INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES

OPEN ACCESS JOURNAL

Vol 15, Issue 4, (2025) E-ISSN: 2225-8329

Tax Digitalisation and Cybercrime: A Systematic Literature Review

Muhammad Amiruddin Azizi Salleh[1], Wan Zurina Nik Abdul Majid[2], Marziana Madah Marzuki[3]

[1]Faculty of Business, UNITAR International University, Tierra Crest, Jalan SS6/3, Kelana Jaya, 47301 Petaling Jaya, Selangor, Malaysia, [2,3]Faculty of Accountancy, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Bukit Ilmu, 18500 Machang, Kelantan, Malaysia

Corresponding Author Email: wzurina@uitm.edu.my

DOI Link: http://dx.doi.org/10.6007/IJARAFMS/v15-i4/26638

Published Online: 10 November 2025

Abstract

This study conducts a systematic literature review (SLR) to examine the relationship between tax digitalisation and cybercrime. While digital technologies have transformed tax administration by improving compliance and efficiency, they have simultaneously introduced new vulnerabilities to cyber threats such as identity theft, phishing, ransomware, and data breaches. Using PRISMA guidelines, this review systematically analysed peer-reviewed articles and official reports published between 2013 and 2022, sourced from databases including Scopus and Web of Science. Out of 223 initial records, 11 studies met the inclusion criteria. The review reveals three dominant themes: (i) the nature and typology of cyber threats in digital tax systems, (ii) the regulatory and institutional responses across jurisdictions, and (iii) the role of technological solutions such as blockchain, artificial intelligence, and secure digital identity systems. The findings highlight that small businesses and individual taxpayers are particularly vulnerable due to limited cyber awareness and insufficient safeguards. Policymakers must balance technological adoption with robust cybersecurity frameworks to safeguard trust in tax systems. This study contributes by consolidating fragmented research and proposing a research agenda for emerging economies. Future work should expand to empirical cross-country analyses and evaluate the effectiveness of cybersecurity measures in sustaining digital tax compliance.

Keywords: Tax Digitalisation, Cybercrime, Tax Identity Theft

Introduction

In line with IR 4.0, tax authorities worldwide have applied sophisticated digital mediums requiring taxpayers to present data promptly. The situation has transformed how businesses manage taxation. The Head of Tax of Ernst & Young Solutions LLP, Singapore emphasised that tax digitalisation constrains time, which poses a challenge for businesses (Ernst & Young Global Ltd., 2020). Therefore, businesses must present accurate information in their system as tax authorities are reviewing the information rapidly with limited time. Given that digital adoption is linked with risks, businesses need to reflect on the extent of security challenges,

such as cyber threats and vulnerabilities. A study on Southeast Asian SMEs by EY revealed that 65.8% of the respondents rated cyber security threats as a core concern when opting for digitalisation (Liew & Choo, 2019). Opting for tax digitalisation could increase cybercrime risks among many small firms and sole traders unless they obtain sufficient government support. Digitalisation refers to the changes in digital technology usage in all aspects of society. Digitalisation also denotes the ability to convert existing products or services into digital variants, therefore offering benefits over tangible products (Henriette et al., 2015; Parviainen et al., 2017).

The growth of technology and innovation in the industry has driven the government to improve its governance and authority, which includes tax administration. Tax administration began in 1986 when electronic tax filing was first piloted by the US Internal Revenue Service. The US Congress then passed the Internal Revenue Service (IRS) Restructuring and Reform Act in 1998, which requires the IRS to convert at least 80% of taxpayers to e-filing by 2007 (Lai & Choong, 2010; Ngugi et al., 2022). Consequently, e-filing has gained popularity globally (including in Malaysia) along with the emergence of user-friendly online websites and tax filing software. The electronic tax filing system is an e-government application used by the authorities to improve tax collection efficiency, where taxpayers submit their tax returns or documents to tax authorities using technology, such as software packages and the Internet (Alibraheem & Abdul-Jabbar, 2016; Muturi & Kiarie, 2015). The use of e-filing complements self-assessment applications in encouraging taxpayers to voluntarily disclose their income. In July 2020, Her Majesty's Revenue and Customs (HMRC) of the United Kingdom upgraded their tax digitalisation by announcing that all VAT-registered businesses must file digitally through Making Tax Digital (MTD) from April 2022, regardless of turnover (ACCA Global, 2022). The MTD requires certain persons to submit VAT returns digitally using MTD-compatible software and keep records in a digital format. The approach enables providing information to the HMRC directly from the accounting system or via bridging software through application programming interfaces (APIs). The MTD aims to tackle the tax gap caused by errors and failure to take reasonable care by eliminating any window for mistakes in preparing and submitting tax returns.

Although the Internet presents several benefits, the drawbacks include hacking, identity theft, digital property violation, and denial of service attacks (Kim et al., 2011). The Internet could ease personal or financial identity theft due to its ability to accumulate and disseminate vast amounts of information electronically (Milne et al., 2004). People who lack knowledge of information security tend to develop insecure applications or create insecure networks that are easier to hack, which highlights the importance of information security for organisations (Alhassan et al., 2017). Increased productivity and opportunity also open avenues to technological dangers, such as cyber-attacks. Business interruption costs and reputational damage following an attack can be detrimental to a business. Furthermore, financial service companies are vulnerable as key targets for cybercriminals (Sheehan et al., 2021).

Cyber risks are defined as financial loss or reputational damage resulting from a failure in an organisation's IT system (The Institute of Risk Management, 2014). Cyber risks are dynamic due to continuous digital innovations, increased use of Internet-enabled devices, and ongoing sophistication of hackers (Sheehan et al., 2021). Vulnerability to cyber-attacks grows

exponentially as companies rely more on electronic data, cloud computing, social media, mobile devices, third-party software, and outsourcing (Sheehan et al., 2021). The data breach average cost has increased by 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022, which is a 12.7% increase from USD 3.86 million in 2020 (IBM, 2022). The digital economy, such as the cluster of interconnected e-wallets, social media, and mobile banking, has created facilitating conditions for cybercrime in Malaysia. Crimes, such as hacking credit cards and other private information, are some of the serious threats to digital businesses (Yin Xia et al., 2021). Meanwhile, phishing is a new technology involving theft from e-wallets by hackers and fraudsters (Leu & Masri, 2019). In the first three months of 2019, the losses from cybercrimes were estimated at RM67.6 million from 2,207 cases (Bernama, 2019). The amount has increased drastically in 2021, with over 20,000 cases involving RM560 million worth of losses (Inus, 2022).

The online security of e-filing is a fundamental factor that influences small business taxpayers to use this type of tax payment system. E-filing users are concerned about the online security of their information due to personal information being used for illegal activities or online scams. The e-filing tax system contains sensitive taxpayer information, thus, secure transactions are paramount (Oluka & Nomlala, 2021). The IRS has also witnessed escalating tax-related identity theft since the US Congress passed the IRS Restructuring and Reform Act in 1998. Tax identity theft has grown and reached its peak, where it became the number one “scam” in the US between 1998 and 2014 (Internal Revenue Service, 2014). The act remains one of the top scam tactics among taxpayers, specifically during the pandemic (Internal Revenue Service, 2021).

Tax identity theft is a form of identity stealing that involves the illegal use of a potential taxpayer’s identity (usually the Social Security number) to fraudulently file tax returns and claim refunds (Internal Revenue Service, 2022). Meanwhile, identity theft involves stealing personally identifiable information, such as a social security number, date of birth, and the mother’s maiden name, to fraudulently establish credit, accrue debt, or seize existing financial accounts (U.S. Government Accountability Office, 2002). Tax identity theft starts when an offender acquires a victim’s social security number and electronically files for a tax return on behalf of the victim without their consent. The situation happens early in the tax season as the offender intends to surpass the victim, who is the genuine owner of the social security number. The offender would submit false information on the income earned and tax paid in the year and claim eligibility for various tax credits (such as the earned income tax credit) to maximise the total tax refund. The offender would request the IRS to deposit the refund amount into a direct-deposit bank account or to mail a prepaid card or check. The IRS would usually overlook the fraudulent refund until a second tax return filing is later received from the actual owner (victim) of the stolen social security number. In this situation, the offender would have already received and withdrawn the refund and disappeared.

E-filing has eased business owners in various ways, such as simplified electronic data entry, remote filing, and shortened lead time for a refund (Salleh et al., 2025). Nonetheless, these features contribute to the prevalence of tax identity theft. An offender can file multiple tax returns in a short time (using simplified electronic data entry) remotely from anywhere (including foreign countries) without revealing their identity and with a lower risk of apprehension and prosecution (Ngugi et al., 2022). Apart from increased tax-return filing and

general identity theft, the prevalence of tax identity theft is a result of the rising adoption of e-filing technology, including self e-filing and direct deposit (Ngugi et al., 2022).

Based on the comments above, only a few studies have looked at the direct connection between tax digitalisation and cybercrime. These investigations disregarded the more general elements of cybercrime, such as information security, phishing, malware, and ransomware, and exclusively focused on tax identity theft through the adoption of e-filing (Ngugi et al., 2022). The level of tax digitalisation adopted in Malaysia also remains unexplored. Therefore, the current study attempted to examine and bridge the literature gap by investigating state-of-the-art research in tax digitalisation in Malaysia. Specifically, the study investigated why tax digitalisation is exposed to cybercrime and future research trends on tax digitalisation and cybercrime. The study aligns with the national priority of the government on cybersecurity and Sustainable Development Goal (SDG) 9 on industry, innovation, and infrastructure. A systematic literature review was performed on the implementation of tax digitalisation and its exposure to cybercrime. The findings contribute to the new research area and the Council of Digital Economy in revising or formulating the digital policy to encourage national digital awareness.

Methodology

The systematic review structure is based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework (Page et al., 2021). The PRISMA is a protocol for reporting systematic reviews comprising a checklist and a flow diagram developed in the life science field to increase literature review transparency and accuracy (Page et al., 2021). The study selected PRISMA over other existing protocols due to its comprehensiveness, use in several disciplines worldwide, and potential to increase consistency across reviews (Liberati et al., 2009; Pahlevan-Sharif et al., 2019). The search was conducted from 10 to 17 June 2022. Only articles published in the last 10 years were considered due to the continuous development of cyber risks and their countermeasures. Additionally, the study only included articles published in peer-reviewed journals written in English.

Design a Plan

The study followed Jesson et al.'s (2011) protocol, which involves the following steps:

- Define a research question
- Search for the literature
- Time frame
- Apply exclusion and inclusion criteria
- Conduct a quality assessment
- Discuss the results

Define the Research Question

A systematic review process is based on the research questions that define the subject, object, and scope of research (Booth et al., 2016). Accordingly, the following research questions were constructed:

RQ1. What is the state-of-the-art research in tax digitalisation?
RQ2. How is tax digitalisation exposed to cybercrime?
RQ3. What are the future research trends of tax digitalisation and cybercrime?

Search for the Literature

The study selected Scopus and WoS as the sources of information to ensure scientific robustness and inclusivity. The preliminary set of keywords related to the topic was tax, digitalisation, e-filing, cybercrime, and identity theft. The study excluded non-English articles to avoid comprehension issues and improve the research replicability for the international community. Moreover, a 10-year time filter was applied. The Scopus research string is defined as follows:

(TITLE-ABS-KEY (*tax* AND *digitalisation*) OR TITLE-ABS-KEY (*tax* AND *e-filing*) OR TITLE-ABS-KEY (*tax* AND *cybercrime*) OR TITLE-ABS-KEY (*e-filing* AND *cyber-security*) OR TITLE-ABS-KEY (*e-filing* AND *cybercrime*) OR TITLE-ABS-KEY (*tax* AND *cyber-security*) OR TITLE-ABS-KEY (*tax* AND *identity-theft*)) AND (LIMIT-TO (DOCTYPE , *"ar"*)) AND (LIMIT-TO (PUBYEAR , *2022*) OR LIMIT-TO (PUBYEAR , *2021*) OR LIMIT-TO (PUBYEAR , *2020*) OR LIMIT-TO (PUBYEAR , *2019*) OR LIMIT-TO (PUBYEAR , *2018*) OR LIMIT-TO (PUBYEAR , *2017*) OR LIMIT-TO (PUBYEAR , *2016*) OR LIMIT-TO (PUBYEAR , *2015*) OR LIMIT-TO (PUBYEAR , *2014*) OR LIMIT-TO (PUBYEAR , *2013*)) AND (LIMIT-TO (LANGUAGE , *"English"*))

The WoS research string is as follows:

(TS=(tax AND digitalisation) OR TS=(tax AND e-filing) OR TS=(tax AND cybercrime) OR TS=(e-filing AND cyber-security) OR TS=(e-filing AND cybercrime) OR TS=(tax AND cyber-security) OR TS=(tax AND identity-theft) OR TS=(e-filing AND identity-theft)) AND (PY==("2022" OR "2021" OR "2020" OR "2019" OR "2017" OR "2018" OR "2016" OR "2015" OR "2014" OR "2013") AND DT==("ARTICLE") AND OAJ==("ALL OPEN ACCESS") AND LA==("ENGLISH"))

Time Frame

Studies published between 2013 and 2022 were considered to capture the evolution of digital taxation and cybercrime

Apply Inclusion and Exclusion Criteria

A study needs to manually analyse the titles, abstracts, keywords, and the full article text (if necessary) to determine which articles should be excluded due to irrelevance (Booth et al., 2016). Hence, the excluded articles include those not pertinent to the research questions that had been erroneously captured by the research string. A total of 39 articles were considered relevant as they were linked to the research questions. The study manually assessed the relevance of each article for further refinement by considering the pertinence of the title, keywords, and abstracts based on the research questions. No rigid quantitative rules were applied, but the study considered the relative impact within the specific research area. Overall, 25 studies were considered less relevant, while three of the 14 full-text articles were excluded due to unavailability. Hence, 11 full-text items were thoroughly analysed for the review as depicted in Figure 1.

Conduct a Quality Assessment

Considering that tax digitalisation and cybercrime are recent topics, the study included papers published in journals with moderate to low impact factors.

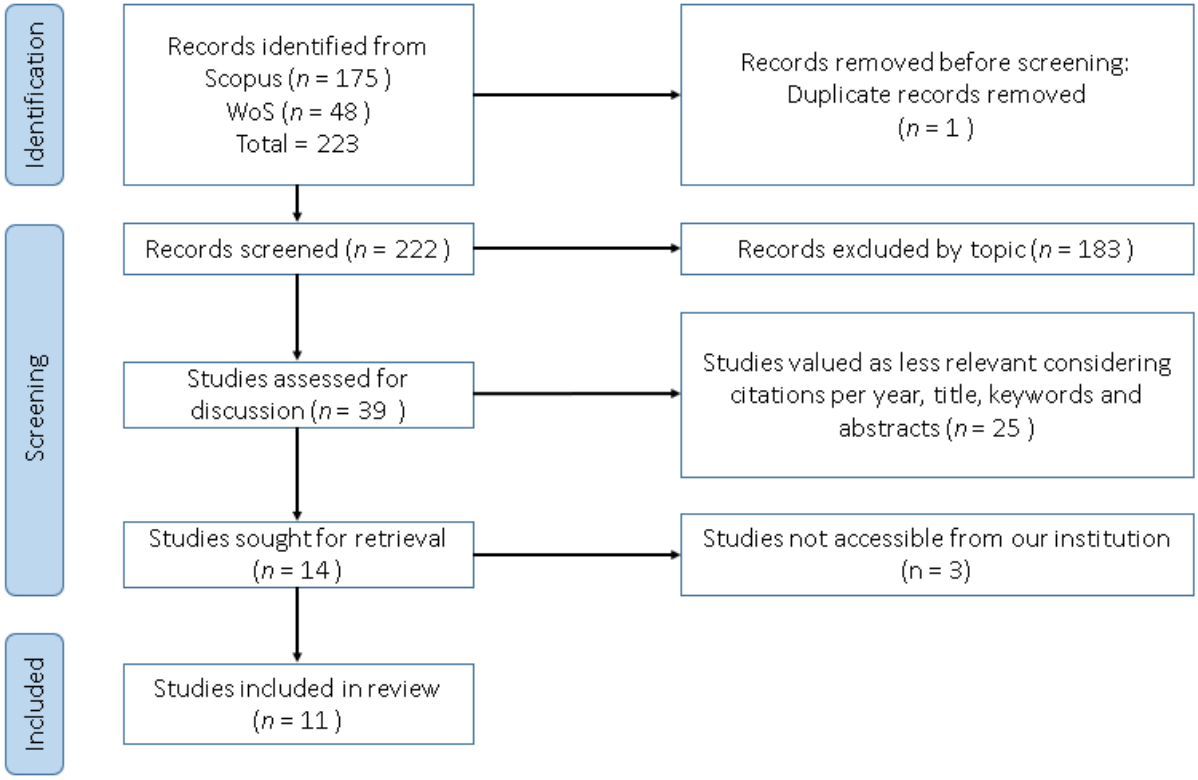

Figure 1: The PRISMA Diagram

Findings

Review of the Bibliography of the Selected Literature

Most of the reviewed articles and journals in Table 1 are impactful to the academic society. The data from the third column, "citations", is the number of publications (within the same index) citing the article. The data were derived from the Scopus and WoS databases. The most cited article was Veeramootoo et al. (2018) published in the Government Information Quarterly with 118 citations, while the least cited articles were from Hermanto et al. (2022), Hidayat et al. (2022), Hultgren et al. (2022), and Ngugi et al. (2022) with 0 citations. The second most cited paper was Tahar et al. (2020) with 14 citations, followed by Burnes et al. (2020) and Lagodiienko and Yakushko (2021) with seven citations, Leighton-Daly (2019) with two citations, and Olowska et al. (2020) and Utama et al. (2022) with one citation. The fifth column of Table 1 lists the impact of the journal on the body of knowledge measured by normalised impact calculations, namely Source-Normalised Impact per Paper (SNIP) for Scopus and Journal Citations Indicator (JCI) for WoS journals. The most impactful journal is the Government Information Quarterly with a 2.38 impact factor, while the lowest impact factor is 0.265 for the eJournal of Tax Research. The review retrieved 11 articles indexed in Scopus and WoS databases, which were published mainly by reputable academic publishers.

Table 1
Selected Previous Studies in SCOPUS and WOS Databases

No.	Article	Citations	Journal	Impacts
1.	What determines the success of an e-government service? Validation of an integrative model of e-filing continuance usage	118	Government Information Quarterly	2.38
2.	Perceived Ease of Use, Perceived Usefulness, Perceived Security and Intention to Use E-Filing: The Role of Technology Readiness	14	Journal of Asian Finance, Economics and Business	N/A
3.	Risk and protective factors of identity theft victimisation in the United States	7	Preventive Medicine Reports	0.71
4.	Digital Innovations in Taxation: Bibliometric Analysis	7	Marketing and Management of Innovations	N/A
5.	Identity theft and tax crime: has technology made it easier to defraud the revenue?	2	eJournal of Tax Research	0.265
6.	Effect of Religiosity, Perceived Risk, and Attitude on Tax Compliance Intention Moderated by e-Filing	1	International Journal of Financial Studies	1.063
7.	The Digitalisation of Tax Administration in China, India and Korea (Rep.) in the Fourth Industrial Revolution	1	Bulletin for International Taxation	0.365
8.	Reducing tax identity theft by identifying vulnerability points in the electronic tax filing process	0	Information & Computer Security	0.945
9.	Identity theft tax refund fraud in the United States	0	eJournal of Tax Research	0.265
10.	Taxpayers' adoption of online tax return reporting: extended meta-UTAUT model perspective	0	Cogent Business & Management	N/A
11.	The effect of attitude and religiosity on tax compliant intention moderated by the utilisation of e-Filing	0	Journal of Financial Services Marketing	N/A

Discussion

Lagodiienko and Yakushko (2021) and Olowska et al.'s (2020) research presents a clear depiction of taxation and digitalisation using a bibliometric method that demonstrates the trend and development in the field. In the last 60 years, the number of scientific publications on taxation has increased extensively, with approximately 249 publications in 1990, 639 publications in 2000, 1,232 publications in 2010, and 2,010 publications in 2020 (Lagodiienko & Yakushko, 2021). The data presents promising growth in taxation every year. This positive development in the sphere of taxation and the interest of researchers is caused by the economic movement in the world, the constant emergence of industries across the globe, policy changes, and technological evolution. One primary aspect of technology is the

adoption of digital media by all parties, such as entrepreneurs, the government, and the public. The situation demonstrates the beginning of a digital era, such as the Internet of Things (IoT), digitalisation, the Internet, and big data. Lagodiienko and Yakushko (2021) added that the enormous growth in the scientific research on digitalisation is depicted through the increase in the number of Scopus publications searched by the word "digitalisation" that increased from 25 documents in 2014 to 227 in 2017, and 945 in 2020.

Tax authorities adapt to technological evolution by moving traditional taxation into a more advanced and sophisticated system. Specifically, electronic tax filing was first introduced in 1986 when it was piloted by the US Internal Revenue Service. Limited studies are available on the direct relationship between tax and digitalisation, as the topic is still new. For instance, Lagodiienko and Yakushko (2021) emphasize that only 18 papers are identified by using the searching term "digitalisation" and "taxes" in the Scopus database at the end of 2021. Nevertheless, the current study revealed 141 articles that indirectly discussed the issues of taxes and digitalisation, thus proving researchers' interest in the topic. Lagodiienko and Yakushko (2021) propose the following to encourage further research: 1) improving the interaction quality between tax authorities and taxpayers and ensuring trust between them, 2) automation of all processes without exception in the collection of taxes, fees, and other payments, 3) reducing the influence of the human factor on the tax system that functions to reduce the manifestation of corruption, and 4) determining the role of information technology (IT) in ensuring the competitiveness of national tax systems worldwide. Therefore, the results addressed the first question of what the state-of-the-art research in tax digitalisation is.

The second research question relates to how tax digitalisation is exposed to cybercrime. The global economic loss from cybercrime was estimated at USD 945 billion in 2020 (Lewis et al., 2020). Cyber vulnerabilities pose significant corporate risks, including business interruption, breach of privacy, and financial losses (Sheehan et al., 2019). Cyber risks are "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems" (Cebula et al., 2014). Common cyber risk cases include data breaches and cyberattacks (Agrafiotis et al., 2018). Recent industry reports have highlighted the increasing exposure and potential impacts of cyber risks, such as Allianz Global Corporate and Specialty (2022) and the World Economic Forum (2022). Cyberattacks on critical infrastructures were ranked top 5 in the World Economic Forum Global Risk Report. The evolving modes of a cyberattack include ransomware, malware, and distributed denial-of-service (DDoS). For example, the ransomware attack on the Colonial Pipeline collapsed the 5,500-mile pipeline system that delivers 2.5 million barrels of fuel per day and critical liquid fuel infrastructure from oil refineries to states along the US East Coast (Brower & McCormick, 2021).

Ransomware is another form of cyberattack. The WannaCry ransomware was launched by cybercriminals in 2017, which attacked Windows software and seized user data in exchange for Bitcoin cryptocurrency (Smart, 2018). Data breaches also incur high costs. The act denotes a "security incident where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorised individual" (Khan et al., 2021). E-filing poses a threat to the users on the security of their information due to cases involving stolen personal information and usage for illegal activities or online scams. Secure transactions are critical as

the e-filing tax system contains sensitive taxpayer information (Oluka & Nomlala, 2021). Users' perceived security of a system influences their intention to use it. Users who perceive the system as a high risk in terms of security tend to avoid the system (Tahar et al., 2020). Perceived security is the users' perception of the function and control of their personal data information in an online system. Essentially, personal data information security is the main concern among users (Hermanto et al., 2022; Hidayat et al., 2022; Tahar et al., 2020; Utama et al., 2022; Veeramootoo et al., 2018). The situation relates to the case of identity theft among taxpayers. Identity theft tax refund fraud in the US has been an issue of the IRS over the last 30 years, including at the state level (Hultgren et al., 2022). The first recorded instance of tax refund fraud in the US occurred in 1988, when the Los Angeles Times reported that Donald Penrod was indicted for fraudulently filing tax forms electronically to receive an illegitimate refund (Nigrini & Peters, 2018).

The increased Identity Theft tax refund fraud occurred subsequent to the information digital age, which made personal identifiable information (PII) easier to obtain. Furthermore, the massive growth in federal and state tax return e-filing allowed this type of fraud to be perpetuated on a large scale. Federal tax e-filing has drastically increased throughout the 21st century. Only 58% of returns were filed electronically in 2008, which has escalated to 81% in 2012 and over 90% by 2016 (Brink & Hansen, 2020; Brody et al., 2014). Under the Identity Theft and Assumption Deterrence Act of 1998, a person has committed a crime if they knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit or to aid or abet any unlawful activity that constitutes a violation of Federal law or a felony under any applicable State or local law (US Federal Trade Commission, 1998). Additionally, identity theft has been the top complaint in the Federal Trade Commission (FTC) Sentinel database for 21 years (2001–2021) (US Federal Trade Commission, 2022).

The IRS maintains a list of the top 12 tax scams (Internal Revenue Service, 2021) to alert taxpayers. Tax identity theft cases have risen over the years and remained among the top five scams on this list for over eight years (Ngugi et al., 2022). In 2012, 2013, and 2016, tax identity theft was the top scam committed and the third top scam from 2015 and 2017 to 2019 (Ngugi et al., 2022). The reports demonstrate that tax identity theft is a prominent fraud. Ultimately, more in-depth research on the topic is required to provide scholars and practitioners with a better understanding of the underlying issues to mitigate the implications.

Conclusion

This systematic review confirms that while tax digitalisation enhances efficiency and compliance, it simultaneously exposes taxpayers and institutions to sophisticated cyber threats. The analysis shows that identity theft, phishing, ransomware, and insider manipulation are among the most prevalent risks. Existing literature also emphasises the challenges faced by small firms and individual taxpayers, who often lack sufficient cyber resilience.

From a policy perspective, the findings stress the urgent need for integrated frameworks that combine digital innovation with strong cybersecurity, continuous monitoring, and public awareness campaigns. Advanced technologies such as blockchain and artificial intelligence offer promising solutions, but their adoption remains uneven across jurisdictions.

The main contribution of this review is the consolidation of fragmented studies into three thematic clusters: threats, responses, and solutions, providing a clearer conceptual lens for future research. Key research gaps include the lack of comparative empirical studies across countries, limited exploration of emerging technologies in tax security, and insufficient focus on behavioural aspects of taxpayer vulnerability.

Future studies should adopt interdisciplinary approaches, combining insights from accounting, information systems, and cybersecurity, to design resilient tax digitalisation frameworks. For practitioners and policymakers, the review highlights that digital transformation in taxation cannot succeed without embedding robust cybersecurity safeguards.

Theoretical and Contextual Contribution

This study contributes theoretically by extending the discourse on digital taxation through the integration of cybersecurity risk dimensions within the framework of tax digitalisation. Existing literature has primarily focused on e-filing adoption, compliance behaviour, and technological readiness, but has given limited attention to the intersection between digital tax systems and cyber vulnerabilities. By consolidating fragmented insights from taxation, information systems, and cybersecurity research, this review advances a more holistic conceptual understanding of the "digital tax–cybercrime nexus." The proposed thematic clusters, threats, institutional responses, and technological safeguards form a theoretical foundation that future scholars can operationalise in empirical models of digital tax resilience. Contextually, the research offers significant implications for emerging economies, particularly Malaysia, where digital transformation in tax administration is rapidly accelerating amid limited cybersecurity awareness among SMEs and individual taxpayers. The study provides a contextualised understanding of how institutional readiness, regulatory enforcement, and technological infrastructure collectively influence cyber exposure in digital tax environments. Therefore, this research not only fills an academic gap but also provides a practical framework to guide policymakers, regulators, and practitioners in designing secure, trust-enhancing tax digitalisation ecosystems aligned with national digital economy agendas.

Acknowledgement

The authors wish to express their gratitude to the FRGS for funding this research project through the FRGS/1/2021/SS01/UITM/02/40.

References

Association of Chartered Certified Accountants (ACCA). (2022). *Making tax digital for VAT is coming — are you ready?* https://www.accaglobal.com/my/en/technical-activities/technical-resources-search/2022/March/making-tax-digital-for-vat-are-you-ready.html

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), tyy006. https://doi.org/10.1093/cybsec/tyy006

Alhassan, M. M., Adjei-Quaye, A., & Alhassan, M. M. (2017). Information security in an organization. *International Journal of Computer.* https://www.researchgate.net/publication/314086143

Alibraheem, M., & Abdul-Jabbar, H. (2016). Electronic tax filing adoption and its impact on tax employees' performance in Jordan: A proposed framework. *World Applied Sciences Journal, 34*(3), 393–399. https://doi.org/10.5829/idosi.wasj.2016.34.3.15671

Allianz Global Corporate & Specialty. (2022). *Allianz risk barometer 2022.* Allianz SE. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2022.pdf

Bernama. (2019, April 8). RM67.6 million lost to cybercrimes in Q1 2019. *New Straits Times.* https://www.nst.com.my/news/crime-courts/2019/04/482208/rm676-million-lost-cyber-crimes-q1-2019

Booth, A., Papaioannou, D., & Sutton, A. (2016). *Systematic approaches to a successful literature review* (2nd ed.). SAGE Publications.

Brink, W. D., & Hansen, V. J. (2020). The effect of tax authority-developed software on taxpayer compliance. *Accounting Horizons, 34*(1), 1–18. https://doi.org/10.2308/ACCH-52511

Brody, R. G., Haynes, C. M., & Mejia, H. (2014). Income tax return scams and identity theft. *Accounting and Finance Research, 3*(1), 90–97. https://doi.org/10.5430/afr.v3n1p90

Brower, D., & McCormick, M. (2021, May 13). Colonial pipeline resumes operations following ransomware attack. *Financial Times.* https://www.ft.com/content/b6ac99ea-d7c6-49dd-b7d7-1284ce2e85c0

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports, 17,* 101058. https://doi.org/10.1016/j.pmedr.2020.101058

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). *A taxonomy of operational cyber security risks version 2.* Software Engineering Institute. http://www.sei.cmu.edu

Ernst & Young Global Ltd. (2020). *How digitalisation is changing corporate income tax.* https://www.ey.com/en_kz/tax/how-digitalisation-is-changing-corporate-income-tax

Henriette, E., Feki, M., & Boughzala, I. (2015). The shape of digital transformation: A systematic literature review. In *Proceedings of the 9th Mediterranean Conference on Information Systems.* https://aisel.aisnet.org/mcis2015/10

Hermanto, A. H., Windasari, N. A., & Purwanegara, M. S. (2022). Taxpayers' adoption of online tax return reporting: Extended meta-UTAUT model perspective. *Cogent Business & Management, 9*(1), 2110724. https://doi.org/10.1080/23311975.2022.2110724

Hidayat, K., Utama, M. S., Nimran, U., & Prasetya, A. (2022). The effect of attitude and religiosity on tax compliant intention moderated by the utilization of e-filing. *Journal of Financial Services Marketing.* https://doi.org/10.1057/s41264-022-00171-y

Hultgren, A., Hasseldine, J., & Nash, J. (2022). Identity theft tax refund fraud in the United States. *eJournal of Tax Research, 19*(2), 424–437.

IBM. (2022). *Cost of a data breach report 2022 – Malaysia.* IBM Security. https://www.ibm.com/my-en/security/data-breach

Internal Revenue Service. (2014). *IRS releases the "Dirty Dozen" tax scams for 2014: Identity theft, phone scams lead list.* https://www.irs.gov/newsroom/irs-releases-the-dirty-dozen-tax-scams-for-2014-identity-theft-phone-scams-lead-list

Internal Revenue Service. (2021). *IRS announces "Dirty Dozen" tax scams for 2021.* https://www.irs.gov/newsroom/irs-announces-dirty-dozen-tax-scams-for-2021

Internal Revenue Service. (2022). *Taxpayer guide to identity theft.* https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft

Inus, K. (2022, August 11). RM560mil lost due to cyber crimes last year, says Home Ministry. *The Star.* https://www.thestar.com.my/news/nation/2022/08/11/rm560mil-lost-due-to-cyber-crimes-last-year-says-home-ministry

Jesson, J., Matheson, L., & Lacey, F. M. (2011). *Doing your literature review: Traditional and systematic techniques.* SAGE Publications.

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: An integrated risk model. *Information and Management, 58*(1), 103392. https://doi.org/10.1016/j.im.2020.103392

Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems, 36*(3), 675–705. https://doi.org/10.1016/j.is.2010.11.003

Lagodiienko, N., & Yakushko, I. (2021). Digital innovations in taxation: Bibliometric analysis. *Marketing and Management of Innovations, 5*(3), 66–77. https://doi.org/10.21272/mmi.2021.3-06

Lai, M. L., & Choong, K. F. (2010). Motivators, barriers and concerns in adoption of electronic filing system: Survey evidence from Malaysian professional accountants. *American Journal of Applied Sciences, 7*(4), 562–567. https://doi.org/10.3844/ajassp.2010.562.567

Leighton-Daly, M. (2019). Identity theft and tax crime: Has technology made it easier to defraud the revenue? *eJournal of Tax Research, 16*(3), 578–593.

Leu, J. F. Y., & Masri, R. (2019). Dilemma of SMEs in business digitization: A conceptual analysis of retail SMEs in Malaysia. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 10*(7), 971–981. https://doi.org/10.14456/ITJEMAST.2019.88

Lewis, J. A., Smith, Z. M., & Lostri, E. (2020). *The hidden costs of cybercrime.* Center for Strategic and International Studies. https://www.csis.org/analysis/hidden-costs-cybercrime

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate healthcare interventions: Explanation and elaboration. *BMJ, 339,* b2700. https://doi.org/10.1136/bmj.b2700

Liew, N. S., & Choo, E. C. (2019). *Redesigning for the digital economy: A study of SMEs in Southeast Asia.* Ernst & Young. https://www.ey.com/en_sg/growth/growth-markets-services/ey-smes-in-southeast-asia-redesigning-for-the-digital-economy

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs, 38*(2), 217–232.

Muturi, H. M., & Kiarie, N. (2015). Effects of online tax system on tax compliance among small taxpayers in Meru County, Kenya. *International Journal of Economics, Commerce and Management, 3*(12), 280–290. http://ijecm.co.uk/

Ngugi, B. K., Hung, K. T., & Li, Y. J. (2022). Reducing tax identity theft by identifying vulnerability points in the electronic tax filing process. *Information & Computer Security, 30*(2), 173–189. https://doi.org/10.1108/ICS-05-2021-0056

Nigrini, M. J., & Peters, J. S. (2018). Identity theft tax refund fraud: An analysis of the fraud schemes using IRS investigation summaries. *Journal of Forensic & Investigative Accounting, 10*(1), 1–25.

Olowska, M., Peshori, P., & Lan, S. (2020). The digitalisation of tax administration in China, India and Korea in the Fourth Industrial Revolution. *Bulletin for International Taxation, 74*(8), 421–432.

Oluka, A., & Nomlala, B. (2021). Tax compliance costs and the use of e-filing by SMMEs. *Journal of Accounting and Management, 11*(2), 50–61.

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., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372,* n71. https://doi.org/10.1136/bmj.n71

Pahlevan-Sharif, S., Mura, P., & Wijesinghe, S. N. R. (2019). A systematic review of systematic reviews in tourism. *Journal of Hospitality and Tourism Management, 39,* 158–165. https://doi.org/10.1016/j.jhtm.2019.04.001

Parviainen, P., Tihinen, M., Kääriäinen, J., & Teppola, S. (2017). Tackling the digitalisation challenge: How to benefit from digitalisation in practice. *International Journal of Information Systems and Project Management, 5*(1), 63–77. https://doi.org/10.12821/ijispm050104

Salleh, M. A. A., Majid, W. Z. N. A., Marzuki, M. M., Zakaria, M., & Ibrahim, Z. (2025). The acceptance of digital tax administration among SMEs in Malaysia: The application of UTAUT model. *Pakistan Journal of Life and Social Sciences, 23*(1), 44–58. https://doi.org/10.57239/PJLSS-2025-23.1.00449

Sheehan, B., Murphy, F., Kia, A. N., & Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research, 24*(12), 1619–1638. https://doi.org/10.1080/13669877.2021.1900337

Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice, 124,* 523–536. https://doi.org/10.1016/j.tra.2018.06.033

Smart, W. (2018). *Lessons learned review of the WannaCry ransomware cyber attack.* National Audit Office. https://www.nationalarchives.gov.uk/doc/open-government-licence/

Tahar, A., Riyadh, H. A., Sofyani, H., & Purnomo, W. E. (2020). Perceived ease of use, perceived usefulness, perceived security and intention to use e-filing: The role of technology readiness. *Journal of Asian Finance, Economics and Business, 7*(9), 537–547. https://doi.org/10.13106/JAFEB.2020.VOL7.NO9.537

The Institute of Risk Management. (2014). *Cyber risk resources for practitioners.* https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf

U.S. Federal Trade Commission. (1998). *Identity Theft and Assumption Deterrence Act.* https://www.ftc.gov/legal-library/browse/rules/identity-theft-assumption-deterrence-act-text

U.S. Federal Trade Commission. (2022). *Consumer Sentinel Network data book 2021.* https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf

U.S. Government Accountability Office. (2002). *Identity theft: Greater awareness and use of existing data are needed.* https://www.gao.gov/products/gao-02-766

Utama, M. S., Nimran, U., Hidayat, K., & Prasetya, A. (2022). Effect of religiosity, perceived risk, and attitude on tax compliant intention moderated by e-filing. *International Journal of Financial Studies, 10*(1), 1–14. https://doi.org/10.3390/ijfs10010008

Veeramootoo, N., Nunkoo, R., & Dwivedi, Y. K. (2018). What determines success of an e-government service? Validation of an integrative model of e-filing continuance usage. *Government Information Quarterly, 35*(2), 161–174. https://doi.org/10.1016/j.giq.2018.03.004

World Economic Forum. (2022). *The global risks report 2022.* World Economic Forum. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Yin Xia, L., Nor Aziati, A. H., Hamid Ahmad, A., & Seah, S. (2021). The factors and challenges affecting digital economy in Malaysia. In *Conference on Management, Business, Innovation, Education and Social Science.* https://www.researchgate.net/publication/352118174