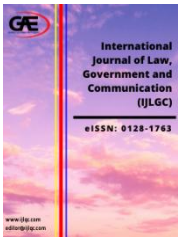
International Journal of Law, Government and Communication
IJLGC
EISSN : 0128-1763
Volume: 11 Issue: 46 (December 2026) PP. 17-32



INTERNATIONAL JOURNAL OF LAW, GOVERNMENT AND COMMUNICATION (IJLGC)
www.gaexcellence.com/ijlgc

CYBERSECURITY RISK, CONTROL AND GOVERNANCE IN DIGITAL DATA: A CHRONOLOGICAL REVIEW

Nur Syuhada Mohamad Rodzi[1]*, Ganthan Narayana Samy[2], Noor Hafizah Hassan[3], Mohamad Fadli Zolkipli[4], Siti Nur Aqilah Ab-Wahab[5]

[1]Faculty of Artificial Intelligence, Universi Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia
Department of Information Technology and Communication, Politeknik Balik Pulau (PBU), Penang, Malaysia
syuhada.rodzi@gmail.com https://orcid.org/0000-0003-4409-841X
syuhadarodzi@pbu.edu.my

[2]Faculty of Artificial Intelligence, Universi Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia
ganthan.kl@utm.my https://orcid.org/0000-0001-6169-3400

[3]Faculty of Artificial Intelligence, Universi Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia
noorhafizah.kl@utm.my https://orcid.org/0000-0002-6348-9136

[4]School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, (UUM), Kedah, Malaysia
m.fadli.zolkipli@uum.edu.my https://orcid.org/0000-0002-6780-8480

[5]Labuan Faculty of International Finance, Universiti Malaysia Sabah (UMS), Sabah, Malaysia
nuraqilah@ums.edu.my https://orcid.org/0000-0001-8551-7604

*Corresponding Author

Article Info:

Article history:
Received date: 28.09.2026
Revised date: 13.10.2026
Accepted date: 02.11.2026
Published date: 01.12.2026

To cite this document:

Rodzi, N. S. M., Samy, G. N., Hassan, N. H., Zolkipli, M. F., & Ab-Wahab, S. N. A. (2026). Cybersecurity Risk, Control and Governance in Digital Data: A Chronological Review. *International Journal of Law,*

Abstract:

The rapid expansion of digital technologies and data dependent operations has increased organizational exposure to cyber threats, privacy breaches, operational disruption, and regulatory noncompliance, strengthening the need for effective cybersecurity risk management, control, and governance. However, existing knowledge remains dispersed across technical, behavioural, organizational, and regulatory perspectives, making the historical development and changing priorities of this research domain difficult to understand. This study presents a chronological literature review of cybersecurity risk, control, and governance in digital data. A systematic advanced search was conducted in the Scopus database using keyword combinations related to "cybersecurity," "risk management," "risk governance," and "risk assessment," supported by predefined screening and eligibility criteria. The process produced a final dataset of 302 publications covering the period from 2017 to August 2026. Based on publication patterns and changes in research focus, methodological application, and conceptual development, the literature was classified into three chronological phases. The first phase, Emergence and Conceptual

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 46 (December 2026) PP. 17-32

Government and Communication, 11(46), 17-32.

Foundation (2017–2019), primarily addressed risk perception, human behaviour, organizational culture, and socio technical security principles. The second phase, Development and Sustained Growth (2020–2023), extended towards organizational resilience, integrated governance, regulatory compliance, risk quantification, adaptive controls, and digital asset protection. The third phase, Accelerated Expansion and Research Maturation (2024–2026), demonstrated increasing attention to standards-based governance, sector specific frameworks, artificial intelligence, explainable automation, dynamic risk assessment, legal accountability, and human AI collaboration. Overall, the findings reveal a progressive transition from fragmented technical and behavioural approaches towards integrated cybersecurity governance that connects people, processes, technology, regulation, and organizational accountability. This review provides a structured understanding of the field's evolution and supports future development of adaptive, measurable, and context sensitive approaches for managing cybersecurity risks and protecting digital data.

DOI: 10.35631/IJLGC.1146002

Keywords:

Cybersecurity, Digital Data, Risk Control, Risk Governance, Risk Management

© The authors (2026). This is an Open Access article distributed under the terms of the Creative Commons Attribution (CC BY NC) (http://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact ijlgc@gaexcllence.com.

Introduction

Cybersecurity risk, control, and governance in digital data have become defining concerns of the digital economy because organizations now rely on data intensive infrastructures for operations, decision making, service delivery, and innovation, while the same infrastructures expose them to rapidly expanding cyber threats and regulatory demands (Islam et al. 2025; Lee 2021; Reddy, KiranmayeeSattiraju, and Julakanti 2025; Thallada and Alapati 2026; Toussaint, Krima, and Panetto 2024). Digital transformation has widened the attack surface through cloud platforms, mobile systems, IoT, AI enabled services, remote work, and highly interconnected enterprise environments, making cyber risk less a bounded IT problem than a condition of everyday organizational life (Haque et al. 2025; Obiokafor and Iduh 2026; Saeed et al. 2023; Salsabilla 2026). This expansion matters because digital data now represents not only economic value but also legal liability, reputational exposure, and operational dependency, so breaches, unauthorized access, manipulation, and service disruption can directly damage trust, continuity, and financial performance (Melaku 2023; Reddy et al. 2025; Salsabilla 2026). The literature consistently frames protection goals around confidentiality, integrity, and availability, but also shows that data integrity and lawful use have become especially important as organizations move sensitive data across distributed systems and digital workflows (Kumar, Anil, and Babatope 2024; Toussaint et al. 2024). Threats have also become more sophisticated and diverse, spanning ransomware, phishing, malware, data breaches, nation state intrusion, and exploitation of system weaknesses, with attacks often propagating across dependencies inside

interconnected infrastructures (Islam et al. 2025; Qudus 2025; Salsabilla 2026; Tang, Alazab, and Luo 2019). Several studies therefore argue that organizations can no longer protect only a narrow set of critical assets while leaving adjacent systems exposed, because attackers routinely exploit weakly defended components to gain broader access (Tang et al. 2019; Toussaint et al. 2024). In this setting, cybersecurity risk is increasingly understood as systemic and context specific, shaped by infrastructure complexity, human behavior, third party dependencies, compliance pressures, and the speed with which vulnerabilities and attacker methods evolve (Haque et al. 2025; Islam et al. 2025; Salutina, Platunina, and Frank 2024). Control is the operational response to this environment, and the research shows that effective control is not a single technology, but a coordinated set of technical, administrative, and procedural safeguards embedded across the data lifecycle (Kumar et al. 2024; Nayeem 2025). Across the evidence base, stronger security outcomes are associated with integrated approaches that combine encryption, identity and access management, multi factor authentication, information classification, data stewardship, monitoring, incident management, and staff training rather than fragmented, tool by tool deployment (Aliliele et al. 2026; Kumar et al. 2024; Nayeem 2025; Obiokafor and Iduh 2026; Salutina et al. 2024). This integrated view is important because many organizations still show a gap between implementing individual tools and building an overarching cybersecurity framework, which leads to duplicated controls, inconsistent policies, weaker visibility, and slower response to emerging threats (Aliliele et al. 2026; Obiokafor and Iduh 2026; Thallada and Alapati 2026). The literature therefore favors proactive and adaptive risk management, emphasizing regular policy updates, vulnerability assessment, threat monitoring, penetration testing, awareness programs, and continuous improvement rather than static compliance exercises (Melaku 2023; Qudus 2025; Toussaint et al. 2024). This shift is reinforced by evidence that vulnerability management remains overly reactive in practice, even though organizations face a large and growing volume of disclosed vulnerabilities and only a small fraction are actually exploited, which means prioritization must reflect exploit likelihood, temporal context, and asset dependencies (Islam et al. 2025; Tang et al. 2019).

More recent work accordingly incorporates AI enabled analytics, explainability, and cyber threat intelligence to support strategic, operational, and tactical decisions about which risks require urgent control action (Ampel et al. 2024; Islam et al. 2025). Human factors remain central within this control environment, because employee awareness directly influences the effectiveness of controls and several governance models treat security education and awareness as foundational rather than supplementary measures (Melaku 2023; Obiokafor and Iduh 2026; Salsabilla 2026). Governance gives cybersecurity control its strategic direction, accountability, and institutional coherence by aligning security decisions with organizational leadership, legal obligations, business continuity, and long-term resilience (Melaku 2023; Nayeem 2025). A strong theme across the literature is that cybersecurity, privacy, data governance, and compliance should not be managed as isolated domains, because integrated governance improves policy consistency, audit readiness, transparency, accountability, incident response, and trust across distributed digital operations (Aliliele et al. 2026; Thallada and Alapati 2026). Governance frameworks are also expected to define roles, ownership, cross functional councils, and stewardship responsibilities so that security, legal, risk, engineering, and management functions operate through shared controls and common risk language (Aliliele et al. 2026; Kumar et al. 2024; Ogbodo et al. 2025; Reddy et al. 2025). Regulation is a major driver of this convergence, with studies repeatedly pointing to GDPR, HIPAA, CCPA, PCI-DSS, ISO 27001, NIST oriented controls, and related legal frameworks as forces requiring not only technical safeguards but also demonstrable governance, evidence collection, and

continuous assurance (Majeed1, Majeed2, and Minhas 2026; Melaku 2023; Nayeem 2025; Ogbodo et al. 2025; Reddy et al. 2025). At the same time, the evidence identifies persistent obstacles, including complex frameworks, high implementation costs, skill shortages, fragmented international policy, weak awareness, and a recurring gap between regulatory expectations and operational reality (Majeed1 et al. 2026; Melaku 2023; Ogbodo et al. 2025; Qudus 2025). For that reason, current governance models increasingly emphasize simplicity, adaptability, public private collaboration, international cooperation, resilience-oriented planning, and the separation of governance from day-to-day management (Majeed1 et al. 2026; Melaku 2023). Taken together, the literature presents cybersecurity risk, control, and governance in digital data as a single strategic agenda in which risk identifies exposure, control reduces it through coordinated safeguards, and governance ensures that protection remains accountable, adaptive, compliant, and resilient in increasingly data dependent systems (Aliliele et al. 2026; Kumar et al. 2024; Ogbodo et al. 2025; Qudus 2025).

Materials and Methods

Data Collection

The rapid expansion of digital ecosystems has intensified organizational dependence on data while simultaneously increasing exposure to cybersecurity risks arising from cyberattacks, unauthorized access, data breaches, insider threats, technological vulnerabilities, and weak security practices. Consequently, effective cybersecurity requires more than technical protection; it demands an integrated approach that aligns risk assessment, security controls, accountability, policy, and governance. Although research on cybersecurity risk, control, and governance has grown considerably, the literature remains fragmented across technical, managerial, regulatory, and organizational domains, making it difficult to understand how scholarly priorities and knowledge structures have evolved over time. Therefore, this review systematically examines the development of the field by identifying major publication patterns, influential contributions, thematic transitions, and emerging research directions. Data were collected through a single step retrieval process using the Scopus database, selected for its broad coverage of peer reviewed, high-quality scholarly literature and comprehensive bibliographic metadata. A carefully constructed search strategy was applied to relevant publication fields using predefined keywords related to cybersecurity risk, security controls, governance, and digital data. The retrieved records were then assessed against established eligibility parameters, including topical relevance, publication type, language, document status, and study period, to ensure that only publications aligned with the review objectives were retained. Rigorous and systematic data collection is essential because the accuracy of a chronological review depends directly on the completeness, consistency, and relevance of its evidence base. Transparent search procedures reduce selection bias, improve reproducibility, and strengthen the reliability and validity of the findings. Moreover, consistent inclusion criteria enable publication growth, thematic shifts, and emerging research priorities to be interpreted meaningfully across different periods, thereby providing a credible foundation for evaluating the intellectual evolution of cybersecurity risk, control, and governance in digital data.

The data collection employed a structured, single step search in the Scopus database to identify primary studies concerning cybersecurity risk, control, and governance in relation to digital data and assets. The specification of primary data searching is summarized in Table 1. The search strategy integrated three conceptual domains: cybersecurity (“cybersecurity” or “cyber

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 46 (December 2026) PP. 17-32

security"), risk ("risk management," "risk control," "risk governance," or "risk"), and digital resources ("digital data," "digital asset," or "digital security").

Table 1: The Specification for Primary Data Searching

Keyword	Cybersecurity, Risk Management, Risk Control, Risk Governance, Risk, Digital Data, Digital Asset, Digital Security
Inclusion	Article, Journal, English and Computer Science
Exclusion	review article, article in press, other languages
Final Search String (Scopus)	(cybersecurity OR "cyber security") AND ("risk management" OR "risk control" OR "risk governance" OR risk) AND ("digital data" OR "digital asset" OR "digital security") AND PUBYEAR > 2013 AND PUBYEAR < 2027 AND (LIMIT-TO (SRCTYPE , "j")) AND (LIMIT-TO (OA , "all")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (SUBJAREA , "COMP")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (EXACTKEYWORD , "Cybersecurity") OR LIMIT-TO (EXACTKEYWORD , "Cyber Security") OR LIMIT-TO (EXACTKEYWORD , "Risk Assessment") OR LIMIT-TO (EXACTKEYWORD , "Data Privacy") OR LIMIT-TO (EXACTKEYWORD , "Risk Management") OR LIMIT-TO (EXACTKEYWORD , "Information Management") OR LIMIT-TO (EXACTKEYWORD , "Information Security") OR LIMIT-TO (EXACTKEYWORD , "Digital Assets") OR LIMIT-TO (EXACTKEYWORD , "Digital Security") OR LIMIT-TO (EXACTKEYWORD , "Cyber Threats") OR LIMIT-TO (EXACTKEYWORD , "Cyber Attacks") OR LIMIT-TO (EXACTKEYWORD , "Digital Transformation") OR LIMIT-TO (EXACTKEYWORD , "Security Of Data") OR LIMIT-TO (EXACTKEYWORD , "Digital Storage") OR LIMIT-TO (EXACTKEYWORD , "Computer Security") OR LIMIT-TO (EXACTKEYWORD , "Risks Management") OR LIMIT-TO (EXACTKEYWORD , "Risks Assessments") OR LIMIT-TO (EXACTKEYWORD , "Risk Analysis") OR LIMIT-TO (EXACTKEYWORD , "Digitalization") OR LIMIT-TO (EXACTKEYWORD , "Data Protection") OR LIMIT-TO (EXACTKEYWORD , "Sensitive Data") OR LIMIT-TO (EXACTKEYWORD , "Regulatory Compliance") OR LIMIT-TO (EXACTKEYWORD , "Governance") OR LIMIT-TO (EXACTKEYWORD , "Digital Technologies") OR LIMIT-TO (EXACTKEYWORD , "Risk Perception") OR LIMIT-TO (EXACTKEYWORD , "Risk") OR LIMIT-TO (EXACTKEYWORD , "Digitization") OR LIMIT-TO (EXACTKEYWORD , "Digital Devices") OR LIMIT-TO (EXACTKEYWORD , "Cyberattacks") OR LIMIT-TO (EXACTKEYWORD , "Data Security") OR LIMIT-TO (EXACTKEYWORD , "Cyberattack") OR LIMIT-TO (EXACTKEYWORD , "Digital Evidence") OR LIMIT-TO (EXACTKEYWORD , "Compliance") OR LIMIT-TO (EXACTKEYWORD , "Security And Privacy") OR LIMIT-TO (

	EXACTKEYWORD , "Cyber-attacks")) AND (LIMIT-TO (DOCTYPE , "ar")) AND PUBYEAR > 2015 AND PUBYEAR < 2027
Number of Primary Article	302

Boolean operators were used to capture terminological variations while maintaining conceptual alignment with the review scope. The search was further refined through relevant exact keywords, including risk assessment, data privacy, information security, digital assets, cyber threats, data protection, regulatory compliance, and governance. Eligibility was restricted to final stage, open access journal articles written in English and classified within Computer Science. Review articles, articles in press, non-English publications, and other document types were excluded. Although the search string contains two publication period conditions, their combined application establishes an effective coverage period of 2016–2026 because the more restrictive criterion, PUBYEAR > 2015, supersedes PUBYEAR > 2013.

The application of these criteria produced a final corpus of 302 primary articles. This result indicates a substantial and sufficiently focused body of evidence for examining the chronological development of cybersecurity risk, control, and governance in digital environments. Restricting the dataset to peer reviewed journal articles strengthens evidential consistency by excluding preliminary, non-final, and secondary research, while the Computer Science limitation ensures disciplinary relevance to cybersecurity mechanisms, risk analysis, data protection, and digital security. The English language restriction improves consistency in screening and interpretation, although it may underrepresent research published in other languages. Similarly, the open access criterion enhances transparency and reproducibility by ensuring that the selected evidence is accessible for verification, but it may exclude relevant subscription-based studies. The extensive exact keyword filtering increases topical precision and reduces irrelevant retrieval, nevertheless, it may exclude conceptually relevant articles indexed under alternative terminology. Overall, the 302 article shortlisted represents a defensible balance between breadth and specificity, providing a reliable foundation for interpreting publication growth, shifts in research emphasis, and the evolving integration of risk management, security controls, and governance across the 2016–2026 period.

Data Clustering

To facilitate a systematic interpretation of the chronological development of the research, the annual publication data were grouped into distinct temporal clusters based on observable variations in publication year, volume, and growth trajectory. The dataset was retrieved from Scopus, a reputable and comprehensive bibliographic database, using predefined keywords, Boolean operators, and advanced search criteria to ensure the relevance, consistency, and quality of the selected literature. Temporal clustering is particularly important in a chronological review because annual publication counts considered individually may not fully

International Journal of Law, Government and Communication
EISSN : 0128-1763
IJLGC
Volume: 11 Issue: 46 (December 2026) PP. 17-32

reveal broader patterns of scholarly development. By grouping years with comparable levels of research productivity and identifying significant changes in publication volume, the analysis can distinguish formative periods, phases of sustained growth, and stages of accelerated expansion or maturation. This approach reduces the complexity of year-by-year data while preserving meaningful changes in research momentum, thereby enhancing the clarity and interpretability of publication trends. Moreover, clustering enables the identification of transition points at which scholarly attention intensified, stabilized, or shifted in response to evolving cyber threats, digital transformation, regulatory requirements, and emerging governance concerns. Accordingly, the resulting temporal phases provide an analytically robust framework for examining how the literature has progressed over time and for interpreting changes in the prominence, scope, and maturity of cybersecurity risk management, security controls, data protection, and governance research.

The annual publication distribution reveals three clear temporal phases in the development of the research. The classification is based on observable changes in publication volume, growth rate, and research momentum as shows in Figure 1. Two major transition points are evident which is the sharp increase from four publications in 2019 to 16 in 2020 and follow by the subsequent rise from 32 publications in 2023 to 58 in 2024. These structural changes support dividing the 302 publications into three phases respectively which are Phase 1: Emergence and Conceptual Foundation (2017–2019), Phase 2: Development and Sustained Growth (2020–2023) and Phase 3: Accelerated Expansion and Research Maturation (2024–2026).

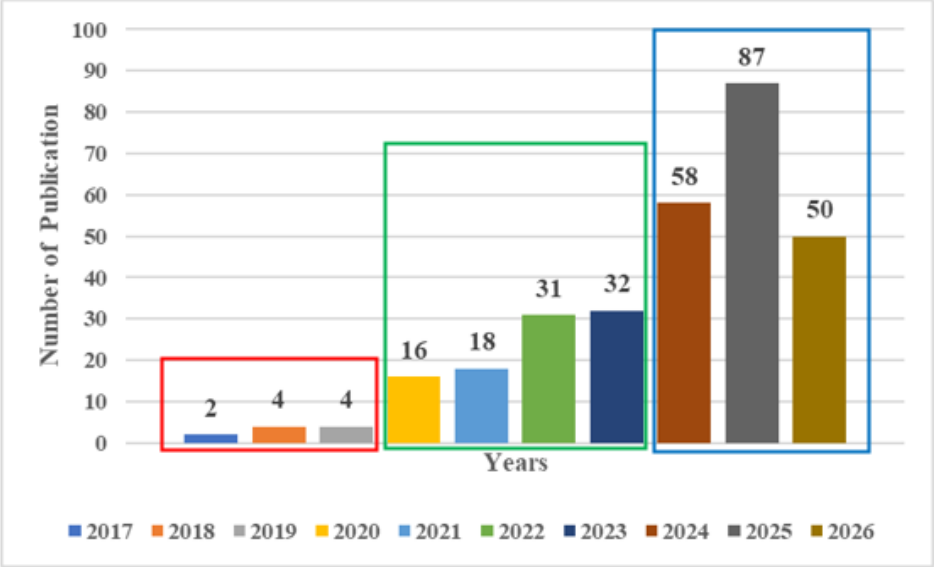


Figure 1: Number of Documents Per Year

Across the three phases, the publication trend shows a clear progression from establishing conceptual foundations in human risk perception, socio technical security, and organizational culture during 2017–2019 to sustained growth in integrated governance, resilience, risk quantification, and adaptive controls during 2020–2023. From 2024 to August 2026, the field reached greater maturity through sector specific frameworks, standards-based governance, explainable artificial intelligence, regulatory compliance, and dynamic risk assessment. Overall, cybersecurity research increasingly treats digital data protection as an integrated

human, technological, organizational, legal, and governance responsibility rather than solely a technical issue.

Phase 1: Emergence and Conceptual Foundation (2017–2019). The first phase represents the formative stage of research on cybersecurity risk, control, and governance in digital data. Publication output remained limited, increasing from two articles in 2017 to four articles in both 2018 and 2019. Only 10 articles, representing 3.3% of the total dataset, were published during this period. This relatively low and stable productivity indicates that the research domain was still emerging, with scholarly attention likely concentrated on establishing foundational concepts relating to cybersecurity risk, information security, digital asset protection, and organizational controls. The absence of substantial annual growth suggests that these topics had not yet developed into a consolidated research stream. Nevertheless, this phase established the intellectual foundation for subsequent studies by highlighting the growing importance of protecting digital data and incorporating risk considerations into organizational cybersecurity practices.

Phase 2: Development and Sustained Growth (2020–2023). The second phase marks the transition from an emerging field to a progressively established area of research. Publication output increased fourfold from four articles in 2019 to 16 in 2020, followed by 18 publications in 2021, 31 in 2022, and 32 in 2023. Collectively, this phase produced 97 articles, accounting for 32.1% of the dataset. The increase reflects heightened scholarly and organizational concern regarding cyberattacks, data breaches, accelerated digital transformation, cloud adoption, remote operations, and regulatory compliance. The near doubling of publications between 2021 and 2022 further indicates that cybersecurity risk was increasingly examined beyond technical protection to include risk assessment, organizational controls, data governance, accountability, and resilience. The comparable outputs recorded in 2022 and 2023 suggest a brief period of consolidation, during which the field developed greater conceptual and methodological stability before entering a more rapid expansion phase.

Phase 3: Accelerated Expansion and Research Maturation (2024–2026). The third phase demonstrates accelerated expansion and increasing maturity in the research domain. Publications rose sharply from 32 in 2023 to 58 in 2024 and reached a peak of 87 in 2025. Although 50 publications were recorded for 2026, this figure should not be interpreted as evidence of declining interest because the data cover only part of the year which is until August 2026 and may also be affected by Scopus indexing delays. This phase contains 195 articles, representing 64.6% of the entire corpus, meaning that almost two thirds of all publications appeared within the most recent three-year period. Such concentration indicates that cybersecurity risk, control, and governance have become central concerns in protecting digital data amid increasingly complex cyber threats, expanding regulatory obligations, artificial intelligence adoption, interconnected digital platforms, and third-party dependencies. The phase therefore reflects not only quantitative expansion but also the maturation of the field toward integrated governance models, adaptive controls, organizational resilience, privacy protection, and proactive management of emerging digital risks.

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 46 (December 2026) PP. 17-32

Result and Discussions

Phase 1: Emergence and Conceptual Foundation (2017–2019)

In year 2017, (van Schaik et al. 2017) found that identity theft, keylogging, cyberbullying, and social engineering generated the strongest perceived risks among students. Precautionary behaviour was particularly influenced by perceived control, while voluntariness, immediacy, dread, potential consequences, Internet experience, and usage frequency shaped risk judgements. These findings indicated that security responses depend on the characteristics of individual hazards and therefore should not be interpreted through aggregated risk measures. In an organizational context, (Damenu and Beaumont 2017) identified substantial internal risks associated with weak governance and security culture in banking. Soft systems methodology supported holistic analysis by producing stakeholder accessible models and facilitating validation. The results positioned cybersecurity as a socio technical concern involving technical safeguards, management, governance, employees, customers, and organizational culture. Collectively, the 2017 literature established that effective control requires both informed user behaviour and systemic organizational oversight.

Next, (Mundra 2018) argued that blockchain implementation requires asset suitability assessment, organizational readiness, change management, standard operating procedures, and training; poorly structured adoption may introduce financial and operational risk instead of reducing exposure. In addition, (Alohali et al. 2018) demonstrated that personality traits, especially conscientiousness, were associated with security risk behaviour, with stronger relationships when combined with age, gender, technological proficiency, and online activity. Eleven of 28 behaviours achieved predictive accuracy of at least 60%, while several reached 92%, supporting more individualized human risk management. Next, (van Schaik et al. 2018) similarly found that information sharing hazards generated the greatest concern and precaution on social networks, whereas less visible privacy and access threats received weaker responses. On the contrary, (Dennis and Minas 2018) challenged rational choice assumptions by explaining security conduct through automatic cognition, suggesting that compliance measures should reshape habitual cues and perceptions of normality. By 2019, emphasis shifted toward applied and adaptive solutions. On the other hand, (Wan et al. 2019) reported that trusted delegation improved older adults' mobile security decisions, with crowdsourced advice further strengthening decision quality. Then, (Addae et al. 2019) showed that behavioural analytics and Bayesian modelling could support personalized and partly automated cybersecurity assistance. Governance also became more prominent as (Arora 2019) proposed fiduciary obligations to balance health data sharing with contextual privacy protection, while (Goodell and Aste 2019) identified cryptocurrency arrangements capable of reconciling regulatory auditability with user anonymity. Overall, Phase 1 progressed from basic risk perception and organizational diagnosis toward personalized controls, technological implementation, privacy accountability, and regulatory accommodation.

Phase 2: Development and Sustained Growth (2020–2023)

Research during 2020 showed that cybersecurity risk had developed beyond isolated technical weaknesses into behavioural, organizational, and infrastructural concerns. (Thompson, Ahmad, and Maynard 2020) found that Internet addiction weakened the influence of privacy concerns on information disclosure decisions, indicating that awareness alone may not produce safer conduct. Then, (Nyblom, Wangen, and Gkioulos 2020) identified considerable differences in

social media risk perception across platforms and user characteristics, supporting targeted rather than uniform awareness measures. At the organizational level, (Ahmad et al. 2020) established that integrating incident response with security management supported organizational learning, while (da Veiga et al. 2020) demonstrated that information security culture requires alignment between academic concepts and industry practices. The 2021 literature extended this direction into ecosystem resilience, regulatory compliance, and collective protection. It begin with (Kropczynski et al. 2021) found value in community based support for older adults' privacy and security management. Then follow by (Khan, Ibrahim, and Hussain 2021) highlighted weaknesses affecting information security in university libraries, whereas (Rashid, Noor, and Altmann 2021) showed that information sharing could create economic value within cybersecurity ecosystems. This period therefore shifted from identifying individual and technical risks towards coordinated organizational learning, community support, and sector-specific governance.

Publication growth during 2022 reflected greater attention to measurable governance, regulatory alignment, and complex digital infrastructures. (Schinagl, Shahim, and Khapova 2022) identified tensions between security control and organizational flexibility, supporting an ambidextrous governance approach. (Bongiovanni et al. 2022) introduced a mechanism for quantifying adherence to information security governance guidelines, while (Zhang et al. 2022) demonstrated that structured threat and risk models could classify exposure within digital data marketplaces. Privacy governance also broadened through findings concerning deletion rights, cumulative personal information risks, and cross border data protection laws. By 2023, research increasingly combined governance principles with automation, artificial intelligence, blockchain, and context specific assessment. (Shah et al. 2023) confirmed that human factors remained central to cyber governance effectiveness. (Cartwright, Cartwright, and Edun 2023) found that small business risk management depended partly on security guidance transferred through IT service providers. (Ghanem et al. 2023) demonstrated the potential of automated expertise extraction for network-security compliance, while (Ibnugraha et al. 2023) examined the reliability of security metrics in academic environments. Collectively, Phase 2 progressed from risk recognition and resilience building to quantified governance, adaptive controls, automated compliance, and integrated protection of digital assets.

Phase 3: Accelerated Expansion and Research Maturation (2024–2026)

Research in 2024 marked a movement from general cybersecurity principles towards measurable risks, operational controls, and sector specific governance. (Eshetu, Mohammed, and Salau 2024) detected extensive weaknesses across Ethiopian university websites, including outdated applications, deficient password practices, weak encryption, and inadequate access control. The discovery of 11,286 findings through Vega and 1,749 vulnerabilities through Nessus demonstrated the value of combining awareness assessment with automated testing and ISO/IEC 27001 guidance. (Metin et al. 2024) found that more objective asset valuation could strengthen security culture and improve risk prioritisation. At the operational level, (Chhetri et al. 2024) indicated that human AI collaboration could reduce alert fatigue in security operations centres, although effective allocation of responsibilities between analysts and automated systems remained necessary. Across the wider literature, blockchain, smart contracts, self-sovereign identity, knowledge graphs, machine learning, and digital twins were increasingly applied to insurance, finance, healthcare, smart cities, cloud platforms, and industrial systems. However, behavioural findings continued to expose low cyber hygiene, uneven professional competence, insider risk, and weaknesses in organizational security culture.

The 2025 studies expanded from isolated security solutions towards resilience, regulation, ethical accountability, and implementation frameworks. (Lier et al. 2025) developed a five phase model containing 19 implementation steps and seven performance indicators for organizational adoption of AI enabled cybersecurity.(Linan-Acosta, Bazalar-Gonzales, and Santisteban 2025) applied NIST CSF 2.0 principles to confidential data protection in higher education, reflecting stronger translation of recognized standards into sector specific architectures. (Proudfoot, Cram, and Madnick 2025) showed that organizations faced difficulty navigating overlapping cybersecurity regulations, making coordination and governance capacity as important as technical compliance. Other findings presented generative AI as both a defensive resource and threat enabler, while virtual reality simulations, behavioural modelling, and targeted education improved risk understanding when feedback and contextual relevance were included. In 2026, research became more integrated, dynamic, and explainable. (Varghese and Bui 2026) consolidated information security risk management into a framework connecting governance, assessment, treatment, monitoring, and organizational context.(Jensen et al. 2026) nevertheless identified symbolic oversight in healthcare boardrooms, showing that formal governance structures may create confidence without sufficient strategic engagement. (Ababneh et al. 2026) combined legal, ethical, and institutional requirements within an integrated governance model, while (Islam et al. 2026) demonstrated that explainable AI could support dynamic risk assessment and cybersecurity certification. Overall, Phase 3 progressed from applied vulnerability identification towards adaptive, evidence-based, legally informed, and human centred governance.

Conclusion

This chronological review examined the evolution of research on cybersecurity risk, control, and governance in digital data from 2017 to August 2026. Through systematic advanced searching of the Scopus database, 302 primary journal articles were identified and analyzed to determine changes in publication growth, research priorities, methodological approaches, and technological development. The review specifically aimed to clarify how cybersecurity research has progressed from foundational discussions of risk and control towards more integrated approaches to digital data governance.

The chronological findings demonstrate substantial growth across three developmental phases. The Emergence and Conceptual Foundation phase (2017–2019) contained 10 articles, representing 3.3% of the corpus, and concentrated mainly on risk perception, precautionary behaviour, organizational culture, privacy, and socio technical security. The Development and Sustained Growth phase (2020–2023) included 97 articles, or 32.1%, reflecting wider attention to organizational resilience, regulatory compliance, measurable governance, risk quantification, adaptive controls, and digital asset protection. The Accelerated Expansion and Research Maturation phase (2024–August 2026) contributed 195 articles, accounting for 64.6% of the dataset. This recent concentration indicates increasing scholarly attention to sector-specific architectures, standards-based governance, dynamic risk assessment, legal and ethical accountability, and proactive cybersecurity management. The lower publication count for 2026 should be interpreted cautiously because the dataset covers only the period up to August and may also be influenced by indexing delays.

Several dominant patterns emerged across the timeline. Earlier research primarily examined individual behaviour, perceived risk, and organizational security weaknesses through surveys, conceptual studies, and socio technical assessments. Subsequent studies adopted more

structured, quantitative, mixed, and context sensitive approaches for evaluating risk exposure, governance compliance, control effectiveness, and organizational resilience. Recent research has increasingly integrated artificial intelligence, machine learning, explainable AI, behavioural analytics, automation, blockchain, digital twins, and human AI collaboration. These developments show that the field has moved beyond isolated technical safeguards towards an integrated governance perspective connecting people, processes, technology, regulation, ethics, and organizational accountability. Nevertheless, the continued presence of human error, weak security culture, fragmented responsibilities, regulatory complexity, and symbolic governance indicates that technological advancement alone cannot ensure effective protection.

Chronological organization contributes to knowledge by making the stages of research development and transition points more visible. Grouping publications by time demonstrates not only the increase in output but also the transformation of research questions, methods, controls, and governance priorities. Compared with a conventional thematic review, the time-based structure reveals how foundational behavioural and socio-technical concerns supported later developments in quantified governance, adaptive protection, automated compliance, and explainable risk assessment. It also identifies the periods in which particular concepts became established, expanded, or integrated into broader cybersecurity frameworks.

The findings provide practical guidance for organizational leaders, cybersecurity professionals, regulators, and data owners. Effective protection of digital data requires coordinated governance structures, clearly assigned responsibilities, continuous risk monitoring, measurable controls, workforce awareness, and alignment with recognized standards and regulatory requirements. Future research should assess advanced governance and AI enabled risk solutions under real organizational conditions, particularly across higher education, healthcare, finance, government, and critical infrastructure. Greater attention is also required for implementation cost, control effectiveness, governance maturity, human oversight, third party dependencies, AI related risks, and the long-term performance of adaptive cybersecurity mechanisms.

Several limitations should be recognized. The review relied solely on Scopus and was restricted to English language, open access, final stage journal articles classified under Computer Science. The selected keywords and exact keyword filters may have excluded relevant studies using alternative terminology or published in other disciplines, languages, databases, and document types. Coverage ending in August 2026 also prevents a complete assessment of that publication year. Future reviews should combine multiple established databases, apply broader interdisciplinary search terms, include multilingual evidence, and conduct comparative, longitudinal, and real-world validation studies. Overall, chronological review provides an important method for capturing the dynamic evolution of scientific knowledge, identifying changes that may remain hidden in thematic synthesis, and guiding evidence-based innovation in cybersecurity risk, control, and governance for digital data.

Acknowledgements: The authors would like to express their sincere gratitude to Universiti Teknologi Malaysia (UTM) Kuala Lumpur, Politeknik Balik Pulau (PBU), Universiti Utara Malaysia (UUM) and Universiti Malaysia Sabah (UMS) for providing the necessary resources and support throughout the course of this research. Special appreciation is extended to colleagues and peers who contributed valuable insights and constructive feedback, which greatly enhanced the quality of this paper.

Funding Statement: This research received no external funding.

Conflict of Interest Statement: The authors certify that they have no conflicting interests in relation to this research.

Ethics Statement: This study did not involve any human participants, animals, or sensitive data requiring ethical approval. The authors confirm that the research was conducted in accordance with accepted academic integrity and ethical publishing standards.

Author Contribution Statement: All authors contributed significantly to the development of this manuscript. Authors Nur Syuhada Mohamad Rodzi, Ganthan Narayana Samy and Noor Hafizah Hassan were responsible for the conceptualization, methodology, and overall supervision of the study. Mohamad Fadli Zolkipli handled data collection, analysis, and interpretation of results. Siti Nur Aqilah Ab-Wahab contributed to the literature review, drafting, and critical revision of the manuscript. All authors read and approved the final version of the manuscript prior to submission.

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 46 (December 2026) PP. 17-32

References

Ababneh, J., H. Attar, H. Alghamdi, I. Obeidat, Y. Sharrab, J. B. Salameh, H. Ali, and M. Hafez. 2026. "Cybersecurity Laws and Ethical Implications: Integrated Cybersecurity Governance Model (CLEI-ICGM)." *Journal of Cloud Computing* 15(1). doi:10.1186/s13677-026-00902-9.

Addae, J. H., X. Sun, D. Towey, and M. Radenkovic. 2019. "Exploring User Behavioral Data for Adaptive Cybersecurity." *User Modeling and User-Adapted Interaction* 29(3):701–50. doi:10.1007/s11257-019-09236-5.

Ahmad, A., K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville. 2020. "How Integration of Cyber Security Management and Incident Response Enables Organizational Learning." *Journal of the Association for Information Science and Technology* 71(8):939–53. doi:10.1002/asi.24311.

Alohali, M., N. Clarke, F. Li, and S. Furnell. 2018. "Identifying and Predicting the Factors Affecting End-Users' Risk-Taking Behavior." *Information and Computer Security* 26(3):306–26. doi:10.1108/ICS-03-2018-0037.

Arora, C. 2019. "Digital Health Fiduciaries: Protecting User Privacy When Sharing Health Data." *Ethics and Information Technology* 21(3):181–96. doi:10.1007/s10676-019-09499-x.

Bongiovanni, I., K. Renaud, H. Brydon, R. Blignaut, and A. Cavallo. 2022. "A Quantification Mechanism for Assessing Adherence to Information Security Governance Guidelines." *Information and Computer Security* 30(4):517–48. doi:10.1108/ICS-08-2021-0112.

Cartwright, A., E. Cartwright, and E. S. Edun. 2023. "Cascading Information on Best Practice: Cyber Security Risk Management in UK Micro and Small Businesses and the Role of IT Companies." *Computers and Security* 131. doi:10.1016/j.cose.2023.103288.

Chhetri, M. B., S. Tariq, R. Singh, F. Jalalvand, C. Paris, and S. Nepal. 2024. "Towards Human-AI Teaming to Mitigate Alert Fatigue in Security Operations Centres." *ACM Transactions on Internet Technology* 24(3). doi:10.1145/3670009.

Damenu, T. K., and C. Beaumont. 2017. "Analysing Information Security in a Bank Using Soft Systems Methodology." *Information and Computer Security* 25(3):240–58. doi:10.1108/ICS-07-2016-0053.

Dennis, A. R., and R. K. Minas. 2018. "Security on Autopilot: Why Current Security Theories Hijack Our Thinking and Lead Us Astray." *Data Base for Advances in Information Systems* 49(s1):15–37. doi:10.1145/3210530.3210533.

Eshetu, Ali Yimam, Endris Abdu Mohammed, and A. Salau. 2024. "Cybersecurity Vulnerabilities and Solutions in Ethiopian University Websites." *Journal of Big Data* 11. doi:10.1186/s40537-024-00980-z.

Ghanem, M. C., T. M. Chen, M. A. Ferrag, and M. E. Kettouche. 2023. "ESASCF: Expertise Extraction, Generalization and Reply Framework for Optimized Automation of Network Security Compliance." *IEEE Access* 11:129840–53. doi:10.1109/ACCESS.2023.3332834.

Goodell, G., and T. Aste. 2019. "Can Cryptocurrencies Preserve Privacy and Comply With Regulations?" *Frontiers in Blockchain* 2. doi:10.3389/fbloc.2019.00004.

Ibnugraha, Prajna Deshanta, Anas Satria, Fabian Sekar Nagari, Moch Fahru Rizal, and Khamla Nonalinsavath. 2023. "The Reliability Analysis for Information Security Metrics in Academic Environment." *International Journal on Informatics Visualization* 7(1):92–97. doi:10.30630/joiv.7.1.1593.

Islam, S., B. Sardar, E. M. Kalogeraki, K. Lampropoulos, and S. Papastergiou. 2026. "Hybrid AI-Based Dynamic Risk Assessment Framework with Explainable AI Practices for

Composite Product Cybersecurity Certification." *International Journal of Information Security* 25(2). doi:10.1007/s10207-026-01218-0.

Jensen, J., F. Quayuum, L. Røstad, and O. Lysne. 2026. "Strategic Illusion and Symbolic Oversight: An Empirical Study of Cybersecurity in Healthcare Boardrooms." *Computers and Security* 170. doi:10.1016/j.cose.2026.105051.

Khan, A., M. Ibrahim, and A. Hussain. 2021. "An Exploratory Prioritization of Factors Affecting Current State of Information Security in Pakistani University Libraries." *International Journal of Information Management Data Insights* 1(2). doi:10.1016/j.jjimei.2021.100015.

Kropczynski, J., Z. Aljallad, N. J. Elrod, H. Lipford, and P. J. Wisniewski. 2021. "Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities." *Proceedings of the ACM on Human-Computer Interaction* 4(CSCW3). doi:10.1145/3432954.

Lier, S. K., T. M. Eppers, J. Gerlach, P. Müller, and M. H. Breitner. 2025. "An Iterative Five-Phase Process Model to Successfully Implement AI for Cybersecurity in a Corporate Environment." *Electronic Markets* 35(1). doi:10.1007/s12525-025-00802-x.

Linan-Acosta, B., O. Bazalar-Gonzales, and J. Santisteban. 2025. "GuardNet: An Architecture Based on NIST v2.0 for Confidential Data Protection in Higher Education Institutions in Peru." *Engineering, Technology and Applied Science Research* 15(6):28977–85. doi:10.48084/etasr.12978.

Metin, B., S. Duran, E. Telli, M. Mutlutürk, and M. Wynn. 2024. "IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture." *Information (Switzerland)* 15(1). doi:10.3390/info15010055.

Mundra, S. 2018. "Blockchain Initiatives and Implementation." *Information Services and Use* 38(3):187–89. doi:10.3233/ISU-180022.

Nyblom, P., G. Wangen, and V. Gkioulos. 2020. "Risk Perceptions on Social Media Use in Norway." *Future Internet* 12(12):1–40. doi:10.3390/fi12120211.

Proudfoot, J. G., W. A. Cram, and S. Madnick. 2025. "Weathering the Storm: Examining How Organisations Navigate the Sea of Cybersecurity Regulations." *European Journal of Information Systems* 34(3):436–59. doi:10.1080/0960085X.2024.2345867.

Rashid, Z., U. Noor, and J. Altmann. 2021. "Economic Model for Evaluating the Value Creation through Information Sharing within the Cybersecurity Information Sharing Ecosystem." *Future Generation Computer Systems* 124:436–66. doi:10.1016/j.future.2021.05.033.

van Schaik, P., J. Jansen, J. Onibokun, J. Camp, and P. Kusev. 2018. "Security and Privacy in Online Social Networking: Risk Perceptions and Precautionary Behaviour." *Computers in Human Behavior* 78:283–97. doi:10.1016/j.chb.2017.10.007.

van Schaik, P., D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev. 2017. "Risk Perceptions of Cyber-Security and Precautionary Behaviour." *Computers in Human Behavior* 75:547–59. doi:10.1016/j.chb.2017.05.038.

Schinagl, S., A. Shahim, and S. Khapova. 2022. "Paradoxical Tensions in the Implementation of Digital Security Governance: Toward an Ambidextrous Approach to Governing Digital Security." *Computers and Security* 122. doi:10.1016/j.cose.2022.102903.

Shah, M. U., F. Iqbal, U. Rehman, and P. C. K. Hung. 2023. "A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance." *IEEE Access* 11:87970–84. doi:10.1109/ACCESS.2023.3296580.

Thompson, N., A. Ahmad, and S. Maynard. 2020. "Do Privacy Concerns Determine Online Information Disclosure? The Case of Internet Addiction." *Information and Computer Security* 29(3):558–69. doi:10.1108/ICS-11-2020-0190.

Varghese, B. B., and Q. N. Bui. 2026. "An Integrated Framework for Information Security Risk Management: A Mixed-Methods Systematic Literature Review." *Computers and Security* 168. doi:10.1016/j.cose.2026.104957.

da Veiga, A., L. V Astakhova, A. Botha, and M. Herselman. 2020. "Defining Organisational Information Security Culture—Perspectives from Academia and Industry." *Computers and Security* 92. doi:10.1016/j.cose.2020.101713.

Wan, Z., L. Bao, D. Gao, E. Toch, X. Xia, T. Mendel, and D. Lo. 2019. "AppMoD: Helping Older Adults Manage Mobile Security with Online Social Help." *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3(4). doi:10.1145/3369819.

Zhang, L., A. Taal, R. Cushing, C. de Laat, and P. Grosso. 2022. "A Risk-Level Assessment System Based on the STRIDE/DREAD Model for Digital Data Marketplaces." *International Journal of Information Security* 21(3):509–25. doi:10.1007/s10207-021-00566-3.