. The most useful approach for cooperative e-commerce is the use of a trade secret. High organizational trust e-commerce collaboration calls for the use of shared best practices via policies and standards.

Trade secrets must be safeguarded against cybercriminals and a future trade secret model should be utilized to gauge knowledge sharing awareness. The long-term social and economic benefits of business-to-business relationships between firms should be the subject of future research in this area. Additionally, e-commerce major players may benefit from stronger and more secure digital assets through the deployment of technology like blockchain during knowledge sharing.

## 9. Acknowledgement

The authors would like to acknowledge UPNM for the financial support under grant UPNM/2022/GPJP/ICT/3.

## References

1. Holland, C. P.; and Gutiérrez-Leefmans, M. (2018). A Taxonomy of SME E-Commerce Platforms Derived from a Market-Level Analysis. *International Journal of Electronic Commerce*, 22(2),161–201.
2. Sen, R.; and Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, 32(2), 314–341.
3. Kim, B.; Johnson, K.; and Park, S.-Y. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management*, 4(1).
4. Mingione, M.; and Leoni, M. (2019). Blurring B2C and B2B boundaries: corporate brand value co-creation in B2B2C markets. *Journal Marketing Management*, 36(1-2), 72–99.
5. Seals, T. (2021). IoT Attacks Skyrocket, Doubling in 6 Months | Threatpost. Retrieved April 1, 2022, from https://threatpost.com/iot-attacks-doubling/169224/
6. Taiano, J. (2021). B-to-B and B-to-C Boundaries Are Blurring. Retrieved March 5, 2022, from https://www.adweek.com/performance-marketing/b2b-b2c-boundaries-blurring-what-it-means-for-marketers/
7. Aggarwal, P.; Gonzalez, C.; and Dutt, V., (2020). HackIt: a real-time simulation tool for studying real-world cyberattacks in the laboratory. *In Handbook of Computer Networks and Cyber Security*, 949-959.
8. Awad, S.W. (2020). A framework for improving information security using cloud computing. *International Journal of Advanced Research in Engineering and Technology*, 11(6).
9. Fan, Q. (2019). An exploratory study of cross border e-commerce (CBEC) in China: opportunities and challenges for small to medium size enterprises (SMEs). *International Journal of E-Entrepreneurship and Innovation (IJEEI)*, 9(1), 23-29.
10. Khurana, A.; and Mehra, J. (2015). E-commerce: Opportunities and challenges. *The International Journal of Business & Management*, 3(1), 1501-049.
11. Shahriari, S.; Shahriari, M.; and Gheiji, S. (2015). E-commerce and it impacts on global trend and market. *International Journal of Research* – Granthaalayah, 3(4).
12. Bhalekar, P.; Ingle, S.; and Pathak, K. (2014). The study of ecommerce. *Asian Journal of Computer Science and Information Technology*, 4(3).
13. Lim, E. (2014). Adoption of E-Commerce in Manila. *Proceedings from the DLSU Research Congress, Manila, Philippines*.

14. Nanehkaran, Y.A. (2013). An introduction to electronic commerce. *International Journal of Scientific & Technology Research,* 2(4).

15. Khoshnampour, M.; and Nosrati, M. (2011). An overview of E-commerce. *World Applied Programming,* 1(2).

16. Organisation For Economic Co-Operation and Development (OECD) (2015). Chapter 3. Approaches to The Protection of Trade Secrets. *Enquiries into Intellectual Property's Economic Impact*, 127–172.

17. Zwass, V. (1996). Electronic Commerce: Structures and Issues. *International Journal of Electronic Commerce*, 1(1) Available at: https://pdfs.semanticscholar.org/9f36/c5cea1838378b66b102c6afb996b77e78233.pdf

18. Chaffey, D. (2011). *Digital Business and E-commerce Management: Strategy, Implementation and Practice.* United Kingdom, Pearson.

19. Nemat, R. (2011). Taking a look at different types of e-commerce. *World Applied Programming,* 1(2), 100–104.

20. Manzoor, A. (2010). E-Commerce: An Introduction. Saarbrucken: Lambert Academic Publishing

21. Turban, E; King, D.; Lee J.K.; Liang, T.P.; and Turban D.C. (2015). Electronic Commerce. Switzerland: Springer International Publishing.

22. Thulani, D.; Tofara, C,; and Langton, R. (2010). Electronic Commerce Benefits and Adoption Barriers in Small and Medium Enterprises in Gweru Zimbabwe., *The Journal of Internet Banking and Commerce,* 15(1), 1-17.

23. Simpson, M.; and Docherty, A.J. (2004). E-commerce adoption support and advice for UK SMEs, *Journal of Small Business and Enterprise Development,* 11(3), 315–328.

24. Al-Qirim, Nabeel A. Y; and Brian J. Corbitt (2001). Determinants of innovation adoption in small to medium enterprises in New Zealand: an electronic commerce capability model. Retrieved October, 12 2019, from https://pdfs.semanticscholar.org/a875/4bea4dd2925337ce615354576736a30536f9.pdf

25. Alam, S.S.; Ali, M.Y.; and Jani, M.F.M. (2011). An Empirical Study of Factors Affecting Electronic Commerce Adoption among SMES in Malaysia. *Journal of Business Economics and Management,* 12(2), 375–399.

26. Andrijcic, E.; and Horowitz, B., (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk analysis*, 26(4), 907-923.

27. Phillips, C.; and Meeker, M. (2000). The B2B Internet Report - Collaborative Commerce. Retrieved April, 16, 2019 from www.msdw.com/mrchuck

28. Schwab, K. (2016). *The Fourth Industrial Revolution.* Geneva: World Economic Forum.

29. Rahman, K. M (2018). A Narrative Literature Review and E-Commerce Website Research, *EAI Endorsed Transactions on Scalable Information Systems*, 5(17), 1–11.

30. Loebbecke, C.; van Fenema, P. C.; and Powell, P. (2016). Managing inter-organizational knowledge sharing. *The Journal of Strategic Information Systems*, 25(1), 4–14.

31. Arrasvuori, J.; Liting, L.; and Kuusisto, J. (2014). Management of Confidential Business Information and Trade Secrets: Findings of an International Survey. *Proceedings of the 11th International Conference on Innovation and Management*, Vols I and Ii, 1323–1334.

32. Scott, B. (2018). The role of e-commerce in the Fourth Industrial Revolution. Retrieved May 10 2019 from https://www.digitalcommerce360.com/2018/01/11/role-e-commerce-fourth-industrial- revolution/

33. Falkenreck, C.; and Wagner, R. (2017). The Internet of Things – Chance and challenge in industrial business relationships. *Industrial Marketing Management*, 66,181–195.

34. Alsaad, A.; Mohamad, R.; & Ismail, N. A. (2017). The moderating role of trust in business to business electronic commerce (B2B EC) adoption. *Computers in Human Behavior*, 68, 157-169.

35. Ratnasingam, P. (2005). Trust in inter-organizational exchanges: a case study in business to business electronic commerce. *Journal of Decision Support Systems*, 39(3), 525–544.

36. Ying-Hueih Chen; Tzu-Pei Lin; David C. Yen (2014). How to facilitate inter-organizational knowledge sharing: The impact of trust. *Information & Management*, 51(5), 568-578.

37. Chang, T. et al. (2009). A case study for implementing a B2B collaborative information system: a textile case. *Journal of Manufacturing Technology Management*, 20(3), 330–347.

38. Schoenthaler, F.; Augenstein, D.; and Karle, T. (2015). Design and Governance of Collaborative Business Processes in Industry 4.0. Retrieved May 13, 2019 from http://ceur-ws.org/Vol- 1408/paper3-xoc-bpm.pdf

39. Harvey, S.; and Evans, D. (2016). Defending Against Cyber Espionage: The US Office of Personnel Management Hack as a Case Study in Information Assurance. *National Conference on Undergraduate Research*, North Carolina.

40. Penttinen, E. et al. (2018). What Influences Choice of Business-to-Business Connectivity Platforms? *International Journal of Electronic Commerce*, 22(4), 479–509.

41. Fosfuri, A.; and Rønde, T. (2004). High-tech clusters, technology spillovers, and trade secret laws. *International Journal of Industrial Organization*. North-Holland, 22(1), 45–65.

42. Chiara Verbano; Karen Venturini (2011). Development Paths of Risk Management: Approaches, Methods and Fields of Application. *Journal of Risk Research*, 14(5), 519-550.

43. Seyed M. Seyed H; Siamak N.; and Mohammad A. H. (2008). A gap analysis on the project risk management processes. *Kuwait Science Engineering Journal*, 35(1B), 217–234.

44. Fischer, E. A. (2016) *Cybersecurity Issues and Challenges: Cyberwarfare.* New York: Greenhaven Publishing.

45. Whitman, M. E.; & Mattord, H. J. (2021). *Principles of information security.* Cengage learning.

46. Brotby, W. K. (2009). *Information Security Governance : A Practical Development and Implementation Approach.* Hoboken, N.J.: John Wiley & Sons.

47. Von S. R. and Van N. J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. doi: 10.1016/j.cose.2013.04.004.

48. International Telecommunication Union (ITU) (2018). Guide to developing a national cybersecurity strategy. *Strategic Engagement in Cybersecurity. International Telecommunication Union (ITU).*

49. Humphreys, E. (2010) *Information Security Risk Management Handbook for ISO/IEC 27001.* UK: British Standard Institution.

50. Wheeler, E. (2011). Security risk management: building an information security risk management program from the ground up. Retrieved April 18, 2019 from http://ebookcentral.proquest.com.

51. Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, 40(1), 183-199.

52. Chapman, C. (1997). Project risk analysis and management - PRAM the generic process. *International Journal of Project Management* 15 (1997): 273-281.

53. Cherdantseva, Y.; and Hilton, J. (2013). A Reference Model of Information Assurance & Security. *International Conference on Availability, Reliability and Security,* 546–555.

54. Fenz, S. et al. (2014). Current challenges in information security risk management. *Journal of Enterprise Information Management,* 22(5), 410–430.

55. Ustundag, A; and Cevikcan, E. (2018). *Manufacturing Industry 4.0: Managing The Digital Transformation.* Switzerland: Springer Series in Advanced Manufacturing.

56. Hitpass, B; and Astudillo, H. (2019). Industry 4.0 Challenges for Business Process Management and Electronic- Commerce. *Journal of theoretical and applied electronic commerce research,* 14(1).

57. Kumar, R.; R.C.Tripathi; and M.D.Tiwari (2012). Trade Secrets Protection in Digital Environment: A Global Perspective. *International Journal of Economics & Management Sciences 2012 2:4. Management Journals*, 2(4).

58. Lionel B.; and Brad S. (2014). *Intellectual Property Law*. Oxford: Oxford University Press.

59. Soares, M. N.; and Kauffman, M. E. (2018). Intellectual Property Law in the Fourth Industrial Revolution: Trade Secrets Risks and Opportunities. *Revista Juridica*, 03(52), 199–224.

60. Bone, R. G. (1998). A New Look at Trade Secret Law: Doctrine in Search of Justification. *California Law Review*, 86(2), 243.

61. Collins Dictionary (2019) *Definition, Thesaurus and Translations.* Glasgow, Collins English Dictionary.

62. Lemley, M. A. (2008). The Surprising Virtues of Treating Trade Secrets as IP Rights. *Stanford Law Review*, 61(2).

63. Ritala, P. et al. (2013). Value creation and capture mechanisms in innovation ecosystems: a comparative case study. *International Journal of Technology Management*, 63(3/4), 244.

64. Centre for the Protection of National Infrastructure (CPNI) (2013). Insider data collection study- Report of man finding. Centre for the Protection of National Infrastructure (CPNI), 1–15.

65. Linton, K. (2016). The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research. *International Trade eJournal.*

66. Maskus, K. E. (2018). Fostering Innovation in Digital Trade. *Intellectual Property and Digital Trade in the Age of Artificial Intelligence and Big Data Global Perspectives and Challenges for the Intellectual Property System*, 5, 19–28.

67. Süli, D. F. (2019). Intellectual Property', in Electronic Enclosure, Housings and Packages. *Woodhead Publishing Series in Electronic and Optical Materials*

68. Giachetti, C.; and Lanzolla, G. (2016). Product Technology Imitation Over the Product Diffusion Cycle: Which Companies and Product Innovations do Competitors Imitate More Quickly? Long Range Planning. *Pergamon*, 49(2), 250–264.

69. Omid N.; and Patricia A.N. (2002). Industrial Espionage: The dark side of the "Digital Age". *Competitive Review: An International Business Journal*, 12(2), 96–101.

70. Fazzini, K. (2019). Huawei exec accused of stealing trade secrets from chip company CNEX. Retrieved May 31, 2019 from https://www.cnbc.com/2019/05/22/huawei-executive-accusetd-of-stealing-trade-secrets-from-axas- company-backed-by-microsoft-and-dell.html

71. Abd Jalil, J.; and Hassan, H. (2020). Protecting Trade Secret from Theft and Corporate Espionage: Some Legal and Administrative Measures. *International Journal of Business and Society*, 21.

72. Ezell, S.; and Cory, N. (2019). The Way Forward for Intellectual Property Internationally | ITIF. *Information Technology & Innovation Foundation.* Retrieved May 19, 2020, from https://itif.org/publications/2019/04/25/way-forward-intellectual-property-internationally/

73. Kohen, I (2018). Protecting Intellectual Property against Cyberattack. Ahead of the Threat. Retrieve August 19, 2020 from

https://www.csoonline.com/article/3245310/protecting-intellectual-property-against-cyberattack.html

74. Niebel, R.; de Martinis, L.; and Clark, B. (2018). The EU Trade Secrets Directive: all change for trade secret protection in Europe? *Journal of Intellectual Property Law & Practice*, 13(6), 445– 457.

75. Salamai, A. A. (2021). Feedback and User Behavior Trust and Reputation in Risk Management. *Journal of Computer Science and Information Systems*, *20* (4 April 2021).

76. Madan, S.; Pérez-Morón, J.; Chua, X. N.; Kee, D. M. H.; Chua, J.; Chua, K. Z.; and Vidal, L. D. S. (2022). Analysis of the Shopee's Strategies to Succeed in the Global E-commerce Market: Malaysia Case. *International journal of Tourism and hospitality in Asia Pasific (IJTHAP)*, *5*(1), 34-48.

77. Giuffrida, M.; Jiang, H.; and Mangiaracina, R. (2021). Investigating the relationships between uncertainty types and risk management strategies in cross-border e-commerce logistics. *The International Journal of Logistics Management*, *32*(4), 1406-1433.

78. Zhang, X.; Lu, J.; and Li, D. (2020). Confidential information protection method of commercial information physical system based on edge computing. *Neural Computing and Applications*, 33(3), 897–907. https://doi.org/10.1007/s00521-020-05272-0

79. Wijaya, T. (2022). A Bibliometric Study of E-commerce Reputation. *The Journal of Industrial Distribution & Business*, 13(6), 1-7.