Trust and Risk Management Interplay: A Review in the Digital Context

Julija Saveljeva[a]
Department of Economics and Finance, BA School of Business and Finance, K. Valdemara Street 161, Riga, Latvia

Keywords: Risk Management, Trust, Digital Environment, Systematic Literature Review, Trust Integration, Perceived Risk.

Abstract: This paper provides a comprehensive overview of previous studies on the relationship between trust and risk management in the digital environment, highlighting multiple ways trust elements can enhance risk management practices. PRISMA 2020 methodology was used to perform this analysis, and 281 papers retrieved from Scopus and Web of Science databases were examined. 45 papers selected based on specific inclusion and exclusion criteria formed the foundation of this study.
The main research findings are: 1. A strong, mutual relationship exists between trust and perceived risk. Increased trust reduces perceived risk and leads to more user adoption and engagement with digital services. In turn, higher perceived risk lowers trust and discourages the adoption. 2. Trust integration into assessments for decision-making improves risk management by enhancing accuracy, fairness, and uncertainty handling in online environments. 3. Since the trust is dynamic by its nature, its regular reassessments are important. 4. Furthermore, even when cooperating with trusted services and platforms, it is necessary to continuously monitor providers to avoid over-reliance risks.

1 INTRODUCTION

The relationship between trust and risk has long been a research subject, highlighting their inherent relationship (Jøsang & Presti, 2004). This was also confirmed by a search using the keywords "risk management" AND "trust" limited to article titles, abstracts, keywords and articles and conference papers in the Scopus (Elsevier, n.d.) database in July 2024, which provided 2068 papers meeting these criteria. According to the analysed documents, interest in the topic started to appear in the early 1990s, with a wave of growth in 2004 and increased interest since 2020, as illustrated in Figure 1.

In recent years, the European Union has increasingly emphasised regulatory measures to enhance risk management in the digital environment (European Commission, 2022b, 2022a). However, the effectiveness of the risk management system within the European context remains a relevant question (Ghazieh & Chebana, 2021), raising the issue of an effective risk management framework (Luther et al., 2023). At the same time, with increased cybersecurity threats, traditional risk mitigation actions are losing their effectiveness (Aslan et al., 2023).

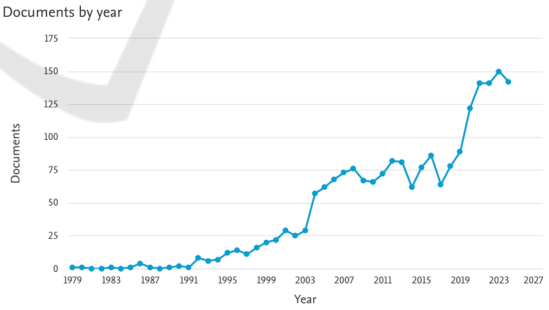

Figure 1: Identified publications distribution by the years.

Therefore, the research on the possibility of enhancing risk management practices in the digital environment by incorporating the trust element is becoming actual. This study aims to provide a comprehensive overview of the previous studies on the relationship between trust and risk management in

[a] https://orcid.org/0009-0007-2385-5852

Saveljeva, J.
Trust and Risk Management Interplay: A Review in the Digital Context.
DOI: 10.5220/0013344200003956
In *Proceedings of the 7th International Conference on Finance, Economics, Management and IT Business (FEMIB 2025)*, pages 189-196
ISBN: 978-989-758-748-1; ISSN: 2184-5891

the digital environment. To fulfil this aim, the following research questions were formulated:

RQ1: What industries are studied within the scope of trust and risk management relationships in the digital environment?

RQ2: What is the main focus of the research on trust and risk management in a digital environment?

RQ3: What are the main findings on the relationship between trust and risk management in the digital environment?

RQ4: How can trust elements be incorporated into risk management practices?

2 RESEARCH DESIGN AND METHODOLOGY

A systematic literature review was conducted following the PRISMA 2020 (Page et al., 2021) methodology to analyse the relationship between trust and risk management in a digital environment.

Scopus (Elsevier, n.d.) and Web of Science (WoS) (Clarivate, n.d.) - two leading scientific databases (Pranckutė, 2021; Zhu & Liu, 2020) - were used for this research to ensure that the latest sources are covered and to avoid indexation bias. The search included the keywords trust AND "risk management" AND ("digital" OR "online" OR "cyber"). It was limited to paper titles, abstracts, keywords, and document types such as articles and conference papers. The search based on these parameters was conducted on 30.06.2024 in Scopus (n=272) and on 07.07.2024 in WoS (n=55). Removing the duplicates, 281 unique papers were identified for further review.

The first relevance check phase included reading and reviewing the abstracts, using the following inclusion criteria: discussing risk management and trust correlation in a digital, cyber, or online environment. In turn, the exclusion criteria were a focus on trust as a technical element of the solution and a trust management topic from the perspective of computer science.

Based on these criteria, 85 papers qualified for the full-text paper review. Out of this scope, nine papers were unavailable to the author, and 31 papers were excluded from the analysis based on the previously described criteria. As a result, 45 papers (22 conference papers and 23 journal articles) were included in further bibliographical and contextual analysis.

3 RESEARCH FINDINGS

3.1 Bibliometric Analysis Results

A total of 141 authors from 21 countries (based on their affiliations) have shown interest in risk management and trust in digital settings. The most represented countries are the United Kingdom (n=9), the United States of America (n=8), China (n=7), India (n=4), and Tunisia (n=3).

The bibliographical analysis identified an increased interest in the topic by two authors: Lifen, L.(Lifen, 2008a, 2008b), who published two conference papers, and Youssef, S.B.H., and Boudriga, N. (Hadj Youssef & Boudriga, 2021; Youssef & Boudriga, 2022), who contributed with a conference paper and a scientific article. Furthermore, two journals were notable for their contributions to the topic: *Online Information Review*, which published three articles, and *Computers in Human Behavior*, which published two articles.

Author keywords (n=171) from the identified papers were analysed. Focusing on the keywords that appeared three or more times, the most common were, as expected, "trust" (n=19) and "risk management" (n=11). Other frequently appearing keywords included "electronic commerce" and "e-commerce" (n=7), as well as "perceived risk" and "risk perception" (n=6). The keywords "privacy", "cyber-physical systems", and "cybersecurity" each appeared three times. Such distribution provides insights into the most popular research sector, highlights the previous research focus on the correlation between trust and risk perception and emphasises cyber security as a component of digital trust.

Afterwards, VOSviewer software (*VOSviewer*, n.d.) was used to perform a full-count co-occurrence keyword analysis and identify clusters. 24 keywords appearing more than twice were included in the study, resulting in six identified clusters depicted in Figure 2, each with a distinct focus:

- **Green**: Focuses on risk management in contexts where human factors, security, and privacy are critical.
- **Yellow**: Connects perceived risk with user adoption and behavioural intention frameworks like UTAUT2 (Unified Theory of Acceptance and Use of Technology).
- **Red**: Centres on cyber risks in the context of social media and broader cyber security concerns.

- **Purple**: Focuses on cyber-physical systems and their associated information security risks, emphasising risk analysis.
- **Blue**: Explores the intersection of risk management and emerging technologies like blockchain, particularly in e-commerce.

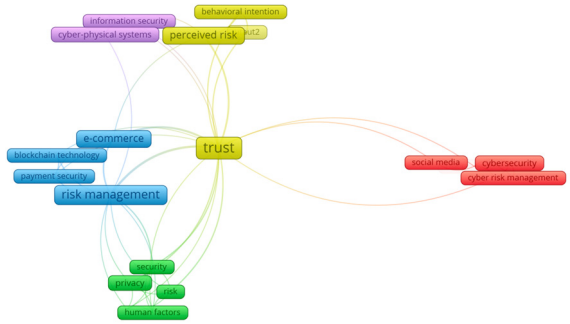

Figure 2: Keywords co-occurrence clustering results.

3.2 Context Analysis Results

Further context analysis was applied to the selected studies to address the formulated research questions.

3.2.1 Industries Studied Within Trust and Risk Management Relationship Scope in the Digital Environment

Based on the previously conducted keyword analysis, one of the most researched areas is e-commerce. Nevertheless, context analysis revealed a different proportion of such studies.

The financial industry was reviewed the most, with ten papers devoted to the research of trust and risk management. The general focus was on digital services, often with a more narrow focus on payment solutions (Hadj Youssef & Boudriga, 2021; Youssef & Boudriga, 2022), investments (Putri et al., 2022; Sun et al., 2016), banking (Kaur & Arora, 2021; G. Liu et al., 2008), and lending (Amalia et al., 2019).

E-commerce was the focus of nine articles, for example (Chang & Chen, 2008; Chong & Abawajy, 2007; San Martín & Camarero, 2009).

Four papers each concentrated on information technology (Mollazehi et al., 2024; Rogers et al., 2016; Shaytura et al., 2021; Terry Morris et al., 2020) and different aspects of social media (Abdul-Rahman & Hailes, 2000; Hansen et al., 2018; M. Liu et al., 2021; X. A. Zhang & Cozma, 2022). Two papers examined trust and risk management from an agricultural sector perspective (Carter, 2022; Y. Zhang et al., 2016), and one focused on healthcare (Ksibi et al., 2023), maritime (Larsen et al., 2022), oil and gas (Oudina et al., 2024), communication (Tehrani et al., 2020) and hospitality (Hong & Kim, 2024). The other eleven articles were not concentrated on any particular industry.

3.2.2 Main Focus of the Research on Trust and Risk Management in a Digital Environment

Five groups can be identified when analysing the research focuses of the papers. The papers' distribution between the groups is based on their primary focus. Nevertheless, it is subjective since the thematic aspects discussed are often interrelated.

1. Research on perceived risk, trust, and consumer behaviour. This largest thematical group (n=15, 33%) focuses on how perceived risk and trust influence consumer behaviour, technology acceptance, and decision-making in online environments such as e-commerce, online banking, social media, and digital platforms.

For example, the research of J.M. Hansen, G. Saridakis and V. Benson (2018) examines how perceived risk, trust, and the interaction between elements of the Technology Acceptance Model (TAM) and Theory of Planned Behavior (TPB) influence consumers' intentions to use social networking services for transactions.

2. Research on trust management models, frameworks, and assurance. The main focus of this group (n=14, 31%) is on developing and analysing models and frameworks for trust management, risk management, and assurance across various systems, including e-commerce, cyber-physical systems, and virtual communities. These studies aim to enhance the reliability and security of digital systems by proposing methodologies to manage trust and reduce vulnerabilities.

As an example, the study by Li et al. (2023) establishes a novel conflict-eliminating framework with a dynamic trust risk management mechanism to manage trust risks and promote consensus.

3. Research on trust and risk in emerging technologies. The aim of these papers (n=7, 16%) is to study the impact of emerging technologies like blockchain, artificial intelligence, and digital transformation on trust and risk management practices. They analyse how these technologies can enhance security, reduce risks, and build trust in digital transactions and infrastructures.

As an illustration, the study by Shaytura may be mentioned (Shaytura et al., 2021) since it aimed to analyse the possibilities of using blockchain technology to ensure technogenic safety and risk management.

4. Research on human factors in cybersecurity and trust. This group (n=6, 13%) explores how human factors, such as individual differences, social engineering, and behavioural aspects, affect trust and risk-taking in cybersecurity contexts.

For example, the goal of Bishop et al. (2020) was to determine which specific individual differences influence cybersecurity behaviours to create tailored interventions that can be used within businesses to mitigate human susceptibility to cyber threats.

5. Research on privacy concerns and trust. This smallest category of papers (n=3, 7%) investigates privacy issues and their relationship with trust and risk in digital environments. As an illustration, the paper of Oudina et al. (2024) examines trust concerns. It identifies the key trust-related fears and needs that have shaped the development of trust quality in cyber-physical systems from the early design phase.

3.2.3 Main Findings on the Relationship Between Trust and Risk Management in the Digital Environment

Analysing the results and conclusions of the analysed papers, one of the main findings is that trust and perceived risk are closely interrelated and mutually influence each other. Increased trust mitigates perceived risk, enhancing user acceptance and positive behavioural intentions toward digital services (Aldás-Manzano et al., 2009; Ksibi et al., 2023; San Martín & Camarero, 2009). Opposingly, high perceived risk can reduce trust levels, slowing down adoption (Putri et al., 2022).

Furthermore, the findings suggest that individuals are more likely to engage in risk-taking behaviours when they trust the source, advisor, or platform. Trust influences decisions in financial investments, social engineering contexts, sharing economy platforms, and information sharing on digital platforms (Hansen et al., 2018; Mollazehi et al., 2024; Sun et al., 2016).

An important identified aspect is that excessive trust in systems, suppliers, or advanced technologies can result in overconfidence, less attention to risks, and greater vulnerability. This overreliance may lead individuals to underestimate potential threats and neglect necessary precautions (Bishop et al., 2020; Larsen et al., 2022; Terry Morris et al., 2020).

In the analysed papers were numerous positive confirmations of adopting assurance frameworks and emerging technologies like blockchain to enhance trust by reducing uncertainties and transaction risks. These were confirmed to improve risk management practices across various sectors (Ghaffarian et al., 2023; Hampton et al., 2021; Shaytura et al., 2021).

It was proven that providing transparent, explainable information and engaging in effective risk communication enhance trust and help manage public risk perceptions (Ghaffarian et al., 2023; Windelberg, 2016). When trust is low, individuals adopt risk-averse strategies, such as avoiding new or complex tasks, technologies, or interactions (McInnis et al., 2016; Setty, 2018).

Incorporating trust assessments into decision-making processes and identifying trust concerns enhance the effectiveness of risk management models. Trust-based approaches lead to more accurate predictions, fairer systems, and better handling of uncertainties in online environments (Oudina et al., 2024; Yuan et al., 2010).

Finally, an important finding confirmed in a digital environment is that social, cultural, and individual factors significantly affect trust development and risk perceptions. Effective risk management requires understanding these influences and customising approaches to different cultural contexts to build trust and address specific concerns (Bhattacharya & Saha, 2004; Windelberg, 2016).

3.2.4 Trust Element Incorporation into Risk Management Practices

Previous studies reveal numerous ways to incorporate trust into risk management practices in the digital environment. As a service provider, building and demonstrating trust in a digital environment helps to address the risk concerns of the customer or user. It can be achieved through:

- Strengthening security protocols and safeguarding user data (San Martín & Camarero, 2009).
- Openly sharing information about risk management practices and system capabilities (Ghaffarian et al., 2023; Tehrani et al., 2020).
- Tailoring communication to align with different user groups' cultural norms and expectations (Bhattacharya & Saha, 2004).
- Enhancing transparency and explainability in the data management (Li et al., 2023) of used technologies.
- Involving individuals in developing and improving digital services to build trust and address their concerns (McInnis et al., 2016; Y. Zhang et al., 2016).

In turn, the trust element might be integrated into the organisation's internal risk-management practices:

- Trust metrics might be integrated into risk assessment practices using trust scoring

systems that evaluate partners, suppliers, and users (Abdul-Rahman & Hailes, 2000; Yuan et al., 2010).
- These metrics could be supported with independent audits and certifications to verify the security and reliability of services or systems (Hafver et al., 2021).
- The usage of services that include trusted emerging technology by design, such as blockchain, might be considered (Shaytura et al., 2021).

While integrating these trust elements into internal risk management practices, it is essential to regularly re-assess the trust levels, as trust is dynamic (Oudina et al., 2024). Even with trusted services and platforms, it is essential to keep monitoring the providers and not over-trusting them (Larsen et al., 2022).

4 DISCUSSION AND CONCLUSIONS

The results of the industry analysis previously studied in the context of trust and risk management relationships are unsurprising since the topic of trust and trustworthiness in the financial sector has been crucial for decades (Litovtseva et al., 2022), and interest in the subject within the digital environment seems natural.

The research on trust as an element of the risk management framework is not dominating in the selected papers' range, keeping this topic relevant for future research. Nevertheless, the findings of these papers already prove the possibility of using trust and its assessed level to enhance risk management frameworks in a digital environment. Moreover, this study summarises overall directions that might be considered while integrating the trust element into the organisation's risk management practices.

Further research on this topic might be devoted to developing a risk management framework and standardised decision-making processes, including integrated trust metrics, and exploring the methods for assessing and constantly monitoring trust levels in the digital context.

ACKNOWLEDGEMENTS

This research is supported by the grant received within a project nr. 5.2.1.1.i.0/2/24/I/CFLA/007 "Internal and External Consolidation of the University of Latvia".

Since the author's first language is not English, the paper's text was proofread using the Open AI GPT-4o model (OpenAI, 2025) and Grammarly (Grammarly, n.d.) to ensure it had no orthographical or grammar mistakes. After applying these services/tools, the text was reviewed, and the author took full responsibility for the publication's content.

REFERENCES

Abdul-Rahman, A., & Hailes, S. (2000). Supporting trust in virtual communities. Proc. Annu. Hawaii Int. Conf. Syst. Sci., 2000-January. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85094162508&partnerID=40&md5=07a90713207 ea1a535184152f578700b

Aldás-Manzano, J., Lassala-Navarré, C., Ruiz-Mafé, C., & Sanz-Blas, S. (2009). Key drivers of internet banking services use. Online Information Review, 33(4), 672–695. Scopus. https://doi.org/10.1108/14684520910985675

Amalia, N., Dalimunthe, Z., & Triono, R. A. (2019). The effect of lender's protection on online peer-to-peer lending in Indonesia. In Soliman K.S. (Ed.), Proc. Int. Bus. Inf. Manag. Assoc. Conf., IBIMA: Educ. Excell. Innov. Manag. Vis. (WOS:000510675601048; pp. 6056–6066). International Business Information Management Association, IBIMA; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85074066697&partnerID=40&md5=f368ac8813189c826339722a0eed9920

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333

Bhattacharya, K. K., & Saha, S. (2004). Trust dimensions in E-retailing: A strategic exploration. IEEE Int Eng Manage Conf, 2, 825–828. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-17644387597&partnerID=40&md5=3e39f71a22f513246ea3b98a9bd19c6b

Bishop, L. M., Morgan, P. L., Asquith, P. M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020). Examining human individual differences in cyber security and possible implications for human-machine interface design. In Moallem A. (Ed.), Lect. Notes Comput. Sci.: Vol. 12210 LNCS (pp. 51–66). Springer; Scopus. https://doi.org/10.1007/978-3-030-50309-3_4

Carter, M. R. (2022). Can digitally-enabled financial instruments secure an inclusive agricultural transformation? Agricultural Economics (United Kingdom), 53(6), 953–967. Scopus. https://doi.org/10.1111/agec.12743

Chang, H. H., & Chen, S. W. (2008). The impact of online store environment cues on purchase intention: Trust and perceived risk as a mediator. Online Information Review, 32(6), 818–841. Scopus. https://doi.org/10.1108/14684520810923953

Chong, S.-K., & Abawajy, J. H. (2007). Feedback credibility issues in trust management systems. Proc Int Conf Multimedia Ubiquitos Eng, 387–394. Scopus. https://doi.org/10.1109/MUE.2007.130

Clarivate. (n.d.). Web of Science. Retrieved 18 November 2024, from https://www.webofscience.com

Elsevier. (n.d.). Scopus. Retrieved 18 November 2024, from https://www.scopus.com

European Commission. (2022a). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Commission. (2022b). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554

Ghaffarian, S., Taghikhah, F. R., & Maier, H. R. (2023). Explainable artificial intelligence in disaster risk management: Achievements and prospective futures. International Journal of Disaster Risk Reduction, 98. Scopus. https://doi.org/10.1016/j.ijdrr.2023.104123

Ghazieh, L., & Chebana, N. (2021). The effectiveness of risk management system and firm performance in the European context. Journal of Economics, Finance and Administrative Science, 26(52), 182–196. https://doi.org/10.1108/JEFAS-07-2019-0118

Grammarly. (n.d.). [Computer software]. Grammarly. https://www.grammarly.com/

Hadj Youssef, S. B., & Boudriga, N. (2021). A Robust and Efficient Micropayment Infrastructure Using Blockchain for e-Commerce. In Arai A. (Ed.), Intell. Comput. - Proc. Comput. Conf. (WOS:000839363100058; Vol. 284, pp. 825–839). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-030-80126-7_58

Hafver, A., Ferreira, C., Agrell, C., McGeorge, D., Hektor, E. A., Pedersen, F. B., van der Meulen, M., Haugen, O. I., Eldevik, S., & Myhrvold, T. (2021). On the meaning of assurance. In Castanier B., Cepin M., Bigaud D., & Berenguer C. (Eds.), Proc. Eur. Saf. Reliab. Conf. (pp. 3288–3295). Research Publishing, Singapore; Scopus. https://doi.org/10.3850/978-981-18-2016-8_465-cd

Hampton, C., Sutton, S. G., Arnold, V., & Khazanchi, D. (2021). Cyber supply chain risk management: Toward an understanding of the antecedents to demand for assurance. Journal of Information Systems, 35(2), 37–60. Scopus. https://doi.org/10.2308/ISYS-19-050

Hansen, J. M., Saridakis, G., & Benson, V. (2018). Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. Computers in Human Behavior, 80, 197–206. Scopus. https://doi.org/10.1016/j.chb.2017.11.010

Hong, I. B., & Kim, M. (2024). Understanding the influence of a host's guest perceptions on sharing intention on the airbnb platform: A signaling theory perspective. Telematics and Informatics, 87. Scopus. https://doi.org/10.1016/j.tele.2023.102096

Jøsang, A., & Presti, S. L. (2004). Analysing the Relationship between Risk and Trust. In C. Jensen, S. Poslad, & T. Dimitrakos (Eds.), Trust Management (Vol. 2995, pp. 135–145). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-24747-0_11

Kaur, S., & Arora, S. (2021). Role of perceived risk in online banking and its impact on behavioral intention: Trust as a moderator. Journal of Asia Business Studies, 15(1), 1–30. Scopus. https://doi.org/10.1108/JABS-08-2019-0252

Ksibi, S., Jaidi, F., & Bouhoula, A. (2023). A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach. Proc. Int. Conf. Syst. Syst. Eng.: Socio-Tech. Perspec., SoSE, 28(1), 107–127. Scopus. https://doi.org/10.1007/s11036-022-02042-1

Larsen, M. H., Lund, M. S., & Bjørneseth, F. B. (2022). A model of factors influencing deck officers' cyber risk perception in offshore operations. Maritime Transport Research, 3. Scopus. https://doi.org/10.1016/j.martra.2022.100065

Li, M., Xu, Y., Liu, X., Chiclana, F., & Herrera, F. (2023). A Trust Risk Dynamic Management Mechanism Based on Third-Party Monitoring for the Conflict-Eliminating Process of Social Network Group Decision Making. IEEE Transactions on Cybernetics, 53(6), 3399–3413. Scopus. https://doi.org/10.1109/TCYB.2022.3159866

Lifen, L. (2008a). Trust derivation and recommendation management in a trust model. Int. Conf. Intelligent Inf. Hiding Multimedia Signal Process., IIH-MSP, 219–222. Scopus. https://doi.org/10.1109/IIH-MSP.2008.18

Lifen, L. (2008b). Trust derivation and transitivity in a recommendation trust model. Proc. - Int. Conf. Comput. Sci. Softw. Eng., CSSE, 3, 770–773. Scopus. https://doi.org/10.1109/CSSE.2008.484

Litovtseva, V. Ye., Vasilyeva, T. A., & Brychko, M. M. (2022). TRUST IN THE FINANCIAL SECTOR: A BIBLIOMETRIC ANALYSIS (1967–2020). Academic Review, 2(57), 87–97. https://doi.org/10.32342/2074-5354-2022-2-57-7

Liu, G., Huang, S.-P., & Zhu, X.-K. (2008). User acceptance of Internet banking in an uncertain and risky environment. Renmin University of China, 381–386. Scopus. https://doi.org/10.1109/ICRMEM.2008.82

Liu, M., Bi, J., Yang, J., Qu, S., & Wang, J. (2021). Social media never shake the role of trust building in relieving

public risk perception. Journal of Cleaner Production, 282. Scopus. https://doi.org/10.1016/j.jclepro.2020.124442

Luther, B., Gunawan, I., & Nguyen, N. (2023). Identifying effective risk management frameworks for complex socio-technical systems. Safety Science, 158, 105989. https://doi.org/10.1016/j.ssci.2022.105989

McInnis, B., Cosley, D., Nam, C., & Leshed, G. (2016). Taking a hit: Designing around rejection, mistrust, risk, and workers' experiences in Amazon Mechanical Turk. Conf Hum Fact Comput Syst Proc, 2271–2282. Scopus. https://doi.org/10.1145/2858036.2858539

Mollazehi, A., Abuelezz, I., Barhamgi, M., Khan, K. M., & Ali, R. (2024). Do Cialdini's Persuasion Principles Still Influence Trust and Risk-Taking When Social Engineering is Knowingly Possible? In Araújo J., de la Vara J.L., Santos M.Y., & Assar S. (Eds.), Lect. Notes Bus. Inf. Process. (Vol. 513, pp. 273–288). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-59465-6_17

OpenAI. (2025). ChatGPT: An AI Language Model [Computer software]. https://chatgpt.com/

Oudina, Z., Derdour, M., Dib, A., & Yaakoubi, M. A. (2024). Identifying and Addressing Trust Concerns in Cyber-Physical Systems for the Oil and Gas Industry. Ingenierie Des Systemes d'Information, 29(2), 469–478. Scopus. https://doi.org/10.18280/isi.290208

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. Systematic Reviews, 10(1), 89. https://doi.org/10.1186/s13643-021-01626-4

Pranckutė, R. (2021). Web of Science (WoS) and Scopus: The Titans of Bibliographic Information in Today's Academic World. Publications, 9(1), 12. https://doi.org/10.3390/publications9010012

Putri, N., Yuliati, E., Mulyono, K., Rahman, Y., & Astuti, D. (2022). The Effect of Perceived Risk on Customer's Behavioral Intention of Digital Gold Platform: The Moderating Role of Trust. University of Indonesia. ICE-BEES 2021. https://doi.org/10.4108/eai.27-7-2021.2316918

Rogers, R., Apeh, E., & Richardson, C. J. (2016). Resilience of the Internet of Things (IoT) from an Information Assurance (IA) perspective. SKIMA - Int. Conf. Softw., Knowl., Inf. Manag. Appl., 110–115. Scopus. https://doi.org/10.1109/SKIMA.2016.7916206

San Martín, S., & Camarero, C. (2009). How perceived risk affects online buying. Online Information Review, 33(4), 629–654. Scopus. https://doi.org/10.1108/14684520910985657

Setty, E. (2018). Young People's Attributions of Privacy Rights and Obligations in Digital Sexting Culture. International Journal of Communication, 12, 4533–4552. Scopus.

Shaytura, S. V., Olenev, L. A., Nedelkin, A. A., Minitaeva, A. M., Ordov, K. V., & Feoktistova, V. M. (2021). Blockchain in Technogenic Safety and Risk Management. International Journal of Emerging Technology and Advanced Engineering, 11(12), 72–78. Scopus. https://doi.org/10.46338/ijetae1221_08

Sun, Q., Gibbert, M., Hills, T. T., & Nowak, E. (2016). Are Financial Advisors Money Doctors or Charlatans? Evidence on Trust, Advice, and Risk Taking in Delegated Asset Management. In Papafragou A., Grodner D., Mirman D., & Trueswell J.C. (Eds.), Proc. Annu. Meet. Cogn. Sci. Soc., CogSci (pp. 895–900). The Cognitive Science Society; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85139186557&partnerID=40&md5=bc9e52309734c3317c9571925c412f27

Tehrani, P. F., von Kalckreuth, N., & Lamprecht, S. (2020). Toward an integrative model of trust for digital emergency communication. In Hughes A.L., McNeill F., & Zobel C.W. (Eds.), Proc. Int. ISCRAM Conf. (Vols 2020-May, pp. 1012–1021). Information Systems for Crisis Response and Management, ISCRAM; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85118609002&partnerID=40&md5=b95f1d5c7b359a237c0d458392574811

Terry Morris, A., Maddalon, J. M., & Miner, P. S. (2020). On the moral hazard of autonomy. AIAA IEEE Dig Avionics Syst Conf Proc, 2020-October. Scopus. https://doi.org/10.1109/DASC50938.2020.9256682

VOSviewer. (n.d.). VOSviewer. Retrieved 26 April 2024, from https://www.vosviewer.com//

Windelberg, M. (2016). Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection, 12, 4–11. Scopus. https://doi.org/10.1016/j.ijcip.2015.11.003

Youssef, S. B. H., & Boudriga, N. (2022). A resilient micro-payment infrastructure: An approach based on blockchain technology. Intell. Comput. - Proc. Comput. Conf., 49(1). Scopus. https://doi.org/10.48129/KJS.V49I1.10578

Yuan, D., Lu, T., Yang, X., & Yan, L. (2010). A theory analysis and model research on e-commerce credit risk management. Proc. Int. Conf. E-Bus. E-Gov., ICEE, 2006–2009. Scopus. https://doi.org/10.1109/ICEE.2010.507

Zhang, X. A., & Cozma, R. (2022). Risk sharing on Twitter: Social amplification and attenuation of risk in the early stages of the COVID-19 pandemic. Computers in Human Behavior, 126. Scopus. https://doi.org/10.1016/j.chb.2021.106983

Zhang, Y., Zhang, Z., & Ren, J. (2016). Transform farming with the help of social media a pioneering Chinese Community Supported Agriculture (CSA) farm and its micro blog usage. Pac. Asia Conf. Inf. Syst., PACIS - Proc. Pacific Asia Conference on Information Systems, PACIS 2016 - Proceedings. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85011022648&partnerID=40&md5=a2371fee33eff1d4fb8b91ea1403d001

Zhu, J., & Liu, W. (2020). A tale of two databases: The use of Web of Science and Scopus in academic papers. Scientometrics, 123(1), 321–335. https://doi.org/10.1007/s11192-020-03387-8