The Journal of Society and Media, October 2025, Vol. 9(2) 409-437
https://journal.unesa.ac.id/index.php/jsm/index
E-ISSN 2580-1341 and P-ISSN 2721-0383
Accredited *KEMENRISTEK/ BRIN No.148/M/KPT/2020*
DOI: 10.26740/jsm.v9n2.p409-437

Mapping the Impact of Digital Maturity on Cyber Resilience: A Bibliometric Analysis

Aulia Kartika Putri[1], Achmad Nurmandi[2*], Herman Lawelai[3], Muhammad Younus[4]
[1,2] Muhammadiyah University of Yogyakarta, Yogyakarta , Indonesia
[3]Muhammadiyah University of Buton, Baubau , Indonesia
[4]TPL Logistics Pvt Ltd, Karachi, Pakistan

Abstract
Rapid digital transformation has prompted organisations to improve digital maturity in response to increasingly complex cybersecurity challenges. This research aims to explore the relationship between digital maturity and the effectiveness of data security measures, with a bibliometric approach to analyze trends, patterns and gaps in related literature. Based on the literature review, digital maturity reflects the level of digital technology adoption integrated with organisational strategy and culture, which is shown to have a significant impact on strengthening data security measures. This study used a bibliometric analysis method based on data from Scopus, involving 315 documents analyzed with VOSviewer and RStudio software to visualize trends and relationships between key variables. The results show that organizations with high digital maturity tend to be more capable of implementing effective data security measures, such as encryption, multi-factor authentication, and cybersecurity frameworks. In addition, the adoption of technologies such as blockchain and artificial intelligence (AI) also contributes to increased resilience against cyber threats. However, the gap between theory and real applications remains a challenge, with the need for more applicable and contextualized models. This research provides important insights for policymakers and practitioners to support a secure and sustainable digital transformation.

Keywords: *Digital Maturity, Cybersecurity, Digital Transformation, Blockchain, Artificial Intelligence*

Paper type: *Research paper*

***Corresponding author**: nurmandi_achmad@umy.ac.i
Received: 22-01-2025; Received in Revised From 22-03-2025; Accepted: 04-10-2025; Available Online: 07-10-2025

Cite this document: Putri, Aulia Kartika, Achmad Nurmandi, Herman Lawelai, and Muhammad Younus. (2025). *Mapping the Impact of Digital Maturity on Cyber Resilience: A Bibliometric Analysis. The Journal of Society and Media,* 9(2), 409–437. DOI: 10.26740/jsm.v9n2.p409-437.

INTRODUCTION

The ongoing digital evolution is driving paradigm shifts in mindsets, behaviour patterns, and social attitudes, giving rise to significant opportunities and challenges that require effective management (Dube and Mohanty 2020). In the near future, there will be a clear demand for Digital Creative Abilities (DCA), which include digital competencies and human capabilities such as problem solving, strategic and creative thinking, and emotional intelligence (Canina and Bruno 2021). The development of these competencies is critical in achieving Digital Maturity, which signifies the capacity to adapt continuously to the evolving digital environment, utilize digital technologies to meet human needs, and foster collaboration.

Advances in information technology, computing capabilities, and communication networks have facilitated the collection and distribution of large amounts of multimedia data, which is now readily available for consumer and enterprise applications (Shyu et al. 2007), to enhance digital maturity, it is imperative to encourage the dissemination of technology co-creation opportunities on a broader scale (Khmeleva and Czegledy 2021). The complexity and interdisciplinary nature of the digital technology co-creation process for regional development is a source of complexity (Zhang, Liao, and Zhou 2021).

Today's digital collaboration characterized by the proliferation of sophisticated and widespread cybersecurity threats, poses considerable challenges to the secure operation of Information and Communication Technology (ICT) and ICT-based services (Bahuguna, Bisht, and Pande 2019) . To protect national interests and maintain public trust in ICT services, all countries must ensure that entities under their jurisdiction have adequate capabilities to effectively counteract cyber threats, thus many countries have adopted various measures and expended substantial resources to enhance the cybersecurity preparedness of organizations within their respective cyber ecosystems (O'Brien et al. 2024; Ogwueleka and Aniche 2021).

In the context of the proliferation of multimedia data and the growing demand for multimedia applications, there is an urgent need for reliable and efficient tools and techniques for multimedia content analysis and retrieval, as well as for secure media streaming, distribution and communication (Heitzenrater 2006; Nasutra,

Setiyoko, and Moro Sundjaja 2023; Polychronaki et al. 2024). Despite much investment in research, these aspects are still in an underdeveloped state, with many unresolved issues. Maturity criteria have been proposed to categorize the digital twin, with digital technologies predominantly distributed across the maturity scale (Korovin 2022).

Data or information security in today's digital era is a crucial thing that needs to be considered by every organisation (Sulistyowati, Handayani, and Suryanto 2020) . Organisational information management is one of the components in realising Good Corporate Governance(Okae, Andoh-Baidoo, and Ayaburi 2019; Yulianto et al. 2023). The measure of an adequate level of protection is an indicator of the cybersecurity awareness aspect of the organisation's business processes in the short, medium and long term, especially in areas related to information and communication technology (ICT)(Bahuguna et al. 2019; Blum 2020; Mayhew and Jahankhani 2020; Möller and Haas 2024). To make this happen, an appropriate security standard is needed and follows its needs to help organisations know the level of cybersecurity maturity in protecting their information security.

Estonia is an important case study in successfully utilising digital maturity to improve its cybersecurity (Alatalu 2019). Through the 'e-Estonia' initiative, the country has developed an integrated digital system that includes digital identity, electronic governance and advanced data protection. Following a significant cyberattack in 2007, Estonia made substantial investments in cybersecurity infrastructure, including the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn(Marican et al. 2024) . The implementation of these initiatives has elevated Estonia to the forefront of digital transformation and cybersecurity advancement.

South Africa has recently embarked on a digital transformation process; however, the implementation of these initiatives remains limited. The public sector in South Africa exhibits a low level of digital maturity, as evidenced by a significant reliance on manual systems and paper-based processes(van Rayne et al. 2023) . Technology infrastructure is limited, and the adoption of advanced technologies such as cloud computing and artificial intelligence has been slow. Barriers to improving

digital maturity are numerous and include a lack of policy and legislative frameworks that support digital transformation, resistance to change among government employees, budget limitations, and ineffective leadership (Mametja, Lebambo, and Tichaawa 2023). Nevertheless, some steps have been taken to improve digital maturity, including the use of video conferencing tools (e.g. Zoom, MS Teams) to support remote working and the implementation of digital services in some agencies, such as the South African Revenue Service (SARS) e-filing system and the digitization of identity services in the Department of Home Affairs (Shibambu and Ngoepe 2024).

Until 2024, the adoption of blockchain technology and artificial intelligence (AI) will continue to increase across various sectors, thereby reinforcing the role of these technologies in supporting the implementation of digital maturity frameworks. Recent studies have demonstrated that blockchain not only improves transparency but also enhances data security through a distributed encryption system. Concurrently, artificial intelligence (AI) assists organisations in faster and more accurate cyber threat detection. These developments underscore the necessity for further research that employs bibliometric analysis to explore novel dynamics in digital transformation and cybersecurity challenges.

Cybersecurity threats to digital infrastructure have also increased manifold(Dube and Mohanty 2020) . This situation demands organizations to improve their digital maturity as part of a defense strategy against such threats. However, while there are many digital maturity models available, many of them have not been validated or do not provide practical guidance and relevant tools for real applications (Vance et al. 2023). This creates a gap between theory and practice, which can hinder organisations' efforts to adopt and implement digital transformation effectively and securely.

This research aims to explore the relationship between the level of digital maturity and an organisation's or country's ability to address cybersecurity threats and protect critical data. Using a bibliometric approach, this research analyses trends, patterns and gaps in the literature related to digital maturity, data security and cybersecurity. It also evaluates the reliability of existing digital maturity models, with the aim of providing recommendations for models that are more applicable and support

practical data security improvements.

Literature Review

Understanding Digital Maturity in the Context of Technological Advancements

Continuously improving the security of information systems requires a unique combination of people, policy, and technology (Chisanga and Ngassam 2017). This serves as leverage to design an access control management approach that utilises only the relevant parts of a system, tailored to the end-user's scope of work. The concept of digital maturity as a new view on the use of digital technology by young people.

Digital maturity is defined as the autonomous utilisation of digital technologies that promotes psychological growth and well-being while reducing potential risks and meeting the requirements of the social environment. (Ilin, Levaniuk, and Dubgorn 2021; Thordsen, Murawski, and Bick 2020). Correlations between digital maturity and personality maturity (i.e., conformity, conscientiousness, and negative emotions) were identified. Hierarchical linear regression analysis showed that digital maturity exerted a differential influence in predicting problematic mobile device use, independent of individual differences in terms of personality, age, and level of mobile device use (Babkin et al. 2024).

Digital maturity is defined as the extent to which an organisation has adopted and integrated digital technologies into its operations, culture and overall strategy (Haryanti, Rakhmawati, and Subriadi 2024; Kupilas et al. 2023; Stromberg, Sundberg, and Hasselblad 2020). It is a measure of an organisation's readiness and ability to leverage digital tools and processes to achieve business objectives and create sustainable added value. Digitally mature organisations not only adopt new technologies, but also ensure that they are used strategically to improve efficiency, drive innovation, and deliver superior customer experiences (Voss et al. 2024).

Digital maturity includes technical, operational, and cultural aspects that support each other to ensure the success of digital transformation, and reflects an organisation's ability to adapt to changing technology and market dynamics. Organisations that are at a higher level of digital maturity are usually better prepared to face challenges, more flexible in responding to change, and more innovative in creating new opportunities (Kaszás, Ernszt, and Jakab 2023; MacHado et al. 2020).

Digital maturity frameworks have evolved significantly to reflect the unique

needs and challenges that different industries face in their digital transformation journey (Kaszás et al. 2023). Digital maturity models (DMMs) are used as strategic tools to guide organisations from analog to digital stages (Guarino et al. 2020; Thordsen and Bick 2023a). these models typically cover dimensions such as strategy, leadership, technology and culture, making them broadly applicable, but over time, there has been an increasing trend in the development of more specific models to meet the unique needs of each sector.

In the conformity assessment industry, for example, a five-stage model has been developed, which reveals that most organisations are at an early to mid-stage in digital maturity, with adoption of advanced technologies such as Blockchain still limited and influenced by country-specific factors (Aagaard et al. 2021). In personal service sectors such as education, retail, and healthcare, a specially designed digital maturity model helps companies go through the stages of transformation with a focus on customer experience and operational efficiency.

In the construction industry, a comprehensive framework covers elements such as strategy, digital infrastructure, and business process digitization, and has been validated in the context of the Chinese market, for small and medium-sized enterprises (SMEs), specialized methodologies such as SBRI (Volf et al. 2024) are designed to address the unique constraints faced, including resource and technology limitations (Williams, Schallmo, and Scornavacca 2022) . This approach provides a structured roadmap that helps SMEs gradually adopt digital technologies, enabling them to improve operational efficiency and competitiveness. The evolution of this digital maturity framework underscores the importance of a flexible and contextualized approach in driving digital transformation across sectors.

Data Security Challenges in Cyberspace: Trends and Vulnerabilities in Data Security

The proliferation of cyber threats has reached a point where they are characterized by a marked increase in the sophistication of attacks. These include advanced persistent threats (APTs), ransomware, and supply chain attacks. In contrast to the use of generic malware, these attacks now rely on tools that have been specifically designed to target specific weaknesses in systems. the growth of cyber

threats is the rapid growth of Internet of Things (IoT) devices (Ladu et al. 2024) . These systems are vulnerable to a number of issues, including weak hardware security, difficulty in detecting malware, and threats to data privacy.

Vulnerabilities are exacerbated by the limited capabilities of IoT devices and the utilization of components that lack full trust The integration of cloud computing technologies poses significant challenges related to data security and privacy (Ioanid, Panduru, and Scarlat 2024; Voss et al. 2024). Organizations often have difficulty managing cloud-related risks, including potential data breaches, challenges in e-discovery processes, and maintaining the integrity of the chain of evidence in distributed environments. The rise of the metaverse introduces new security threats, especially with regard to personal data protection, virtual asset security, and increasingly sophisticated social engineering-based attacks,

Technologies such as machine learning (ML) and artificial intelligence (AI) have now become prevalent in detecting threats and improving cybersecurity solutions (Gao et al. 2023). However, it should be noted that ML algorithms are imperfect and vulnerable to attacks during the training or testing phase, potentially leading to significant security breaches. Given these challenges, it is imperative to adopt a more adaptive and holistic approach to security, which can effectively anticipate and address the ever-evolving threats posed by the metaverse and other emerging technologies.

Common Vulnerabilities

Weak authentication mechanisms and vulnerabilities in systems continue to be key entry points for cyber attackers. By exploiting these weaknesses, attackers can gain unauthorized access to an organization's systems and data, often posing as legitimate users to avoid detection. This technique provides immediate access to sensitive information, valuable assets or critical infrastructure, when authentication is not supplemented with additional security measures, such as multi-factor authentication (MFA) (Kaszás et al. 2023), the risk of these attacks increases significantly. Attackers can exploit weak passwords, stolen information, or technical vulnerabilities in authentication protocols to launch their attacks Data breaches are one of the main consequences of these security weaknesses and continue to be a significant threat to organizations in various sectors, Data breaches can lead to the leakage of

sensitive information, including customers' personal data, financial information, or trade secrets, which can cause substantial financial losses and long-term reputational damage.

Privacy regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), have raised expectations for data protection, with non-compliance resulting in substantial fines and reduced customer trust. the proliferation of personal data in the digital environment, which includes sensitive information and user behaviour patterns, further exacerbates privacy concerns (Carcary, Doherty, and Conway 2019). This wealth of data makes organizations a prime target for attackers, due to its high value in the cyber black market. The challenges posed by privacy are further compounded by the increasing use of cloud-based technologies, which introduce additional risks of data exposure through breaches or misconfigurations. These threats originate from individuals within the organization, such as employees, contractors, or business partners, who have legitimate access to the organization's systems, who can abuse their access rights to steal data, damage systems, or leak information to third parties, and these threats are becoming increasingly complex as they can be both malicious and unintentional, for example through human error.

Many organizations deploy intrusion detection systems (IDS) along with user and entity behaviour analysis (UEBA) (Cali et al. 2023; Chaoui et al. 2024). These technologies facilitate comprehensive monitoring of user activity, aiming to identify suspicious behaviour patterns that may signal an insider threat. In contrast, social engineering attacks persist as a pervasive and challenging cybersecurity threat. These attacks involve exploiting the trust or ignorance of individuals to gain access to confidential information such as login credentials or other sensitive data. Phishing, one of the prevalent forms of social engineering, involves sending fraudulent emails that appear legitimate, with the aim of tricking recipients into divulging sensitive information, due to their inherently human nature, these attacks are difficult to fully address through technological solutions alone. Therefore, cybersecurity education and training for users emerges as an important measure to mitigate these threats.

By increasing user awareness and fostering a comprehensive understanding of cybersecurity best practices, organizations can effectively mitigate the risk of social

engineering attacks and protect their digital assets In the contemporary cyber threat landscape, a holistic approach is essential, which includes implementing advanced authentication mechanisms, enhanced data management practices, proactive surveillance against insider threats, and comprehensive education and training for all individuals within the organization. By integrating technical strategies with human awareness, organizations can strengthen their security posture and better prepare themselves to face the ever-evolving cyber challenges.

Interlinking Digital Maturity and Enhanced Data Security

The capability maturity model for data security plays an important role in helping organizations systematically improve their security practices as their level of digital maturity increases (Gašperlin 2021). Organisations with higher digital maturity typically have stronger data security measures in place, as they understand the importance of protecting their evolving digital assets. The model provides a structured roadmap, allowing organizations to identify weaknesses, evaluate their current level of readiness, and implement the necessary steps to strengthen their security posture. Through a phased approach, the model helps organizations integrate cybersecurity best practices into their operational processes, thus ensuring better data protection.

Additionally, implementing cybersecurity risk management frameworks and standards is a crucial element of this strategy. Frameworks such as the NIST Cybersecurity Framework, ISO 27001, or COBIT provide comprehensive guidance for identifying, assessing, and managing data security risks (Alromaih, Ismail, and Elmedany 2022; Giuca et al. 2021). By following these standards, organisations can ensure that they have a consistent and measurable approach to protecting their digital assets. These frameworks also help in establishing clear processes for detecting and responding to security incidents, thereby minimizing the potential impact of cyber threats (Giuca et al. 2021).

Digital maturity and improved data security are closely intertwined. As organisations progress in their digital maturity, the need for more sophisticated security measures also increases. Organizations should adopt a holistic data security approach, which includes both strategic and technical elements to protect their sensitive information. This involves using technologies such as data encryption, multi-factor

authentication, and AI-based security analytics, while ensuring that security policies are implemented thoroughly across the organizational structure. By balancing these strategic and technical measures, organizations can effectively mitigate risk, build trust, and support the sustainability of their digital transformation

METHODS

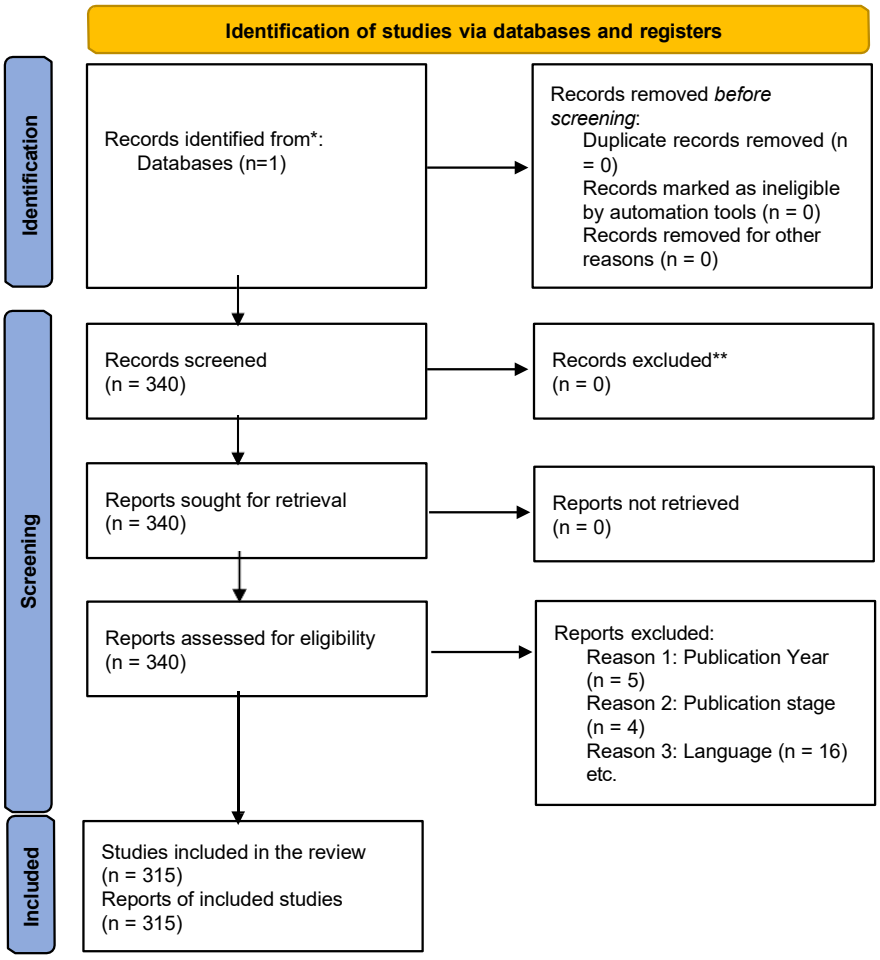
This research uses qualitative and bibliometric analysis methodologies . Qualitative research methodology is particularly suitable for identifying solutions to research problems, which offer results in the form of descriptions and factual data collection (Sugiyono 2019). The bibliometric analysis used in this research involved the aggregation of a wide range of articles, journals and other scholarly works deemed appropriate to meet the research requirements (Prakoso et al. 2023).

This research utilises the Scopus database, a comprehensive resource with scholarly sources, covering a wide range of fields such as social sciences, engineering, computer science, energy, environmental sciences, and arts and humanities (Singh et al. 2021; Subandi et al. 2022). The PRISMA method was used to search for relevant literature on digital maturity in data security. The findings provide insights into local government policies in smart city security and form the basis for further research. Scopus was chosen due to its broader topic and multidisciplinary coverage. This research contributes to the existing literature and serves as a basis for digital maturity to improve data security. The bibliometric analysis involved selecting 338 documents to create a bibliometric map using the VOSviewer analysis tool. This tool provides deep insights into the relevant literature network, allowing researchers to identify trends, patterns and relationships among the selected documents (Donthu et al. 2021; Nurmandi et al. 2021).

Data Collection Techniques

This research takes data from the Scopus database with the following API keys: (TITLE-ABS-KEY (digital AND maturity) AND TITLE-ABS-KEY (data AND security) OR TITLE-ABS-KEY (cyber AND security) OR TITLE-ABS-KEY (threat)) AND PUBYEAR > 2003 AND PUBYEAR < 2025 AND (LIMIT-TO (PUBSTAGE, "final") AND (LIMIT-TO (LANGUAGE, "English")).

Figure 1.
The PRISMA Chart



Source **:** *Created by Author*

Data Analysis Techniques

This study used the bibliometric analysis tools VOSviewer and RStudio to understand the structure, trends, and relationships between relevant documents. VOSviewer visualizes the literature network, and RStudio is used to perform statistical analysis on tree maps, trend analysis, and cluster visualization. The data processing stage involves document selection, visualization, and research keyword analysis, but has limitations such as limited literature

coverage and potential bias. Analysis of co-occurrence and specific topics may not cover all relevant aspects of complex relationships, thus affecting the overall representation of the existing literature network.

RESULTS AND DISCUSSION

Digital maturity, as defined in the extant literature, refers to an organisation's ability to strategically integrate digital technology into its operational processes, organizational culture, and strategic objectives (Kupilas et al. 2023; Stromberg et al. 2020). Digital maturity models, such as the Digital Maturity Model (DMM), offer a structured approach to assess an organisation's preparedness and capacity to utilise digital technology. In accordance with the principles of digital transformation theory, digital maturity encompasses not only the adoption of technological innovations but also the implementation of cultural and managerial changes that foster organisational innovation and flexibility (Thordsen and Bick 2023b).

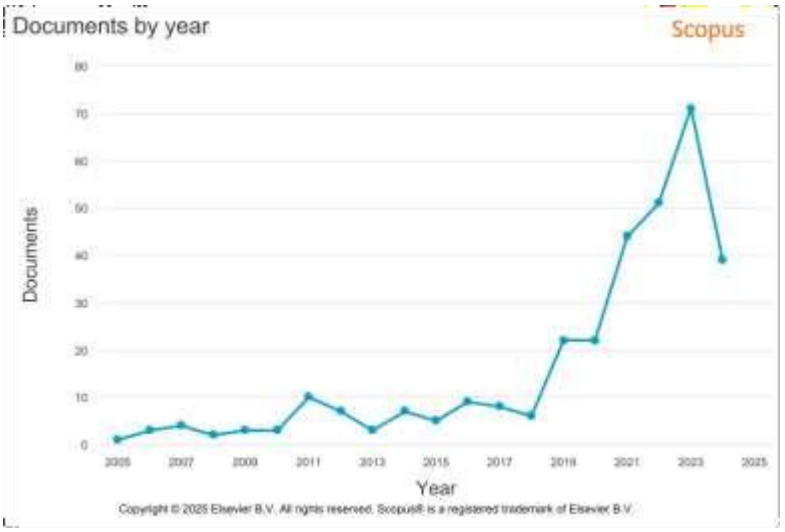
The findings of the present study demonstrate a positive correlation between the degree of digital maturity of an organization and its capacity to withstand cyber threats. This approach is consistent with the open organizational system model, which underscores adaptability and technological integration as pivotal components of organizational sustainability (Strader 2010). To illustrate, the integration of blockchain and artificial intelligence (AI) facilitates data security through encryption and threat analysis based on smart algorithms.

The author's proficiency in bibliometric research is evident in their utilization of VOSviewer and RStudio software for the analysis of trends, patterns, and relationships in the extant literature concerning digital maturity and data security. By leveraging scientific databases such as Scopus, the author has meticulously compiled comprehensive data visualizations. In addition, the findings of this study will be presented in the results and discussion section. There, they will be discussed in depth and analysed critically. This will provide readers with a comprehensive understanding of the issues raised by the study.

Publication by Year

Figure 2.

A number of articles on data security topics



***Source**: analyzed by Scopus*

In Figure 2 above, the Scopus database shows that the number of articles or papers with the topic "Digital AND maturity" AND "Data AND security" OR "Cyber AND security" OR "Threat" released in the period from 2005-2024 experienced a fairly stable increase and decrease . The numbers in the graph above show the number of articles published and recorded in the Scopus database. In 2019, there was a huge increase from the previous years, namely an increase from around 1-10 documents immediately increased to 22 documents. From 2019 to 2023, the increase in the number of article publications is increasingly significant. The highest was achieved in 2023, which was 71 documents. Unfortunately, in 2024 the number of publications on this topic was only 39 documents. It can be said that from 2019-2023 the discussion on this topic was very intensively discussed and studied by several researchers.

Document by Country

Figure 3.

Article Producing countries

***Source** : result data by Scopus and visualize by mapchart.com*

From the figure 3 above, the difference in color shows the number of documents published in each country. The color shown from dark to light shows the lighter the less the number of documents published from that country. The United States has a dark red color which means that the number of article publications in that country is the highest, namely 42 documents. Then followed by China, United Kingdom, India, Germany, Au stralia, Italy, and Indonesia. Indonesia itself has the lightest color, which means that Indonesia has the least number of document or article publications that discuss this topic, which is only 10 documents. The attractiveness of discussing this topic for Australia, Italy, and Indonesia is still less attractive as evidenced by the number of publications from these countries compared to the US, China and the UK.

Word Cloud

Figure 4

RStudio word cloud visuzalization

Source : Processed by the author

Figure 4 illustrates a word cloud depicting key terms related to the worlds of "digital security", "data storage" and "technology transformation". The terms displayed reflect various aspects that are of major concern in today's digital age, especially in the context of data protection, privacy, and the utilization of advanced technologies. One term that stands out is "Digital Storage", which refers to the method of digitally storing data using technologies such as cloud computing, local servers, or other storage devices. In the era of digital transformation, secure and efficient data storage is becoming a fundamental need for organizations and individuals.

The term "Security of Data" is also very important, as it refers to the protection of data from threats such as unauthorized access, theft, or information leakage. In this context, "Cybersecurity" plays a vital role with a focus on protecting computer systems, networks, and data from cyberattacks such as malware, phishing, or hacking. This security covers various aspects, including "Network Security", which ensures computer networks remain protected from external and internal threats. In addition, "Digital Maturity" reflects the level of readiness of an organization or individual to adopt digital technologies effectively and safely. This involves an understanding of "blockchain", a decentralized technology that provides security and transparency in data recording, and "Artificial Intelligence (AI)", which is used to automatically detect security threats and perform in-depth data analysis

Tree Map

Figure 5.

RSudio Tree Map Visualization

***Source** : Processed by the Author*

The figure 5 shows a tree diagram depicting the various topics related to digital maturity, cybersecurity and data privacy, and the number and percentage of their contributions. "Digital Maturity" is one of the topics in this diagram that has 8 entries or 1% of the overall data. Although the percentage is small compared to other topics, digital maturity is an important concept that measures the level of adaptation, integration, and application of digital technology in an organization or entity.

"Digital Maturity" covers various aspects such as the adoption of the latest technologies, efficient data management processes, and an organizational culture that supports innovation and security. Organizations that achieve high digital maturity tend to have secure and efficient digital storage systems, as well as advanced cybersecurity systems to protect their data from cyber threats. For example, in the diagram, "digital storage" has the highest contribution with 53 entries (8%), showing the importance of digital storage in the context of digital maturity and data security. In addition, technologies such as "blockchain" and "block-chain" are also a focus in discussions about digital maturity, with 20 entries (3%) and 17 entries (3%) respectively. These technologies help increase transparency and security in digital transactions, which are important aspects of digital maturity. Digitally mature organizations also pay attention

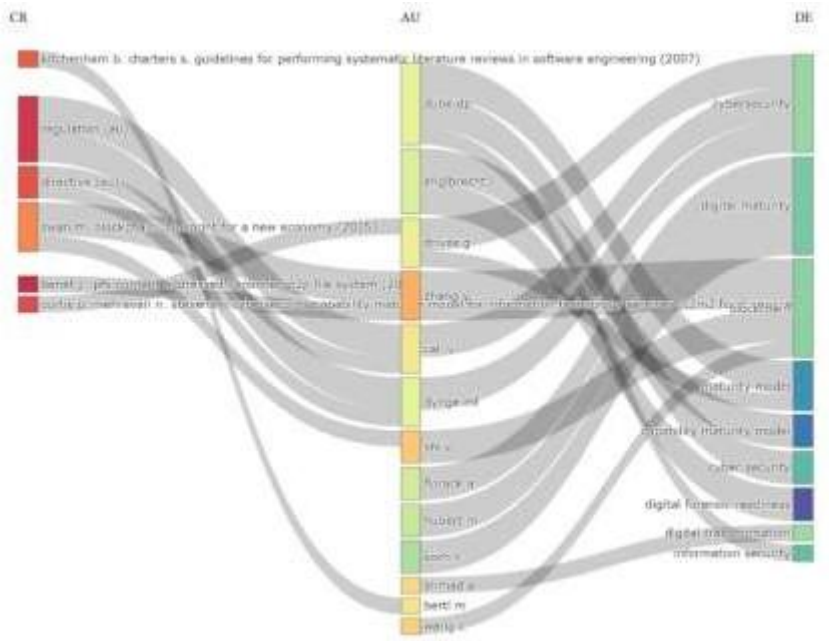
to "data privacy", with 15 entries (2%), to ensure that sensitive data is processed and stored securely.

Overall, it provides a comprehensive overview of relevant topics and their contribution to the discussion on digital maturity, cybersecurity, and data privacy. Organizations that achieve a high level of digital maturity can improve efficiency, innovation, and security in their operations, and are better equipped to face the challenges and take advantage of the opportunities that exist in the digital age.

Three Field Plot

Figure 6.

Three Field Plot visualization RStudio



Source : *processed by the author*

Figure 6 is a Sankey diagram that visualizes the relationship between three main categories, namely CR (References), AU (Authors), and DE (Topics). The CR category contains references to important documents and guidelines, such as "kitchenham b. charters s. guidelines for performing systematic literature reviews in software engineering (2007)" and "swan m. blockchain: blueprint for a new economy (2015)." The AU category lists the main authors or contributors, including names like "dube dp," "englebrecht l," and "zhang y." The DE category covers topics such as "cybersecurity," "digital maturity," and "blockchain."

This diagram uses colored bands to show the connections between documents in CR, authors in AU, and topics in DE. Each band depicts the flow from a document to an author and then to a topic, showing how different documents are related to a particular author and topic. This visualization is very useful and relevant as it provides a clear and concise way to understand the relationship between documents, authors, and topics in a given field. In this context, Sankey's diagram seems to be closely related to the fields of software engineering, cybersecurity, and digital transformation.

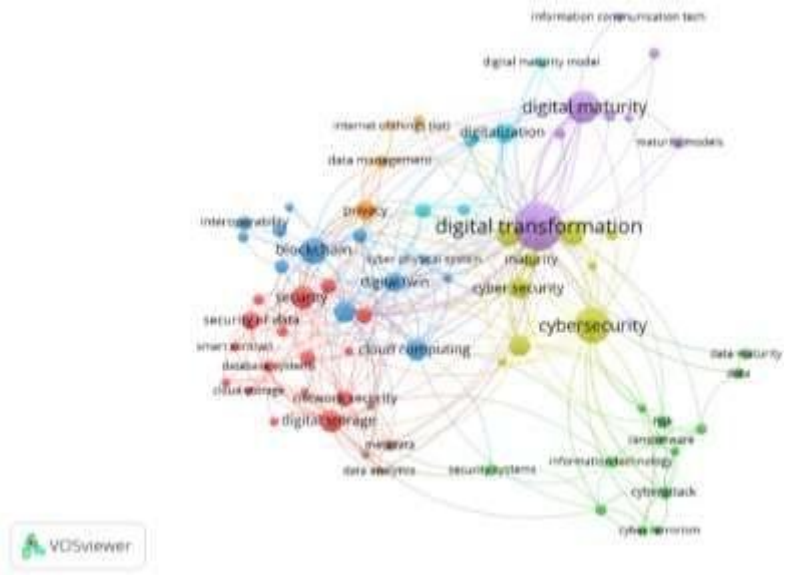
By understanding the relationships depicted in this diagram, researchers can identify research trends, link author contributions to specific topics, and gain in-depth insights into the development of literature in relevant fields. This diagram helps in analyzing how references, authors, and topics interact and influence each other in the broader context of research

Visualization by Keyword

The network relationships in "Digital AND maturity" AND "Data AND security" OR "Cyber AND security" OR "Threat" were 315 articles. The scientific articles were then processed using VOSviewer software, resulting in a visualization of related terms. Overall, there were 8 clusters and 71 items. The text items can be defined as research themes related to digital maturity and impact on cybersecurity.

Figure 7.

VOSviewer Network Visualization

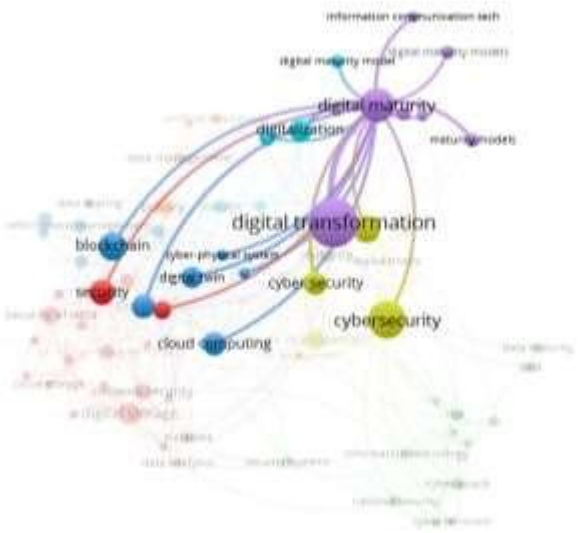


Source : processed by the author

From Figure 7, it explains that each cluster has a different color. The difference illustrates the extent of the concept or term studied in a study. Each node listed has its own network attachment. Network attachments are not only in the same node color, but can be bound between different node colors. From the figure, there are 8 different colors that indicate there are 8 clusters separated according to the strength of the network and its relationship to the main topic.

Figure 8.

Digital Maturity network visualization VOSviewer



Source: Processed by the author

The Figure 8. is a diagram showing the relationship between various

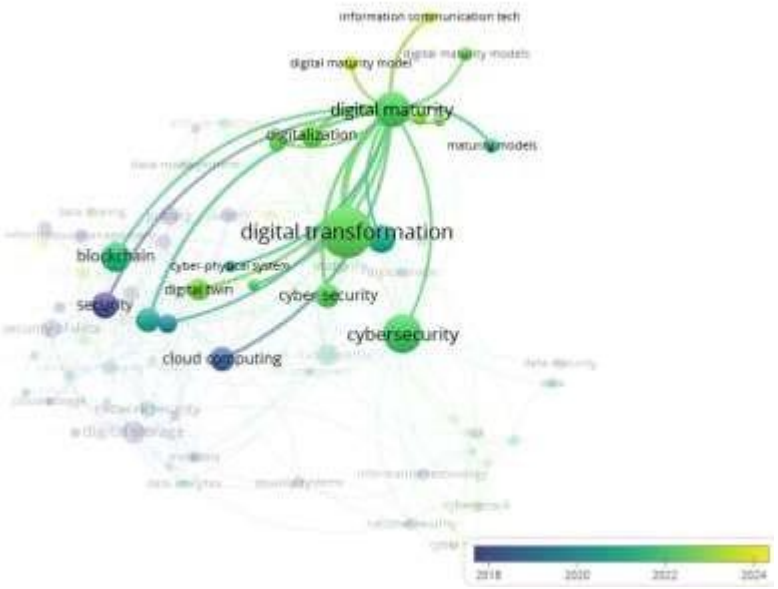
keywords in the context of digital transformation, which is highly relevant to the title "A Bibliometric Analysis of Digital Maturity and Its Impact on Cybersecurity." This concept map highlights several key aspects such as digital maturity, cybersecurity, cloud computing, and blockchain technology.

At the center of the diagram, Digital Transformation is the core concept that connects all the other keywords. Digital transformation is the process by which organizations adopt digital technologies to transform operations and deliver better value to customers. Digital Maturity, which is one of the key buzzwords, measures how far an organization has successfully integrated digital technologies in all aspects of their operations. Organizations with a high level of digital maturity are better able to face the challenges and take advantage of the opportunities that exist in the digital age

Cybersecurity is a crucial aspect that is closely connected to digital transformation. In this diagram, the keyword Cybersecurity highlights the importance of protecting data and information technology infrastructure from various cyber threats. Organisations that achieve high digital maturity usually have sophisticated cybersecurity systems, which involve the use of technologies such as blockchain and cloud computing.

Figure 9.

Overlay Visualization VOSvewer of digital maturity



Source: Processed by the Author

Figure 9 shows a concept map or network of keywords related to digital transformation. The most prominent main keywords are digital transformation, digital maturity, cybersecurity, and cloud computing. These keywords are linked to other relevant terms, such as blockchain, security, digital twin, and privacy. there is a color scale showing the range of years from 2018 to 2024. Green indicates newer terms, while blue indicates older terms. This gives an idea of the evolution and trends of keywords in digital transformation over time.

The keyword digital maturity is seen with a color that falls on the green to blue spectrum, indicating that the term has gained significant attention in recent years and continues to be a relevant topic in discussions about digital transformation. This means that digital maturity is a relatively new concept that is gaining importance year on year. With the green color of the digital maturity keyword, we can see that research and discussion on digital maturity has increased in recent years, reflecting the importance of the adoption and integration of digital technologies in organizations to improve efficiency and cybersecurity.

Rapid digital transformation has driven researchers' attention to the importance of digital maturity and data security (Pörtner, Möske, and Riel 2022). The bibliometric analysis shows an increasing trend in the number of publications related to this topic, especially from 2019 to 2023. This period shows a significant surge in attention to digital maturity as an important element in addressing data security challenges in the digital age. However, in 2024, the number of publications decreased, which may reflect a shift in research focus or other influences such as new priorities in technology.

The geographical distribution of the research shows the dominance of the United States, China, and the United Kingdom as the countries with the highest contributions. Meanwhile, Indonesia, along with countries such as Australia and Italy, still have a relatively low number of publications. This signals the need for increased research efforts in the region, given the importance of digital technology adoption to strengthen data security and drive broader digital transformation

Keyword visualization analysis revealed dominant themes such as "Digital Storage," "Cybersecurity," and "Blockchain." These terms reflect a key need in the era of digital transformation, which is the integration of technologies to ensure operational

efficiency while protecting data from cyber threats. Digital maturity, as a key concept, is identified as a measure of an organization's readiness to effectively adopt digital technologies (Kupilas et al. 2023). Organizations that achieve a high level of digital maturity tend to be better able to deal with security challenges, thanks to the utilization of technologies such as AI, cloud computing, and blockchain (Ladu et al. 2024).

In addition, the link between digital maturity and data security is prominent in this analysis. Organizations with higher levels of digital maturity generally have stronger data security measures in place. This is reflected in the adoption of frameworks such as the NIST Cybersecurity Framework or ISO 27001 (Sulistyowati et al. 2020), which provide comprehensive guidance for identifying risks, protecting digital assets and mitigating the impact of security incidents. With a structured, step-by-step approach, organizations can significantly improve their data security. However, the gap between theory and practice in the implementation of digital maturity models remains a challenge. Many existing models do not provide enough practical guidance for real applications. Therefore, organizations need more relevant and applicable guidance to ensure their digital transformation runs safely and effectively.

CONCLUSION

Digital maturity is a critical factor in bolstering data security and enhancing organisational resilience against cyber threats in the era of digital transformation. Organizations with high levels of digital maturity are more likely to adopt new technologies such as blockchain and artificial intelligence to strengthen their security systems. Nevertheless, the discrepancy between theoretical frameworks and their practical implementation persists as a substantial challenge, particularly in developing countries grappling with infrastructural limitations and policy support constraints. Consequently, this study proposes the formulation of a more contextual, practical, and relevant digital maturity model to facilitate inclusive, efficient, and sustainable digital transformation across various sectors.

Funding Acknowledgement

The research work of this article was supported by Jusuf Kalla School of Government, Universitas Muhammadiyah Yogyakarta. The researcher would like to express his immense gratitude to his supporters, who have provided all the necessary

insight and expertise to assist in this research.

About the Author

Aulia Kartika Putri and Achmad Nurmandi from Master of Government Affairs and Administration, Universitas Muhammadiyah Yogyakarta, Indonesia.

Herman Lawelai from Department of Government Studies of Universitas Muhammadiyah Buton.

Muhammad Younus from Department of product Ressearch and Software Development, TPL Logistics Pvt Ltd, Karachi, Pakistan and Government Affairs and Administration, Universitas Muhammadiyah Yogyakarta, Indonesia.

REFERENCES

Aagaard, Annabeth, Mirko Presser, Tom Collins, Michail Beliatis, Anita Krogsøe Skou, and Emilie Mathilde Jakobsen. 2021. "The Role of Digital Maturity Assessment in Technology Interventions with Industrial Internet Playground." *Electronics (Switzerland)* 10(10). doi: 10.3390/electronics10101134.

Alatalu, Siim. 2019. "Dealing with an Evolving Cyber Threat Picture - Developing a Joint European Response." Pp. 10–20 in *Cyber Defense - Policies, Operations and Capacity Building: CYDEF 2018*. NATO Cooperative Cyber Defence Centre of Excellence, Estonia: IOS Press.

Alromaih, Arwa, Yasser Ismail, and Wael Elmedany. 2022. "Continuous Compliance to Ensure Strong Cybersecurity Posture Within Digital Transformation In Smart Cities." Pp. 464–79 in *IET Conference Proceedings*. Vol. 2022. College of Information Technology, University of Bahrain, Bahrain: Institution of Engineering and Technology.

Babkin, Alexandr, Pavel Mikhailov, Gleb Teplytsky, Akram Ochilov, and Ding Haiqi. 2024. "Approaches to Assessing the Digital Maturity of an Industrial Enterprise." in *BIO Web of Conferences*. Vol. 138, edited by P. E.N., T. I.V., and N. A.R. Peter the Great St.Petersburg Polytechnic University, Polytechnicheskaya, 29, St.Petersburg, 195251, Russian Federation: EDP Sciences.

Bahuguna, Ashutosh, R. K. Bisht, and Jeetendra Pande. 2019. "Assessing Cybersecurity Maturity of Organizations: An Empirical Investigation in the Indian Context." *Information Security Journal* 28(6):164–77. doi: 10.1080/19393555.2019.1689318.

Blum, Dan. 2020. *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*. Apress Media LLC.

Cali, Umit, Marthe Fogstad Dynge, Ahmed Idries, Sambeet Mishra, Ivanko Dmytro, Naser Hashemipour, and Murat Kuzlu. 2023. "Digital Energy Platforms Considering Digital Privacy and Security by Design Principles." Pp. 167–73 in *ACM International Conference Proceeding Series*. Department of Electric Energy, Norwegian University of Science and Technology, Trondheim, Norway: Association for Computing Machinery.

Canina, Mara Rita, and Carmen Bruno. 2021. "Digital Creative Abilities for Achieving Digital Maturity." Pp. 27–35 in *Lecture Notes in Networks and Systems*. Vol. 269, edited by N. S., A. T.Z., and K. W. IDEActivity Center, Design Department, Politecnico di Milano, Via Durando 38/A, Milan, 20158, Italy: Springer Science and Business Media Deutschland GmbH.

Carcary, Marian, Eileen Doherty, and Gerry Conway. 2019. "Personal Data Protection (Pdp): A Conceptual Framework for Organisational Management of Personal Data in the Digital Context." Pp. 87–96 in *European Conference on Information Warfare and Security, ECCWS*. Vols. 2019-July, edited by C. T. and S. P. Innovation Value Institute, Maynooth University, Ireland: Curran Associates Inc.

Chaoui, Kenza, Nadia Kabachi, Nouria Harbi, and Hassan Badir. 2024. "Comprehensive Data Life Cycle Security in Cloud Computing: Current Mastery and Major Challenges." Pp. 195–206 in *Communications in Computer and Information Science*. Vol. 1728 CCIS, edited by T. M., B. H., B. L., B. A., L. A., and M. F. IDS Team ENSAT, Abdelmalek Essaadi University Tangier, Tangier, Morocco: Springer Science and Business Media Deutschland GmbH.

Chisanga, Emmanuel, and Ernest Ketcha Ngassam. 2017. "Towards a Conceptual Framework for Information Security Digital Divide." in *2017 IST-Africa Week Conference, IST-Africa 2017*. CITC Namibia, 1570 Smarties Extension 8, Okahandja, Namibia: Institute of Electrical and Electronics Engineers Inc.

Donthu, Naveen, Satish Kumar, Debmalya Mukherjee, Nitesh Pandey, and Weng Marc Lim. 2021. "How to Conduct a Bibliometric Analysis: An Overview and Guidelines." *Journal of Business Research* 133:285–96. doi: 10.1016/j.jbusres.2021.04.070.

Dube, Durga Prasad, and R. P. Mohanty. 2020. "Towards Development of a Cyber Security Capability Maturity Model." *International Journal of Business Information Systems* 34(1):104–27. doi: 10.1504/IJBIS.2020.106800.

Gao, Jie, Tianyi Wang, Yuhui Han, Lixia Liu, Xingwei Zhang, Lexi Xu, Yang Wu, Zijing Yang, and Chen Cheng. 2023. "An Analysis Strategy of Abnormal Subscriber Warning Based on Federated Learning Technology." Pp. 2104–9 in *Proceedings* -

2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom/BigDataSE/CSE/EUC/iSCI 2023, edited by H. J., M. G., and W. G. China United Network Communications Corporation, Research Institute, Beijing, China: Institute of Electrical and Electronics Engineers Inc.

Gašperlin, Blaž. 2021. "Conceptual Model for Smes' Data Maturity Assessment." Pp. 769–78 in *34th Bled eConference: Digital Support from Crisis to Progressive Change, BLED 2021 - Proceedings*, edited by A. P. A., B. M.K., B. R., C. H., S. A., and V. D. University of Maribor, Faculty of Organizational Sciences, Kranj, 4000, Slovenia: University of Maribor Press.

Giuca, Olivia, Traian Mihai Popescu, Alina Madalina Popescu, Gabriela Prostean, and Daniela Elena Popescu. 2021. "A Survey of Cybersecurity Risk Management Frameworks." Pp. 240–72 in *Advances in Intelligent Systems and Computing*. Vol. 1221 AISC, edited by B. V.E., B. M.M., J. L.C., J. L.C., J. L.C., and S. S.N. Management Department, Faculty of Management in Production and Transportation, "Politehnica" University of Timisoara, Remus Street 14, Timisoara, 300191, Romania: Springer.

Guarino, Massimo, Maria Anna Di Palma, Tullio Menini, and Michele Gallo. 2020. "Digital Transformation of Cultural Institutions: A Statistical Analysis of Italian and Campania GLAMs." *Quality and Quantity* 54(5–6):1445–64. doi: 10.1007/s11135-019-00889-3.

Haryanti, Tining, Nur Aini Rakhmawati, and Apol Pribadi Subriadi. 2024. "Assessing the Digital Transformation Landscapes of Organization: The Digital Transformation Self-Assessment Maturity Model (DX-SAMM)." Pp. 1561–69 in *Procedia Computer Science*. Vol. 234, edited by M. F. Information System, Faculty of Intelligent Electrical and Informatics Technoloy (F-Electics), Institut Teknologi Sepuluh Nopember, Surabaya, 60111, Indonesia: Elsevier B.V.

Heitzenrater, Chad. 2006. "A Government Perspective on Digital Data Embedding: Taking a Systems Approach." P. 77 in *Proceedings of the 7th Multimedia and Security Workshop 2005, MM and Sec'05*. Vol. 2006. Air Force Research Laboratory, Rome, NY, United States.

Ilin, Igor, Daria Levaniuk, and Alissa Dubgorn. 2021. "Assessment of Digital Maturity of Enterprises." Pp. 167–77 in *Advances in Intelligent Systems and Computing*. Vol. 1259 AISC, edited by M. V. and P. V. Peter the Great St. Petersburg Polytechnic University, Polytechnicheskaya 29, St. Petersburg, 195251, Russian Federation: Springer.

Ioanid, Alexandra, Dan Andrei Panduru, and Cezar Scarlat. 2024. "Towards Maturity of

Digital Transformation: Development of Digital Maturity Scorecard." Pp. 471–81 in *Lecture Notes in Networks and Systems*. Vol. 928 LNNS, edited by M. L. and G. A. National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania: Springer Science and Business Media Deutschland GmbH.

Kaszás, Nikoletta, Ildiko Ernszt, and Balint Jakab. 2023. "The Emergence of Organizational and Human Factors in Digital Maturity Models." *Management (Croatia)* 28(1):123–35. doi: 10.30924/mjcmi.28.1.8.

Khmeleva, G. A., and T. Czegledy. 2021. "Towards a New Format of Regional Integration: Co-Creation and Application of Technologies." Pp. 71–77 in *Lecture Notes in Networks and Systems*. Vol. 133. Samara State University of Economics, Samara, Russian Federation: Springer.

Korovin, Grigoriy. 2022. "Digital Twins in the Industry: Maturity, Functions, Effects." Pp. 1–12 in *Lecture Notes in Information Systems and Organisation*. Vol. 54, edited by K. V., L. J., A. V., and K. E. Institute of Economics of the Ural Branch of the Russian Academy of Sciences, 29 Moskovskaya St., Ekaterinburg, 620014, Russian Federation: Springer Science and Business Media Deutschland GmbH.

Kupilas, Krzysztof Jacek, Vicente Rodriguez Montequin, Javier García González, and Guillermo Alonso Iglesias. 2023. "Digital Maturity Model for Research and Development Organization with the Aspect of Sustainability." Pp. 1583–90 in *Procedia Computer Science*. Vol. 219, edited by M. R., R. R., C.-C. M.M., D. D., and P. E. Project Engineering Area, University of Oviedo, C7Independencia 13, Oviedo, 33004, Spain: Elsevier B.V.

Ladu, Luana, Claudia Koch, Parsa Asna Ashari, Knut Blind, and Pavel Castka. 2024. "Technology Adoption and Digital Maturity in the Conformity Assessment Industry: Empirical Evidence from an International Study." *Technology in Society* 77. doi: 10.1016/j.techsoc.2024.102564.

MacHado, Carla G., Peter Almstrom, Anna E. Oberg, Martin Kurdve, and Sultan Y. Almashalah. 2020. "Maturity Framework Enabling Organizational Digital Readiness." Pp. 649–60 in *Advances in Transdisciplinary Engineering*. Vol. 13, edited by S. K. and E. F. Department of Technology Management and Economics, Chalmers University of Technology, Gothenburg, Sweden: IOS Press BV.

Mametja, Thapelo R., Marcia M. Lebambo, and Tembi M. Tichaawa. 2023. "The Adoption of Digital Technologies by Women-Owned Tourism Micro-Enterprises." *African Journal of Hospitality, Tourism and Leisure* 12(2):717–34. doi: 10.46222/ajhtl.19770720.395.

Marican, Mohamed Noordin Yusuff, Siti Hajar Othman, Ali Selamat, and Shukor Abd Razak. 2024. "Quantifying the Return of Security Investments for Technology Startups." *Baghdad Science Journal* 21(7):2449–61. doi: 10.21123/bsj.2023.9077.

Mayhew, Joe, and Hamid Jahankhani. 2020. "Current Challenges of Modern-Day Domestic Abuse." Pp. 267–82 in *Advanced Sciences and Technologies for Security Applications*. Ernst & Young LLP, London, United Kingdom: Springer.

Möller, Dietmar P. F., and Roland E. Haas. 2024. "Cybersecurity Needs and Benefits: The Four Rings Model." Pp. 461–71 in *Lecture Notes in Networks and Systems*. Vol. 839, edited by U. A., A. S., C. D., and D. F. R. Clausthal University of Technology, Clausthal-Zellerfeld, Germany: Springer Science and Business Media Deutschland GmbH.

Nasutra, Rafi Munif Setiyoko, and Arta Moro Sundjaja. 2023. "An Empirical Study of the Impacts Perceived Risk on Trust and Continuous Intention to Use Digital Banking in Indonesia." Pp. 588–93 in *2023 International Conference on Informatics, Multimedia, Cyber and Information Systems, ICIMCIS 2023*. Bina Nusantara University, Business School Master Program, Management Department, Jakarta, Indonesia: Institute of Electrical and Electronics Engineers Inc.

Nurmandi, Achmad, Danang Kurniawan, Misran, and Salahudin. 2021. "A Meta-Analysis of Big Data Security: How the Government Formulates a Model of Public Information and Security Assurance into Big Data." Pp. 472–79 in.

O'Brien, Niki, Roberto Fernandez Crespo, Fiona O'Driscoll, Mabel Prendergast, Deeph Chana, Ara Darzi, and Saira Ghafur. 2024. "Usability and Feasibility Evaluation of a Web-Based and Offline Cybersecurity Resource for Health Care Organizations (The Essentials of Cybersecurity in Health Care Organizations Framework Resource): Mixed Methods Study." *JMIR Formative Research* 8. doi: 10.2196/50968.

Ogwueleka, Francisca Nonyelum, and Aniche Delight Aniche. 2021. "Information and Communication Technology, Cyber-Security and Counterterrorism in Africa." Pp. 129–51 in *The Routledge Handbook of Counterterrorism and Counterinsurgency in Africa*. Computer Science and Cyber Security, Nigerian Defence Academy, Kaduna, Nigeria: Taylor and Francis.

Okae, Samuel, Francis Kofi Andoh-Baidoo, and Emmanuel Ayaburi. 2019. "Antecedents of Optimal Information Security Investment: IT Governance Mechanism and Organizational Digital Maturity." Pp. 442–53 in *IFIP Advances in Information and Communication Technology*. Vol. 558, edited by D. Y., A. E., B. R., and E. J. Nobel International Business School, Accra, Ghana: Springer Science and Business Media, LLC.

Polychronaki, Maria, Michael G. Xevgenis, Dimitrios G. Kogias, and Hellen C. Leligou. 2024. "Decentralized Identity Management for Metaverse-Enhanced Education: A Literature Review." *Electronics (Switzerland)* 13(19). doi: 10.3390/electronics13193887.

Pörtner, Lara, Robert Möske, and Andreas Riel. 2022. "Data Management Strategy Assessment for Leveraging the Digital Transformation: A Comparison Between Two Models: DX-CMM and Camelot DMM." Pp. 553–67 in *Communications in Computer and Information Science*. Vol. 1646 CCIS, edited by Y. M., C. P., M. R., and W. B. Univ. Grenoble Alpes, CNRS, Grenoble INP, G-SCOP, Grenoble, 38000, France: Springer Science and Business Media Deutschland GmbH.

Prakoso, Velandani, Herman Lawelai, Achmad Nurmandi, Eko Priyo Purnomo, and Hazel Jovita. 2023. "Research Trends, Topics, and Insights on Network Security and the Internet of Things in Smart Cities." *Jurnal Studi Ilmu Pemerintahan* 4(2):191–206.

van Rayne, Kiana K., Oluwafemi A. Adebo, Obiro C. Wokadala, and Nomali Z. Ngobese. 2023. "The Potential of Strychnos Spp L. Utilization in Food Insecurity Alleviation: A Review." *Food Reviews International* 39(6):3400–3414. doi: 10.1080/87559129.2021.2012791.

Shibambu, Amos, and Mpho Ngoepe. 2024. "Enhancing Service Delivery through Digital Transformation in the Public Sector in South Africa." *Global Knowledge, Memory and Communication*. doi: 10.1108/GKMC-12-2023-0476.

Shyu, Mei Ling, Shu Ching Chen, Qibin Sun, and Heather Yu. 2007. "Overview and Future Trends of Multimedia Research for Content Access and Distribution." *International Journal of Semantic Computing* 1(1):29–66. doi: 10.1142/S1793351X07000044.

Singh, Vivek Kumar, Prashasti Singh, Mousumi Karmakar, Jacqueline Leta, and Philipp Mayr. 2021. "The Journal Coverage of Web of Science, Scopus and Dimensions: A Comparative Analysis." *Scientometrics* 126(6):5113–42. doi: 10.1007/s11192-021-03948-5.

Strader, Troy J. 2010. "Digital Convergence and Horizontal Integration Strategies." Pp. 113–41 in *Digital Product Management, Technology and Practice: Interdisciplinary Perspectives*. College of Business and Public Administration, Drake University, United States: IGI Global.

Stromberg, J., L. Sundberg, and A. Hasselblad. 2020. "Digital Maturity in Theory and Practice: A Case Study of a Swedish Smart-Built Environment Firm." Pp. 1344–48 in *IEEE International Conference on Industrial Engineering and Engineering*

Management. Vols. 2020-Decem. Mid Sweden University, Department of Information Systems and Technology, Sundsvall, Sweden: IEEE Computer Society.

Subandi, Yeyen, Achmad Nurmandi, Zuly Qodir, Hasse Jubba, Titin Purwaningsih, Tri Nur Rochimah, and M. Syamsurrijal. 2022. "Bibliometric Analysis and Visualization of Political Patronage Articles in Indonesia Indexed in Scopus." in *Proceedings of the First International Conference on Democracy and Social Transformation, ICON-DEMOST 2021, September 15, 2021, Semarang, Indonesia*. EAI.

Sugiyono. 2019. *Metode Penleitian Kuantitatif, Kualitatif, Dan R&d*. Bandung: Alfabeta.

Sulistyowati, Diah, Fitri Handayani, and Yohan Suryanto. 2020. "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using Nist Csf, Cobit, Iso/Iec 27002 and Pci Dss." *International Journal on Informatics Visualization* 4(4):225–30. doi: 10.30630/joiv.4.4.482.

Thordsen, Tristan, and Markus Bick. 2023a. "A Decade of Digital Maturity Models: Much Ado about Nothing?" *Information Systems and E-Business Management* 21(4):947–76. doi: 10.1007/s10257-023-00656-w.

Thordsen, Tristan, and Markus Bick. 2023b. "The Importance of Platforms to Achieve Digital Maturity." Pp. 339–51 in *Lecture Notes in Business Information Processing*. Vol. 464 LNBIP, edited by P. M., R. da C. P., T. M., and C. K. ESCP Business School Berlin, Heubnerweg 8-10, Berlin, 14059, Germany: Springer Science and Business Media Deutschland GmbH.

Thordsen, Tristan, Matthias Murawski, and Markus Bick. 2020. "How to Measure Digitalization? A Critical Evaluation of Digital Maturity Models." Pp. 358–69 in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 12066 LNCS, edited by H. M., M. M., S. H., P. I., D. Y.K., and Mäntymäki M. ESCP Business School Berlin, Berlin, Germany: Springer.

Vance, David, Mingzhou Jin, Christopher Price, Sachin U. Nimbalkar, and Thomas Wenning. 2023. "Smart Manufacturing Maturity Models and Their Applicability: A Review." *Journal of Manufacturing Technology Management* 34(5):735–70. doi: 10.1108/JMTM-03-2022-0103.

Volf, Ludek, Gejza Dohnal, Libor Beranek, and Jiri Kyncl. 2024. "Navigating the Fourth Industrial Revolution: SBRI – A Comprehensive Digital Maturity Assessment Tool and Road to Industry 4.0 for Small Manufacturing Enterprises." *Manufacturing Technology* 24(4):668–80. doi: 10.21062/mft.2024.074.

Voss, Marleen, David Jaspert, Christian Ahlfeld, and Luke Sucke. 2024. "Developing a

Digital Maturity Model for the Sales Processes of Industrial Projects." *Journal of Personal Selling and Sales Management* 44(1):7–28. doi: 10.1080/08853134.2022.2151014.

Williams, Christopher A., Daniel Schallmo, and Eusebio Scornavacca. 2022. "How Applicable Are Digital Maturity Models To Smes?: A Conceptual Framework And Empirical Validation Approach. *International Journal of Innovation Management* 26(3). doi: 10.1142/S1363919622400102.

Yulianto, Semi, Ford Lumban Gaol, Suhono Harso Supangkat, and Benny Ranti. 2023. "A Comprehensive Model for Enhancing Cybersecurity Resilience and IT Governance Through Red Teaming Exercises." in *Proceedings - ICT 2023 - 29th International Conference on Telecommunications: Next-Generation Telecommunications for Digital Inclusion and Universal Access*. Doctor of Computer Science, Bina Nusantara University, Computer Science Department, Jakarta, 11480, Indonesia: Institute of Electrical and Electronics Engineers Inc.

Zhang, Ganglin, Yongjian Liao, and Shijie Zhou. 2021. "A Privacy-Preserving Revocable Framework in the Deep-Learning-as-a-Service Platform System Based on Non Software as a Service." Pp. 1–9 in *Proceedings - 2021 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing and International Conference on Cybe*. School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China: Institute of Electrical and Electronics Engineers Inc.