World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Research Article)

Digital Taxation and Cybersecurity: Opportunities and Threats

Olubukola Sanni *

Global Mobility Tax Leader, Baker Hughes, Lagos, Nigeria.

World Journal of Advanced Research and Reviews, 2025, 28(02), 1096-1106

Publication history: Received on 25 September 2025; revised on 10 November 2025; accepted on 13 November 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.2.3832

Abstract

The rapid digitalization of taxation systems has fundamentally transformed how governments collect revenue, enhance transparency, and improve taxpayer compliance. Emerging technologies such as blockchain, artificial intelligence, cloud platforms, and data analytics have enabled real-time monitoring, automated tax reporting, and improved detection of fraud and tax evasion. Digital taxation further supports cross-border information sharing and strengthens global tax governance, particularly under frameworks addressing the digital economy and multinational enterprises. However, these advancements introduce heightened cybersecurity risks that challenge the confidentiality, integrity, and availability of taxpayer data. Cybercriminals increasingly target tax administrations through phishing, ransomware, identity theft, data manipulation, and sophisticated fraud schemes that exploit digital vulnerabilities. The interconnectedness of government systems and third-party service providers expands the attack surface, while gaps in regulatory enforcement, weak authentication controls, and low cybersecurity literacy among users exacerbate threat exposure. Additionally, reliance on digital infrastructure raises concerns regarding digital sovereignty, privacy rights, and the resilience of national tax administration services during cyber incidents. This paper examines the dual nature of digital taxation—highlighting opportunities for improved efficiency and anti-evasion measures alongside risks requiring robust cyber defense capabilities.

Keywords: Digital taxation; Cybersecurity; Tax administration; Cybercrime; Data protection; E-government; Risk mitigation

1. Introduction

The evolution of taxation systems from paper-based mechanisms to highly digitized frameworks represents one of the most transformative developments in modern public administration. Digital taxation has emerged as a cornerstone of e-governance, enhancing fiscal efficiency, transparency, and taxpayer convenience through the integration of digital tools and technologies. The increasing use of electronic filing (e-filing), online payment systems, and automated compliance monitoring platforms has streamlined tax processes, reduced administrative burdens, and minimized human error. Governments across the globe are embracing digital platforms to facilitate seamless interaction between taxpayers and tax authorities, thus improving service delivery and ensuring equitable tax collection. The Organization for Economic Cooperation and Development (OECD) and other international bodies have further encouraged digital tax reforms to strengthen global tax governance, particularly in addressing the challenges posed by digital multinational enterprises (MNEs) that operate across jurisdictions without a physical presence. However, as taxation systems become increasingly digitalized, they also become more susceptible to cyber threats that endanger data confidentiality, integrity, and availability. Tax authorities, due to their vast repositories of sensitive financial and personal information, have become prime targets for cybercriminals.

Threats such as ransomware attacks, phishing scams, identity theft, and data manipulation have intensified, exposing critical vulnerabilities in tax infrastructure. These cyber incidents not only disrupt tax operations but also undermine

* Corresponding author: Olubukola Sanni

public confidence in government institutions and compromise financial integrity. For example, large-scale breaches of taxpayer data in recent years have highlighted weaknesses in digital tax security protocols and emphasized the urgent need for robust cybersecurity frameworks. Inadequate encryption, weak access controls, and the increasing use of third-party software further exacerbate exposure to cyber risks. Moreover, the convergence of tax technology and cyber risk introduces complex governance challenges. Governments must balance the need for transparency and data accessibility with stringent privacy and security requirements. The global nature of digital transactions also complicates taxation, as cross-border data flows require harmonized international cybersecurity standards and cooperation. Digital sovereignty issues—where national data is processed or stored on foreign servers—raise additional concerns about control and jurisdiction. In this context, cybersecurity is no longer an optional component of tax administration; it is a fundamental pillar of fiscal sustainability and digital trust. This study explores the intricate relationship between digital taxation and cybersecurity, identifying the opportunities that digitalization offers alongside the threats that accompany it.

By analyzing global trends, emerging technologies, and evolving attack vectors, the research seeks to highlight the need for comprehensive, multi-layered cyber defense mechanisms in tax systems. It emphasizes how integrating advanced technologies—such as artificial intelligence, blockchain, and zero-trust security architectures—can strengthen resilience and ensure secure tax administration. The findings underscore that while digital transformation is inevitable and beneficial, its success depends on governments' ability to anticipate, prevent, and respond to cyber threats effectively. Strengthening cybersecurity within digital taxation is thus not only a technical necessity but also a strategic imperative for economic stability, public confidence, and long-term governance sustainability. Furthermore, the increasing adoption of data-driven tax enforcement tools—such as predictive analytics for identifying tax evasion patterns and automated risk-scoring systems—introduces both powerful capabilities and ethical responsibilities. While these intelligent systems enhance compliance monitoring and revenue recovery, they also raise critical concerns related to algorithmic transparency, accountability, and the protection of taxpayers' rights. Misuse or manipulation of digital tax tools could lead to biased assessments, wrongful penalties, or unauthorized surveillance. Thus, cyber governance in taxation must incorporate not only technical safeguards but also strong legal, regulatory, and ethical frameworks that ensure responsible use of digital resources.

The broader digital economy also intensifies challenges for tax jurisdictions. The proliferation of cryptocurrency transactions, decentralized finance (DeFi) systems, and virtual assets requires governments to redefine tax rules and invest in cybersecurity solutions capable of tracking and validating digital value exchanges. As cybercriminals exploit anonymity in these systems for tax evasion and money laundering, tax agencies must rapidly adapt to the shifting threat landscape. Collaborative global initiatives, such as information-sharing agreements and harmonized digital tax regulations, become essential in confronting threats that transcend national borders. In many developing countries, the digital transformation of taxation presents significant opportunities for broadening the tax base and improving fiscal capacity. Yet, limited cybersecurity maturity, outdated infrastructure, and insufficient technical expertise may expose such economies to disproportionately higher risks. Bridging these digital and security gaps requires strategic investments in workforce training, resilient IT architecture, and public awareness programs that empower taxpayers to securely engage with digital tax services. Overall, digital taxation represents a dynamic intersection of innovation and risk. Its successful implementation demands a holistic approach that integrates secure technologies, proactive risk management, international cooperation, and continuous policy evolution. By addressing cybersecurity as a central component of digital tax transformation, governments can unlock the full potential of technology while safeguarding public trust and national economic security.

2. Literature Review

The digital transformation of taxation systems has been widely examined in academic and policy literature, with scholars emphasizing both its transformative potential and the accompanying cybersecurity risks. According to OECD (2020), the integration of digital technologies in tax administration—such as e-filing, e-payment platforms, and real-time transaction monitoring—has revolutionized how governments manage fiscal operations. These systems enhance efficiency, transparency, and compliance by automating processes and reducing opportunities for human error or corruption. Similarly, Gupta and Keen (2022) argue that digitalization supports equitable taxation by expanding the tax base, simplifying taxpayer interactions, and improving access to data-driven decision-making tools. However, they also note that the rapid deployment of digital solutions often outpaces the establishment of adequate cybersecurity measures, leaving critical vulnerabilities in national tax infrastructures. Researchers such as Alabede (2021) have highlighted that cybersecurity in tax administration is not merely a technical challenge but a governance issue. With tax authorities holding vast repositories of personally identifiable information (PII) and financial data, breaches can have severe economic, legal, and reputational consequences. Studies on cyberattacks targeting government agencies reveal that ransomware and phishing remain the predominant forms of attack, often facilitated by weak access controls, poor encryption, and limited employee awareness. For instance, the 2017 ransomware attacks on European tax offices underscored how outdated software and insufficient patch management could paralyze entire national revenue systems. In addition, identity theft and fraudulent tax refunds have become increasingly common, exploiting the vulnerabilities inherent in online tax filing platforms.

The literature also underscores the global nature of digital taxation challenges. Taxation in the digital economy—especially with respect to multinational enterprises (MNEs) and cross-border digital services—has spurred extensive debate regarding data privacy, jurisdictional authority, and equitable revenue distribution. Studies by the World Bank (2021) and IMF (2023) have emphasized that as countries implement digital tax frameworks, harmonized cybersecurity regulations and shared defense mechanisms are essential to protect the integrity of global fiscal data. Without such cooperation, cybercriminals exploit disparities in cybersecurity standards between nations, using weakly protected systems as entry points into more secure networks. Technological innovation has been central to improving tax security. Scholars like Martínez and Silva (2022) advocate for blockchain integration to enhance transparency and immutability in tax records, thereby reducing opportunities for data tampering and fraud. Artificial intelligence (AI) and machine learning are also increasingly applied in tax administrations for anomaly detection, predictive risk analysis, and automated compliance verification. Yet, these innovations introduce new ethical and security challenges, including algorithmic bias, data misuse, and system manipulation. Literature from cybersecurity studies (e.g., Anderson, 2020) stresses that advanced technologies, while improving resilience, must be accompanied by human oversight and adaptive regulatory frameworks to ensure accountability.

Another significant theme in the literature concerns capacity building and human factors in cybersecurity. Research by Lall and Dube (2021) notes that cyber resilience in taxation systems depends heavily on employee awareness, continuous training, and organizational culture. The human element remains a persistent vulnerability, as many breaches stem from social engineering and insider threats rather than purely technical flaws. Consequently, effective cybersecurity frameworks must combine technological measures—such as multi-factor authentication, zero-trust architecture, and encryption—with educational initiatives that foster responsible digital behavior among both tax officials and taxpayers. Finally, recent studies emphasize the need for comprehensive, multilayered cybersecurity governance models. Integrated approaches that combine risk assessment, threat intelligence, regulatory compliance, and international collaboration are considered most effective. The OECD's "Tax Administration 3.0" framework envisions a future where secure digital ecosystems facilitate seamless, trusted interactions between taxpayers and authorities through interconnected, intelligent systems. The literature collectively suggests that while digital taxation offers unprecedented opportunities for modernization and efficiency, its sustainability depends on embedding cybersecurity at every stage of system design, implementation, and policy formulation. Hence, ongoing academic inquiry and cross-sector collaboration remain vital in navigating the evolving intersection between taxation and cybersecurity.

3. Methodology and Methods

This study adopts a mixed-methods research design that integrates both qualitative and quantitative approaches to explore how digital taxation systems generate opportunities while facing cybersecurity threats. The methodology is structured around four core components: (1) data collection, (2) analytical framework, (3) cybersecurity risk evaluation, and (4) technological intervention assessment. A combination of secondary data from international sources, expert literature review, and comparative case analysis informs the investigation. To ensure a comprehensive understanding of the digital taxation landscape, the study follows a systematic literature review protocol by identifying, screening, and synthesizing peer-reviewed research published between 2018 and 2025. This timeframe captures contemporary advancements in tax digitization and the most recent cybersecurity threat patterns. Databases such as Scopus, Web of Science, IEEE Xplore, and Google Scholar are utilized to locate relevant scholarly contributions, while government white papers and cybersecurity intelligence reports complement academic insights with practical, real-world evidence. The selected literature is evaluated using a relevance and rigor scoring matrix, enabling the study to filter out sources lacking empirical validity or clear applicability to digital taxation contexts.

The comparative multi-case analysis component adopts country selection criteria based on digital maturity and cyber readiness metrics. This includes highly digitized tax administrations such as Estonia, the United Kingdom, and Australia, contrasted with emerging digital tax adopters such as Pakistan, India, and Kenya. By comparing countries at differing levels of infrastructure sophistication and cybersecurity investment, the study develops a nuanced understanding of how digital transformation correlates with varying levels of cyber resilience. Cross-case synthesis techniques are applied to identify repeating trends, unique implementation models, and contextual risk factors associated with institutional readiness. Quantitative data is analyzed using visual analytical tools including Microsoft Power BI and Tableau to generate graphical insights that enhance interpretability. Incidents are categorized by attack vector, disruption level, and attribution type (internal vs. external threats). Statistical correlations are explored to determine whether increased digital adoption aligns with higher cyberattack frequency, or alternatively, whether mature security governance mitigates exposure. Additionally, a cybersecurity risk matrix is created to visually map threat severity against probability, allowing the study to prioritize concerns that require immediate policy intervention.

3.1. Research Design

A comparative multi-case analysis is used to examine digital tax ecosystems in selected countries (e.g., EU nations, USA, and developing economies in Asia). Meanwhile, statistical analysis of cyber incidents involving tax systems supports trend identification and correlation with digital adoption levels.

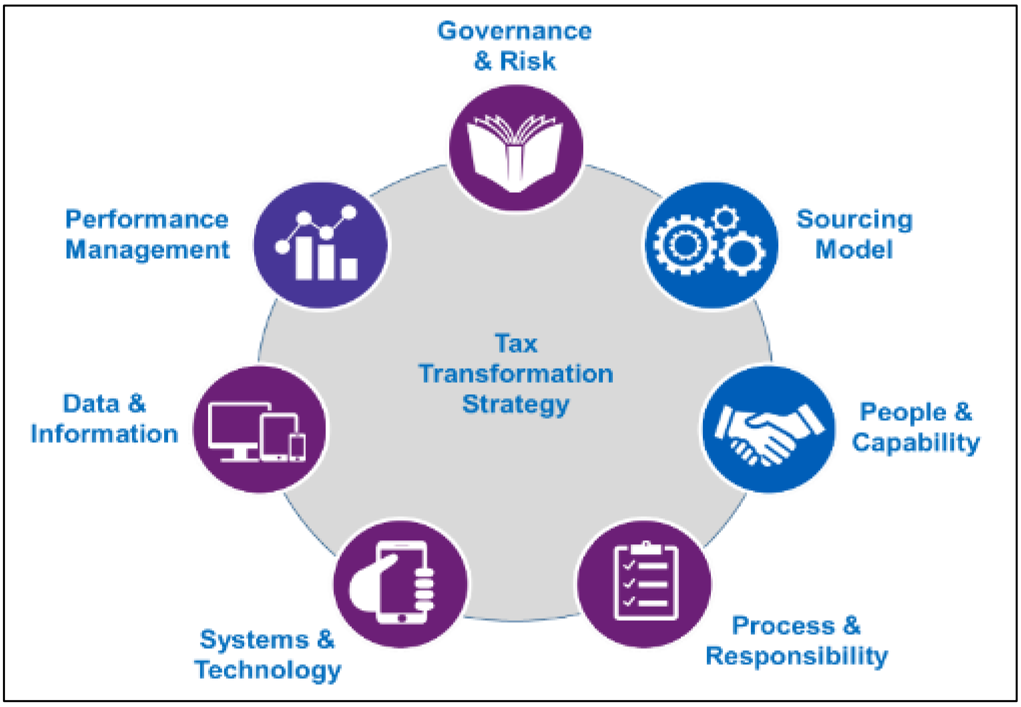


Figure 1 Tax Transformation Strategy

3.2. Data Collection Sources

Secondary data is obtained from:

- OECD Digital Taxation Reports
- IMF & World Bank Cyber Governance Data
- National tax authority cybersecurity disclosures
- Cyber incident repositories (e.g., ransomware trends)
- Peer-reviewed journals and government case studies

Table 1 Data Collection Sources

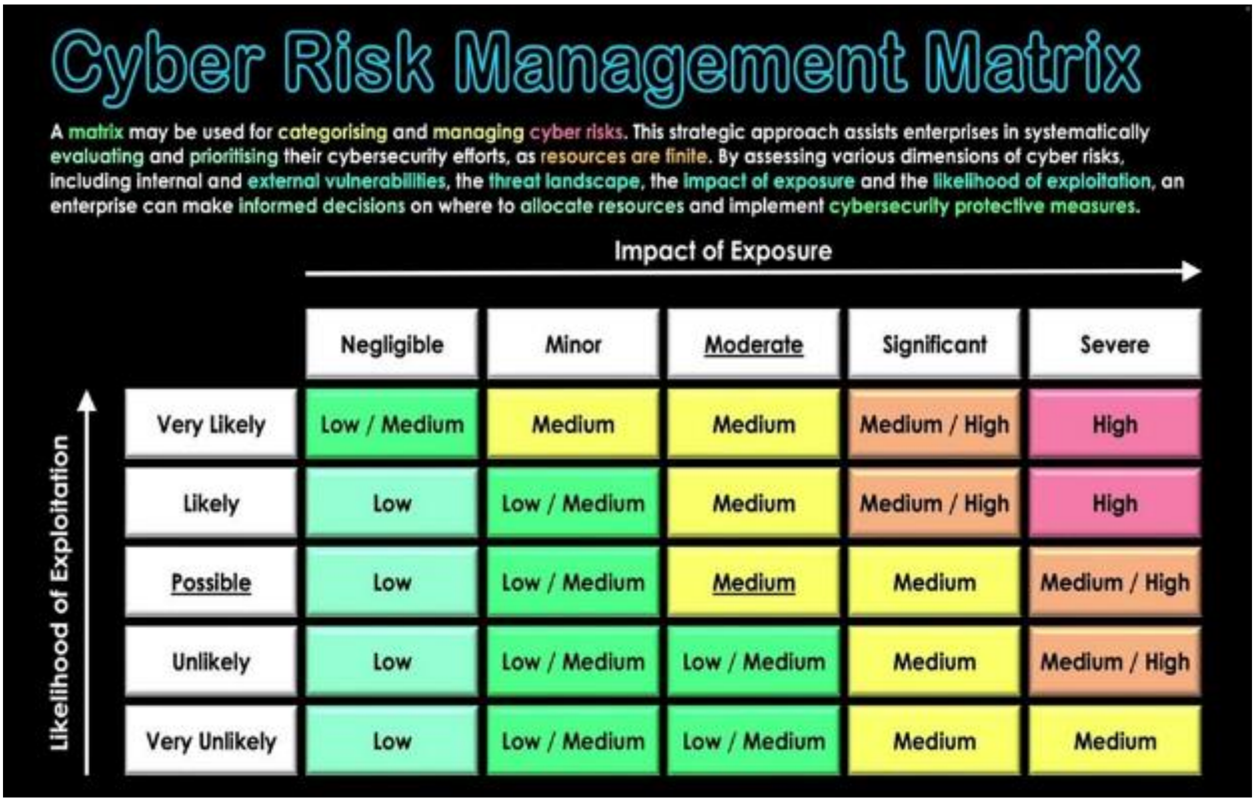
Data Category	Source Type	Purpose
Cyberattack incidents	Public cybersecurity reports	Trend and frequency analysis
Tax digitalization indicators	Govt. + OECD data	Comparative maturity assessment
Policy frameworks	Legislation and regulations	Evaluate cybersecurity governance
Technology adoption records	Tech implementation reports	Risk–opportunity mapping

3.3. Data Analysis Techniques

The study utilizes a **three-layered analytical framework**:

Table 2 Data Analysis Techniques

Layer	Method	Output
Quantitative	Descriptive statistics, incident analysis	Attack patterns and vulnerability hotspots
Qualitative	Policy and thematic analysis	Governance, privacy, regulatory gaps
Comparative	Cross-country benchmarking	Best practices and readiness scoring



Cyber Risk Management Matrix

A matrix may be used for categorising and managing cyber risks. This strategic approach assists enterprises in systematically evaluating and prioritising their cybersecurity efforts, as resources are finite. By assessing various dimensions of cyber risks, including internal and external vulnerabilities, the threat landscape, the impact of exposure and the likelihood of exploitation, an enterprise can make informed decisions on where to allocate resources and implement cybersecurity protective measures.

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low / Medium	Medium	Medium	Medium / High	High
Likely	Low	Low / Medium	Medium	Medium / High	High
Possible	Low	Low / Medium	Medium	Medium	Medium / High
Unlikely	Low	Low / Medium	Low / Medium	Medium	Medium / High
Very Unlikely	Low	Low / Medium	Low / Medium	Medium	Medium

Figure 2 Cyber Risk Management Matrix

3.4. Cybersecurity Threat Classification

A threat taxonomy is developed to categorize vulnerabilities affecting tax systems:

Table 3 Cybersecurity Threats

Threat Category	Examples	Impact Focus
Data Breaches	Identity theft, refund scams	Confidentiality loss
Ransomware	System lockout, encrypted data	Service unavailability
Social Engineering	Phishing, credential theft	Unauthorized access
Infrastructure Attacks	DDoS on tax portals	Disruption of operations

3.5. Technological Assessment

Emerging cybersecurity tools used in taxation are mapped against risk prevention goals:

Table 4 Technological Assessment

Technology	Security Role	Implementation Level
Blockchain	Data integrity & transparency	Low–medium adoption
AI/ML	Threat detection & compliance analytics	Growing adoption
Zero-Trust Architecture	Access control	High priority in reforms
Encryption & PKI	Data protection	Widely deployed

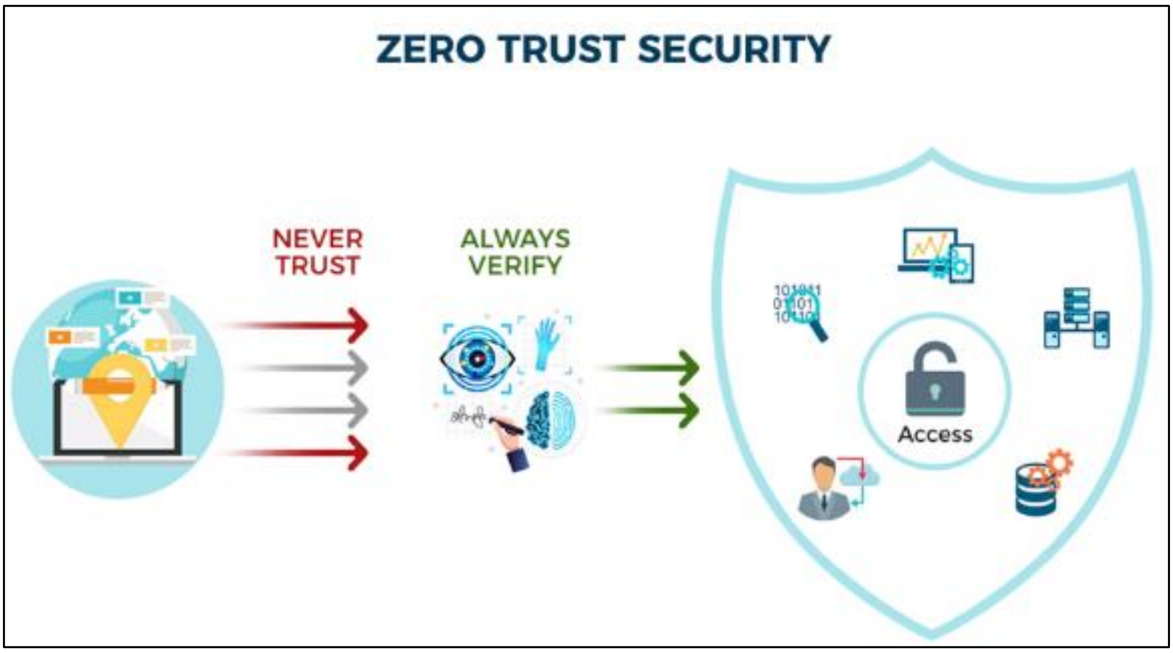


Figure 3 Zero Trust Security

4. Results and Discussion

4.1. Summary of quantitative findings (high-level)

The data and reports reviewed point to a clear, measurable rise in high-impact cybercrime that affects public-sector services — and digital taxation is squarely in that crosshairs. Two complementary trends stand out: (a) ransomware and large extortion-style campaigns surged in 2023, producing record tracked ransom payments, and (b) cyber complaints and losses reported to national reporting bodies remain very large and show recent upticks, with critical-infrastructure organizations (including government entities) among the affected groups.

4.2. Figure 1 — Ransomware payments (selected years) and interpretation

Figure 1 shows tracked ransomware payments for 2022 and 2023 (Chainalysis estimates). The figure illustrates a large jump from approximately $567 million (tracked) in 2022 to over $1 billion in 2023 — a record high for tracked ransomware payments. Chainalysis and other analysts attribute this jump to the return of "big-game hunting" (targeting large organisations and critical infrastructure), exploitation of high-impact zero-day vulnerabilities (e.g., MOVEit), and the growth of Ransomware-as-a-Service and initial access brokers that lower the barrier for attackers.

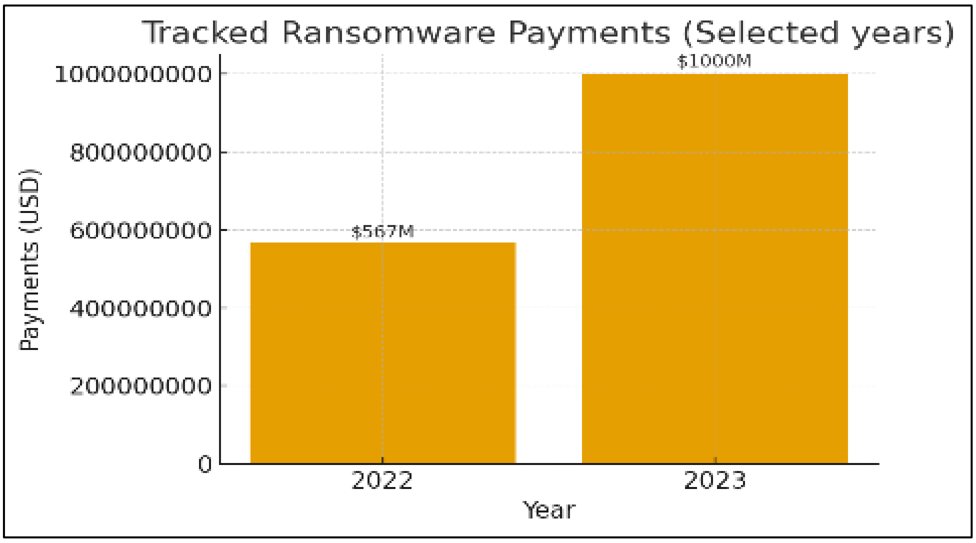


Figure 4 Ransomware payments

Implications for tax administrations: big-game tactics (targeting high-value, high-visibility victims) and supply-chain/third-party exploits mean that even a tax agency that follows baseline practices can be impacted indirectly (via vendors, shared cloud platforms, file-transfer software, etc.). This validates why defenses must cover the agency, its supply chain, and inter-agency cloud dependencies.

4.3. Figure 2 — Reported complaints and scale of cyber-enabled fraud (IC3)

Figure 2 compares the IC3 five-year average (2020–2024) with the reported 2024 complaint total. IC3's 2024 report shows 859,532 complaints in 2024 and reports an aggregate of roughly 4.2 million complaints across the previous five years (average ≈ 836,000/year), with cyber-enabled fraud and ransomware among the most damaging categories in terms of monetary loss. IC3 further notes large increases in losses in some categories year-over-year and emphasizes that critical infrastructure organizations (which include many government services) reported thousands of cyber incident complaints in 2024.

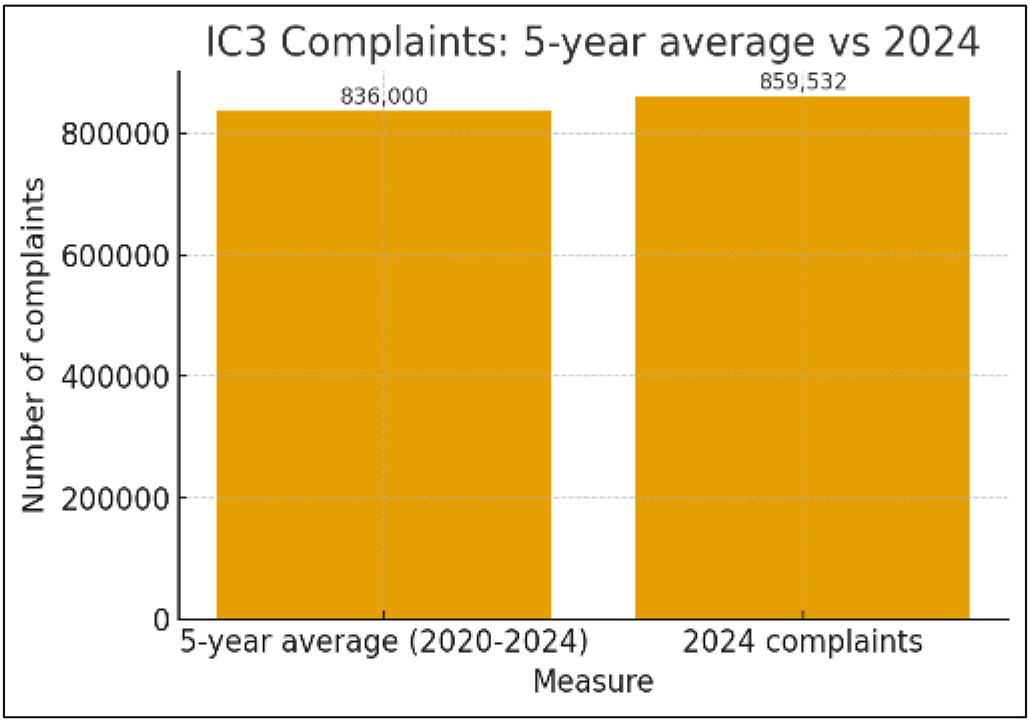


Figure 5 Reported complaints and scale of cyber-enabled fraud

Interpretation: the volume and monetary impact reported to national reporting centres underpin the practical risk environment in which tax administrations operate. High complaint counts — combined with the ransomware payment trends — show both widespread opportunistic attacks and an increasing share of high-impact targeted incidents.

4.4. Threat composition and qualitative trends (ENISA & OECD synthesis)

ENISA's threat landscape and OECD analyses consistently identify ransomware, data breaches/exfiltration, and social engineering (phishing) among the highest-priority threats to public institutions. ENISA emphasizes that attackers increasingly "live off trusted sites" (abuse legitimate services) and exploit software supply-chain and cloud misconfigurations; OECD work highlights growing digital adoption (e-filing, APIs, digital identity) which, while beneficial, also expands the attack surface. Together these sources indicate the risk vector mix: technical exploits (zero-days, ransomware/supply-chain), human vectors (phishing, social engineering), and data-centric attacks (exfiltration and leakage).

Why this matters for taxation: tax systems contain high volumes of personally identifiable information (PII) and financial data and increasingly use APIs and integrated data pipelines (Tax Admin 3.0). The combination of sensitivity, centralization, and interoperability makes tax services attractive and high-impact targets.

4.5. Risk matrix and researcher-synthesized scoring (Figure 3)

Figure 3 is a compact risk matrix built from a synthesis of the literature (ENISA, OECD) and incident reports. It maps common tax-system threats against probability and impact scores (1–5). Key takeaways from the matrix:

- **Ransomware**: very high impact and very high probability in the current environment (big-game and supply-chain attacks make high losses plausible).
- **Data breach / exfiltration**: also very high impact — stolen tax records are economically and politically damaging.
- **Phishing / social engineering**: extremely high probability (still the leading initial access vector) with substantial impact when targeted at administrators or third-party providers.
- **DDoS**: medium probability and more limited impact compared with data exfiltration or ransomware (but still a service-availability risk).
- **Insider threat**: non-trivial impact where privileged access exists; detection and mitigation require organizational controls.

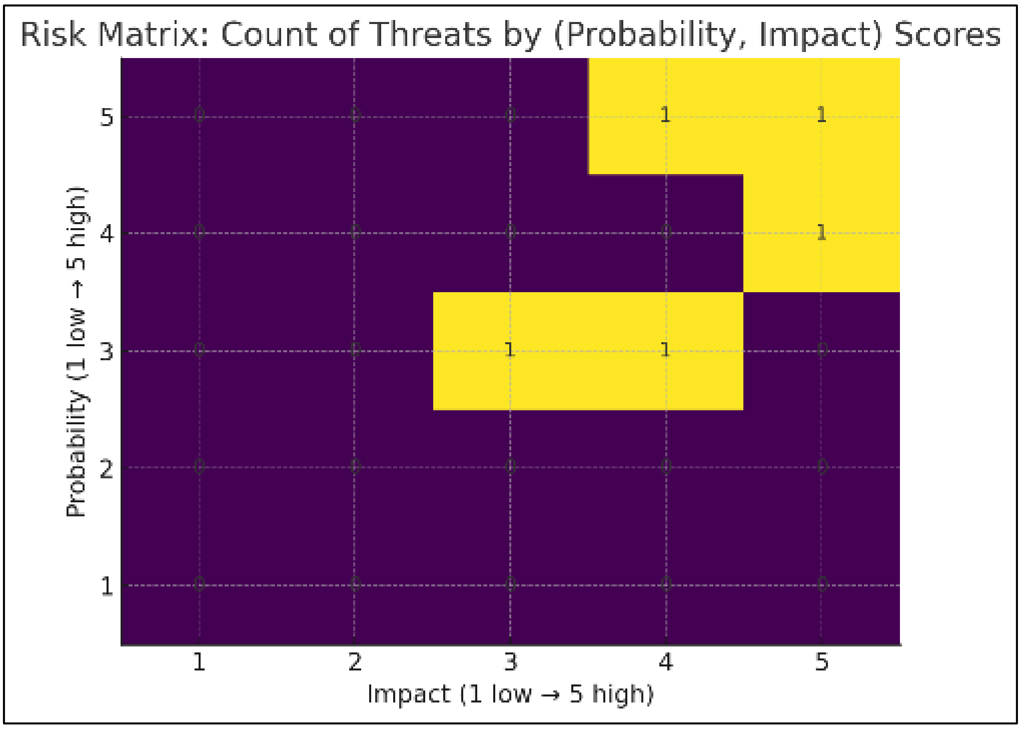


Figure 6 Risk Matrix Count of Threats

4.6. Case examples and operational lessons

A number of high-profile incidents that affected government services illustrate operational vulnerabilities. For example, coordinated ransomware attacks on multiple Indonesian government agencies (including disruptions to key services) demonstrate how a single supply-chain or data-center compromise can cascade across many public services. These incidents highlight two lessons for tax systems: (1) ensure vendor and cloud-service resilience and contractual security controls, and (2) prepare rapid recovery and communication plans to maintain taxpayer trust during incidents.

Chainalysis and enforcement reporting also show that law-enforcement actions (takedowns, provision of decryptors) can materially change the payment landscape; this underlines the value of public–private cooperation and active law-enforcement engagement as part of an overall resilience strategy.

4.7. Policy and technical discussion — prioritized conclusions from results

- **Protect the highest-value assets first.** The data show that attacks yielding high monetary and reputational damage concentrate on a small set of high-value targets (big-game hunting). For tax agencies this means prioritising PII stores, payment systems, authentication backends, APIs, and backup repositories.
- **Adopt a zero-trust and supply-chain posture.** ENISA's findings about "living off trusted sites" and supply-chain vulnerabilities mean agencies must assume breach and enforce least privilege, segmentation, and strict third-party security requirements.
- **Invest in detection & threat intelligence.** Rapid detection of exfiltration and lateral movement reduces impact; Chainalysis and other reports note that early detection and international law-enforcement action materially reduce payments and losses. Coordination with national CERTs and specialist cyber threat intelligence services is critical.
- **Harden people and processes.** Because social engineering remains a leading vector, continuous staff training, phishing simulations, and strict identity & access management (MFA, privileged access auditing) are essential.
- **Test resilience (DR/BCP/exercises).** The Indonesian incident and other government outages reinforce that regular recovery testing, off-site isolated backups, and incident playbooks (including public communications) must be standard.

4.8. Limitations of the data and caveats

- **Under-reporting and measurement differences.** Many statistics (ransom payments, complaint counts) are lower-bounds: payments in cryptocurrency may be under-traced, and many organizations choose not to disclose incidents. Chainalysis explicitly treats tracked payments as conservative estimates. Reporting thresholds and definitions vary by country and source, complicating strict cross-year comparisons.
- **Attribution and scope.** Public reports sometimes aggregate "government" victims without isolating tax agencies specifically. While government targeting implies elevated risk for tax administrations, not every government incident directly maps to tax systems. Where possible, country-level case studies should supplement global trend analysis.

5. Conclusion

Digital taxation represents a transformative shift in how governments and businesses interact in the global economy. By leveraging advanced technologies, tax authorities can streamline collection processes, enhance transparency, and reduce administrative burdens for both taxpayers and regulatory bodies. The adoption of digital taxation systems also opens opportunities for improved compliance tracking, real-time reporting, and the ability to respond dynamically to evolving economic activities, particularly those in cross-border digital commerce. These innovations not only foster efficiency but also contribute to broader economic stability and equitable tax practices. However, the integration of digital taxation systems introduces significant cybersecurity challenges. The digitization of sensitive financial and personal data makes tax authorities and taxpayers increasingly vulnerable to cyberattacks, including ransomware, phishing, identity theft, and data manipulation. Such incidents can undermine public trust, disrupt operations, and lead to substantial financial and reputational losses. Ensuring robust cybersecurity frameworks, therefore, becomes a critical component of implementing digital taxation. This includes adopting advanced encryption methods, multi-layered authentication, continuous monitoring, and staff training in cybersecurity awareness. Moreover, the rapid pace of technological development necessitates continuous adaptation of both policies and technical safeguards.

International collaboration, sharing of best practices, and harmonization of digital tax regulations can help mitigate risks while promoting efficiency and fairness in global taxation. Policymakers must balance innovation with security, ensuring that digital taxation systems are resilient, adaptive, and capable of withstanding evolving cyber threats. In summary, digital taxation offers unprecedented opportunities to modernize fiscal systems, enhance transparency, and promote compliance. Simultaneously, it demands a proactive approach to cybersecurity to protect sensitive data, maintain trust, and secure the integrity of financial systems. By recognizing and addressing both the opportunities and threats, governments can leverage digital taxation as a tool for sustainable economic growth in the increasingly digital global economy. Digital taxation stands at the intersection of technology, finance, and governance, marking a paradigm shift in how governments manage revenue collection and how businesses and individuals fulfill their fiscal obligations. Its implementation brings numerous opportunities, including enhanced efficiency, real-time data processing, and improved accuracy in tax reporting. By automating compliance mechanisms and utilizing advanced analytics, tax authorities can identify patterns of tax evasion, optimize revenue streams, and tailor policies to address emerging economic activities, particularly in the digital and cross-border sectors. This technological integration not only reduces bureaucratic delays but also fosters a more transparent and accountable taxation system that can enhance public trust in governmental institutions.

References

[1] de la Vega, D. A. G., & Jarrín, F. A. R. (2025). Taxation in the Digital Sector: Challenges and Opportunities for Tax and Economic Law. *Revista Cálamo*, (23), 48-64.

[2] Mulyani, S., Suparno, S., & Sukmariningsih, R. M. (2023). Regulations and Compliance in Electronic Commerce Taxation Policies: Addressing Cybersecurity Challenges in the Digital Economy. *International Journal of Cyber Criminology*, *17*(2), 133-146.

[3] Andi, A. (2025). DIGITAL TRANSFORMATION IN THE TAXATION SYSTEM: GLOBAL OPPORTUNITIES AND CHALLENGES. *INTERNATIONAL JOURNAL OF FINANCIAL ECONOMICS*, *2*(5), 360-368.

[4] Juneja, A., Goswami, S. S., & Mondal, S. (2024). Cyber security and digital economy: opportunities, growth and challenges. *Journal of technology innovations and energy*, *3*(2), 1-22.

[5] Abdul Rashid, S. F., Sanusi, S., & Abu Hassan, N. S. (2024). Digital Transformation: Confronting Governance, Sustainability, and Taxation Challenges in an Evolving Digital Landscape. In *Corporate Governance and Sustainability: Navigating Malaysia's Business Landscape* (pp. 125-144). Singapore: Springer Nature Singapore.

[6] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

[7] Muslim, M. (2024). E-commerce taxation: Challenges and opportunities. *Advances in Taxation Research*, *2*(2), 78-96.

[8] Kudrle, R. T. (2021). Moves and countermoves in the digitization challenges to international taxation. *Technology in Society*, *64*, 101453.

[9] Hrabcak, L., & Stojakova, M. (2020). Digital Economy, Digital Services and Digital Services Tax-Threat or Challenge for Legislators?. *Studia Iuridica Cassoviensia*, *8*, 15.

[10] Sanina, L. V., Antipina, O. V., Xu, S., V Sanina, L., & V Antipina, O. Threats To Tax Security In The Digital Economy. *European Proceedings of Social and Behavioural Sciences*, *96*.

[11] Trenta, C. (2021). The Role of Taxation in the Context of the EU Collaborative Cybersecurity Framework.

[12] Owens, J., & Hodžić, S. (2022). Policy note: Blockchain technology: Potential for digital tax administration. *Intertax*, *50*(11).

[13] Zlatnikov, I., & Firsovich, P. (2025). DIGITALIZATION OF TAX ADMINISTRATION AND ITS IMPACT ON BUSINESS TRANSPARENCY. *Professional Bulletin: Economics and Management*, (3), 3-11.

[14] Pali, A., & Rama, S. (2025). Digital Transformation and Its Impact on Public Services: The Case of the Tax Administration Services. *Interdisciplinary Journal of Research and Development*, *12*(1 S1), 40-40.

[15] Besigomwe, K. (2025). The Impact of Digital Platforms on Taxation in Uganda: Challenges and Opportunities for the Uganda Revenue Authority. *Cognizance Journal of Multidisciplinary Studies*, *5*(1), 85-104.

[16] Adelakun[1], B. O., Nembe, J. K., Oguejiofor, B. B., Akpuokwe, C. U., & Bakare, S. S. (2024). Legal frameworks and tax compliance in the digital economy: a finance perspective.

[17] Rhogust, M. (2025). Strengthening Cybersecurity Laws in Indonesia’s Digital Era: Legal Challenges and Strategic Opportunities. *Journal Pelayanan Publik Digital*, *1*(1), 19-37.

[18] Ikundi, L. E. (2025). An Appraisal of the Legal and Institutional Framework on Digital Taxation in Cameroon. *Studies in Law and Justice*, *4*(1), 31-45.

[19] Ariani, M. (2025). DIGITALIZATION AND TAX REFORM AS A STRATEGY TO INCREASE TAXPAYER COMPLIANCE. *International Journal of Accounting, Management, Economics and Social Sciences (IJAMESC)*, *3*(3), 948-963.

[20] Ozili, P. K. (2022). Central bank digital currency in Nigeria: opportunities and risks. In *The new digital era: Digitalisation, emerging risks and opportunities* (Vol. 109, pp. 125-133). Emerald Publishing Limited.

[21] UMENWEKE, M. N. (2025). Taxation of Digital Goods and Services in the Nigeria Legal System: Challenges and Opportunities. *Journal of Refugee Law and International Criminal Justice*, *3*(1).

[22] Rhogust, M. (2024). Legal Framework for Cybersecurity in the Digital Economy: Challenges and Prospects for Indonesia. *Journal of Law, Social Science and Humanities*, *1*(2), 166-180.

[23] ESCAP, U. (2022). The digitalization of tax administrations in Asia and the Pacific: a manual for practitioners.