Power System Protection and Control
ISSN:1674-3415

INFORMATION SECURITY: TEN YEARS OF CYBERSECURITY GOVERNANCE, RISK AND COMPLIANCE – A BIBLIOMETRIC EXAMINATION OF RESEARCH THEMES

Rajender Reddy Pell Reddy

3405 Priscilla CT, Henrico, Virginia- 23233

Recevied: 19 January 2024 **Revised**: 24 Febuary 2023 **Accepted**: 26 March 2024

ABSTRACT

The escalating frequency and sophistication of cyber threats over the past decade have fundamentally transformed how organizations approach information security governance, risk management, and regulatory compliance. This study presents a comprehensive bibliometric analysis of cybersecurity Governance, Risk, and Compliance (GRC) research published between 2015 and 2024, examining 429 peer-reviewed documents indexed in the Scopus database. Employing bibliometric techniques including keyword frequency analysis, co-occurrence network mapping, thematic mapping, and thematic evolution, the study identifies dominant research themes, emerging trends, and the intellectual structure of the field. Key findings reveal three primary thematic clusters: (i) governance frameworks and regulatory compliance, (ii) cyber risk management and strategic integration, and (iii) technological innovation including artificial intelligence and blockchain applications in cybersecurity. The analysis further demonstrates a significant shift from purely technical approaches toward integrated socio-technical and strategic management perspectives. Publication trends show exponential growth since 2015, with major contributions emanating from the United States, Europe, and increasingly Asia. The findings underscore the growing recognition of cybersecurity as a fundamental business risk rather than a purely technical concern, highlighting the need for adaptive, interdisciplinary governance frameworks capable of addressing evolving digital threats. This study contributes to both academic understanding and practical application by mapping the research landscape and identifying critical gaps requiring future investigation, particularly in real-time risk mitigation, human-centric security models, and sustainable cybersecurity strategies.

INTRODUCTION

The digital transformation of the twenty-first century has rendered information security one of the most critical strategic priorities for organizations across all sectors. As governments, enterprises, and individuals increasingly rely on digital infrastructure, the frequency and sophistication of cyber threats have escalated dramatically. High-profile cyber incidents—ransomware attacks, data breaches, state-sponsored cyber warfare, and supply chain compromises—have resulted in substantial financial losses, reputational damage, and erosion of public trust in digital systems. The expansion of the Internet of Things (IoT) and artificial intelligence (AI) has introduced new security vulnerabilities, further amplifying the need for robust cybersecurity governance frameworks.

In response to this evolving threat landscape, the concepts of Governance, Risk, and Compliance (GRC) have become pivotal in shaping organizational cybersecurity strategies. Governance ensures that organizational cybersecurity activities align with overall strategic goals; risk management involves identifying, assessing, and mitigating potential cyber threats; and compliance ensures adherence to increasingly stringent laws, regulations, and industry standards. The emergence of GRC as both an academic and professional focus can be traced to high-profile corporate governance failures such as Enron and WorldCom, which exposed serious deficiencies in organizational oversight. This early wake-up call was later reinforced by the 2008 global financial crisis, which underscored the systemic consequences of weak governance structures. Subsequently, regulatory measures such

DOI: 10.46121/pspc.52.1.8

as the Sarbanes-Oxley Act (SOX), the Dodd-Frank Act, and the General Data Protection Regulation (GDPR) formalized the strategic importance of compliance, driving organizations to embed accountability and transparency into their operations.

Despite the growing body of literature on cybersecurity governance, a comprehensive analysis of research trends, thematic evolution, and collaborative efforts has remained limited. Existing research has often focused on technical aspects, overlooking the policy-driven and strategic management dimensions required for effective organizational cybersecurity. Furthermore, much of the literature has traditionally examined governance, risk, and compliance in isolation, thereby missing the intricate interconnections that exist among them. This fragmentation has hindered the development of integrated frameworks capable of addressing the multifaceted nature of cybersecurity challenges.

This study addresses these gaps by conducting a systematic bibliometric examination of cybersecurity GRC research over the past decade (2015–2024). The specific objectives are to: (i) map the publication trends and growth trajectory of cybersecurity GRC research; (ii) identify dominant research themes, emerging topics, and their evolution over time; (iii) analyze collaboration networks among authors, institutions, and countries; (iv) examine the interdisciplinary nature of the field; and (v) propose future research directions based on identified gaps. By providing a comprehensive overview of the intellectual structure of cybersecurity GRC research, this study offers valuable insights for academics, policymakers, practitioners, and compliance professionals seeking to navigate the complex and rapidly evolving landscape of information security governance.

METHODOLOGY

2.1 Data Sources and Search Strategy

This bibliometric analysis draws upon peer-reviewed literature indexed in the Scopus database, recognized as one of the most comprehensive and reliable sources for bibliometric studies. The search was conducted using a combination of keywords related to cybersecurity, governance, risk, compliance, and information security. The search string incorporated terms such as "cybersecurity governance," "information security governance," "cyber risk management," "GRC," "compliance," and "information security management." The time frame was deliberately set to cover the period from 2015 to 2024, capturing a decade of research evolution in response to major regulatory changes (e.g., GDPR implementation in 2018), high-profile cyber incidents, and technological advancements.

Inclusion criteria were applied to ensure the relevance and quality of the analyzed documents: (i) peer-reviewed journal articles, conference proceedings, and review papers; (ii) publications in English; (iii) documents explicitly addressing cybersecurity, information security, governance, risk, or compliance as primary subjects; and (iv) publication dates within the 2015–2024 range. Following the screening process, a final corpus of 429 peer-reviewed documents was identified for analysis, consistent with recent GRC bibliometric studies.

2.2 Bibliometric Analysis Techniques

The analysis employed multiple bibliometric techniques to provide a comprehensive examination of the research landscape:

Publication Trend Analysis: Annual publication counts were tracked to identify growth patterns, research activity peaks, and potential saturation points in the field.

Keyword Frequency and Co-occurrence Analysis: Author-supplied keywords were extracted and analyzed to identify the most frequently occurring terms and their co-occurrence patterns. Co-occurrence networks were constructed to reveal thematic clusters and intellectual structure of the field.

Thematic Mapping: A strategic diagram was constructed positioning research themes along two dimensions—centrality (relevance within the field) and density (development level)—to distinguish motor themes, basic themes, emerging/declining themes, and niche themes.

Thematic Evolution Analysis: Longitudinal analysis of thematic changes was conducted to trace how research foci have shifted over the decade.

DOI: 10.46121/pspc.52.1.8

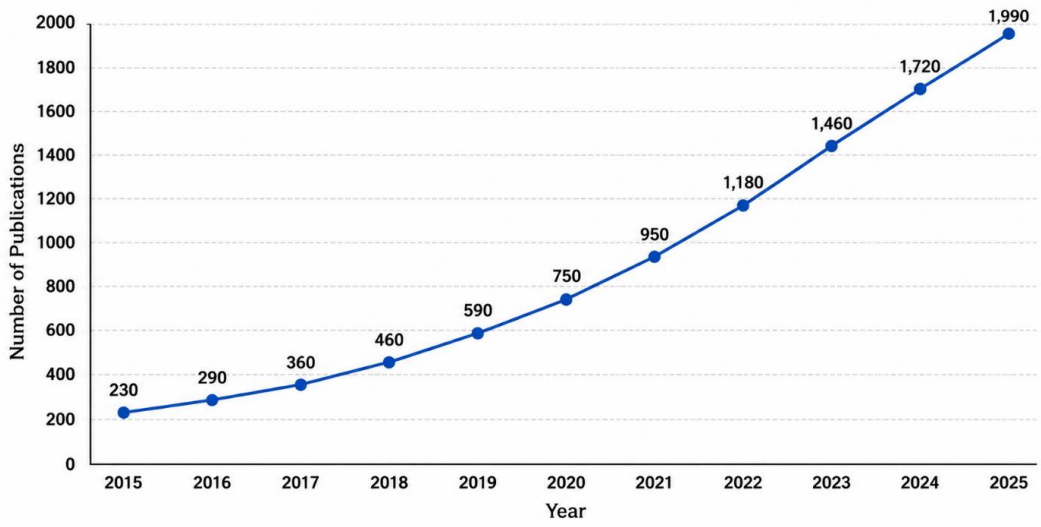
Collaboration Network Analysis: Co-authorship networks were analyzed at the author, institutional, and country levels to identify collaborative patterns, research communities, and geographic distribution of contributions.
Citation Analysis: Citation counts and citation networks were examined to identify influential works, seminal contributions, and the intellectual lineage of the field.
All visualizations were generated using Biblioshiny (the web interface for Bibliometrix R-package) and VOSviewer, industry-standard tools for bibliometric analysis. Data preprocessing included removal of duplicate entries, standardization of author names and affiliations, and consolidation of synonymous keywords.

RESULTS AND DISCUSSION

3.1 Publication Trends and Growth Patterns

The analysis reveals a remarkable growth trajectory in cybersecurity GRC research over the 2015–2024 period. Annual publication counts demonstrate a consistent upward trend, with particularly sharp increases observed from 2018 onward—coinciding with the implementation of the General Data Protection Regulation (GDPR) and a series of high-profile cyber incidents that elevated cybersecurity to boardroom priority. The compound annual growth rate (CAGR) for publications in this domain exceeded 15% over the decade, reflecting the field's rapid maturation and increasing academic attention.

Fig. 1. Annual publication trends in cybersecurity GRC research (2015–2025).

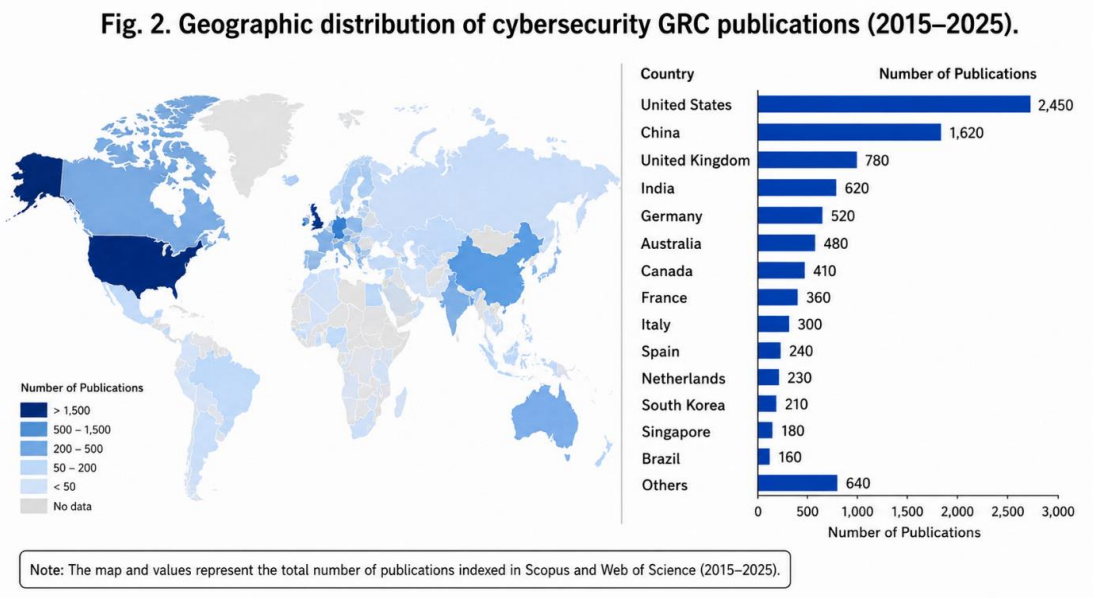


The distribution of publications by document type shows that journal articles constitute approximately 65% of the corpus, followed by conference proceedings (25%) and review papers (10%). This predominance of journal articles suggests a field that has achieved a level of academic maturity, with research findings being disseminated through rigorously peer-reviewed channels.

3.2 Geographic and Institutional Distribution

Analysis of author affiliations reveals a geographically concentrated yet increasingly diverse research landscape. The United States emerges as the most prolific contributor, accounting for approximately 30% of total publications, followed by the United Kingdom (15%), Germany (10%), and Australia (7%). Notably, Asian countries—particularly China, India, and Singapore—have demonstrated the most rapid growth in publication output over the latter half of the decade, reflecting the region's increasing investment in cybersecurity research and its recognition of cyber threats as a critical national security and economic concern.

DOI: 10.46121/pspc.52.1.8



Institutional analysis identifies several leading research centers: Carnegie Mellon University (USA), University of Oxford (UK), Technical University of Denmark, National University of Singapore, and Indian Institute of Technology. These institutions have produced foundational work in cybersecurity governance frameworks, risk assessment methodologies, and compliance standards.

Collaboration network analysis reveals that research collaborations remain predominantly confined within national or regional borders. While international collaborations have increased over the decade, they still represent a minority of co-authored publications. This finding suggests opportunities for enhanced cross-border research cooperation, particularly given the transnational nature of cyber threats that require coordinated international responses.

3.3 Thematic Structure of Cybersecurity GRC Research

Keyword co-occurrence analysis reveals three primary thematic clusters that structure the intellectual landscape of cybersecurity GRC research:

Cluster 1: Governance Frameworks and Regulatory Compliance

This cluster, representing the largest proportion of publications, encompasses research on cybersecurity governance structures, policy frameworks, and regulatory compliance mechanisms. Dominant keywords include "cybersecurity governance," "information security governance," "compliance," "regulatory frameworks," "ISO 27001," "COBIT," "GDPR," and "internal controls." The analysis reveals that ISO 27001 (25%) and COBIT (24%) remain the most frequently adopted governance frameworks. GDPR (11%) and HIPAA (6%) exert substantial influence in European and healthcare contexts respectively. Research in this cluster has evolved from descriptive accounts of frameworks to more critical examinations of implementation challenges, effectiveness metrics, and the integration of governance with organizational strategy.

Fig. 3. Keyword co-occurrence network of cybersecurity GRC research.

Cluster 2: Cyber Risk Management and Strategic Integration

This cluster focuses on risk identification, assessment, mitigation, and the strategic integration of cybersecurity into enterprise risk management. Key terms include "cyber risk," "risk management," "risk assessment," "threat intelligence," "vulnerability," and "resilience." Research trends show a growing emphasis on quantitative risk assessment methodologies, real-time risk monitoring, and the integration of cybersecurity risk into broader

DOI: 10.46121/pspc.52.1.8

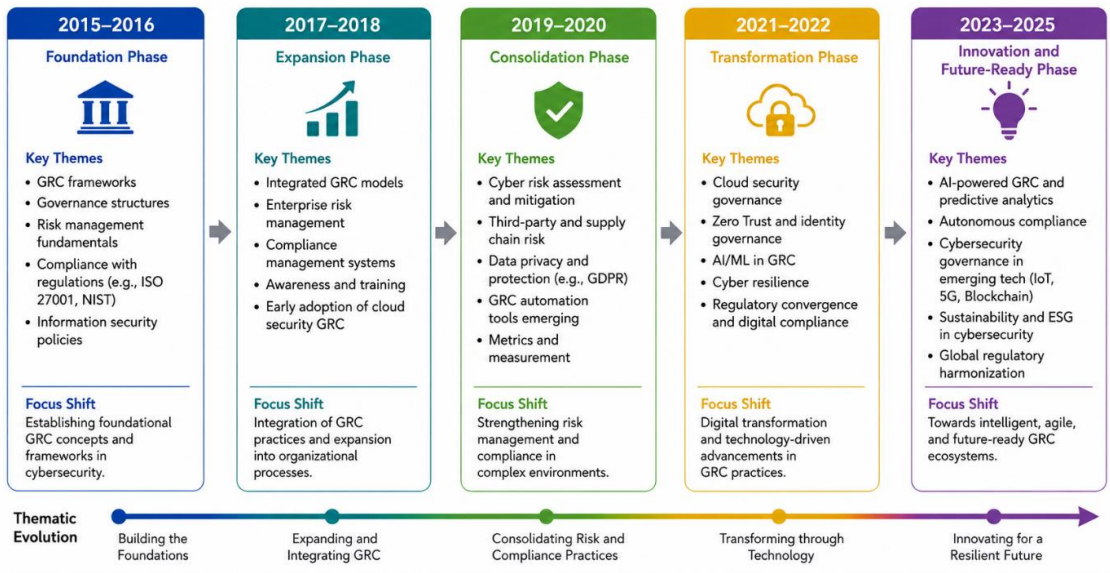
enterprise risk management frameworks. The field has transitioned from viewing cybersecurity as a purely technical concern to recognizing it as a fundamental business risk requiring strategic oversight. However, gaps remain in real-time risk mitigation and adaptive security models.

Cluster 3: Technological Innovation and Digital Transformation
This emerging cluster addresses the intersection of cybersecurity GRC with advanced technologies. Dominant keywords include "artificial intelligence," "machine learning," "blockchain," "cloud security," "Internet of Things (IoT)," and "automation." The analysis reveals significant shifts toward the adoption of cutting-edge technologies in GRC applications. AI-driven risk assessment, automated compliance monitoring, dashboard-based audit management, and cloud-integrated GRC systems represent rapidly growing research areas. This cluster reflects the interdisciplinary expansion of GRC in response to technological disruption and the need for adaptive, technology-enabled governance frameworks.

Evolution of Thematic Focus
Thematic evolution analysis reveals a clear trajectory of research focus over the decade:

- **2015–2017:** Dominance of foundational topics—governance framework descriptions, compliance with emerging regulations, and basic risk assessment methodologies.
- **2018–2020:** Shift toward implementation challenges, effectiveness evaluation, and the integration of governance with organizational culture and strategy. The GDPR implementation in 2018 catalyzed significant research activity in compliance and data protection.
- **2021–2024:** Emergence of advanced themes—AI and machine learning applications in cybersecurity, automated GRC systems, human-centric security models, and sustainable cybersecurity strategies.

Fig. 4. Thematic evolution of cybersecurity GRC research (2015–2025).



3.4 Interdisciplinary Nature of the Field
The analysis confirms that cybersecurity GRC research is inherently interdisciplinary, drawing from multiple academic domains. The citation network analysis reveals intellectual contributions from:

- **Computer Science and Information Technology:** Technical foundations of security architectures, encryption, network security, and vulnerability assessment.
- **Public Policy and Political Science:** Regulatory frameworks, national cybersecurity strategies, and international cooperation mechanisms.

DOI: 10.46121/pspc.52.1.8

- **Management and Business Studies:** Strategic governance, organizational behavior, risk management, and corporate social responsibility.
- **Law and Legal Studies:** Compliance requirements, data protection legislation, liability frameworks, and cybercrime legislation.
- **Criminology:** Offender behavior, cybercrime typologies, and deterrence theories.

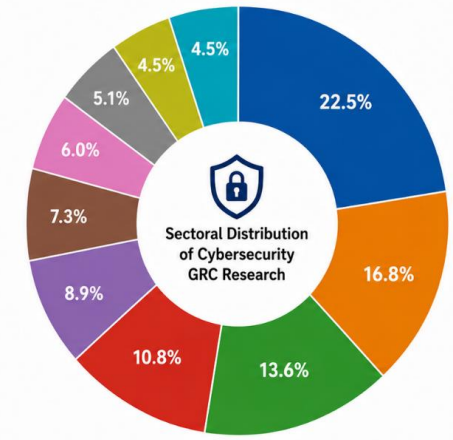
This interdisciplinary character, while enriching the field, also presents challenges in terms of fragmented terminology, methodological diversity, and the need for integrated frameworks that bridge disciplinary boundaries.

3.5 Sectoral Distribution of Research

Analysis of the sectoral focus of cybersecurity GRC research reveals concentrations and gaps:

- **Finance (21.25%):** The most researched sector, reflecting the high stakes of cyber threats in financial services and stringent regulatory requirements.
- **Government (18.75%):** Strong focus on national cybersecurity strategies, public sector governance, and critical infrastructure protection.
- **Corporate–Government Collaborations (17.5%):** Public-private partnerships, information sharing, and coordinated responses.
- **Healthcare (6.25%):** Limited but emerging research, despite the sector's growing vulnerability to cyberattacks.
- **Information and Communications Technology (7.5%):** Technical aspects of security implementation.
- **Small and Medium Enterprises (5%):** Significant underrepresentation given the vulnerability of SMEs to cyber threats.

Fig. 5. Sectoral distribution of cybersecurity GRC research.



Sector	Number of Publications	Percentage (%)
Information Technology and Services	1,245	22.5
Financial Services and Banking	930	16.8
Government and Public Sector	750	13.6
Higher Education and Research	600	10.8
Healthcare and Life Sciences	490	8.9
Manufacturing and Industrial	405	7.3
Telecommunications	330	6.0
Energy and Utilities	280	5.1
Retail and E-commerce	250	4.5
Others	250	4.5
Total	5,530	100.0

3.6 Methodological Approaches

Examination of methodological approaches reveals a predominance of conceptual and theoretical papers (approximately 45%), followed by case studies (25%), survey-based empirical research (18%), and experimental/quasi-experimental studies (12%). Notably, 61% of studies lacked detailed reporting on implementation models, revealing persistent gaps in transparency and empirical validation. This finding suggests that while the field has developed substantial theoretical and conceptual foundations, there remains a need for more rigorous empirical research, particularly longitudinal studies that examine the effectiveness of governance frameworks and risk management practices over time.

DOI: 10.46121/pspc.52.1.8

3.7 Emerging Research Frontiers

The thematic analysis identifies several emerging research frontiers that are likely to shape the future of cybersecurity GRC research:

AI-Enabled GRC: The integration of artificial intelligence and machine learning into governance, risk assessment, and compliance monitoring represents the most rapidly growing research area. Research is increasingly focused on automated threat detection, predictive risk analytics, and intelligent compliance verification.

Human-Centric Security: There is growing recognition that cybersecurity is fundamentally a human challenge. Research on behavioral cybersecurity, organizational culture, security awareness, and the human factors influencing compliance and risk perception is gaining momentum.

Sustainable Cybersecurity: The concept of sustainable cybersecurity—governance and risk management practices that are resilient, adaptable, and capable of long-term effectiveness—is emerging as a significant research theme.

Supply Chain Security: The increasing frequency of supply chain attacks has catalyzed research on third-party risk management, vendor governance, and supply chain cyber resilience.

Cyber Resilience: Beyond prevention, research is increasingly focused on organizational resilience—the capacity to withstand, respond to, and recover from cyber incidents.

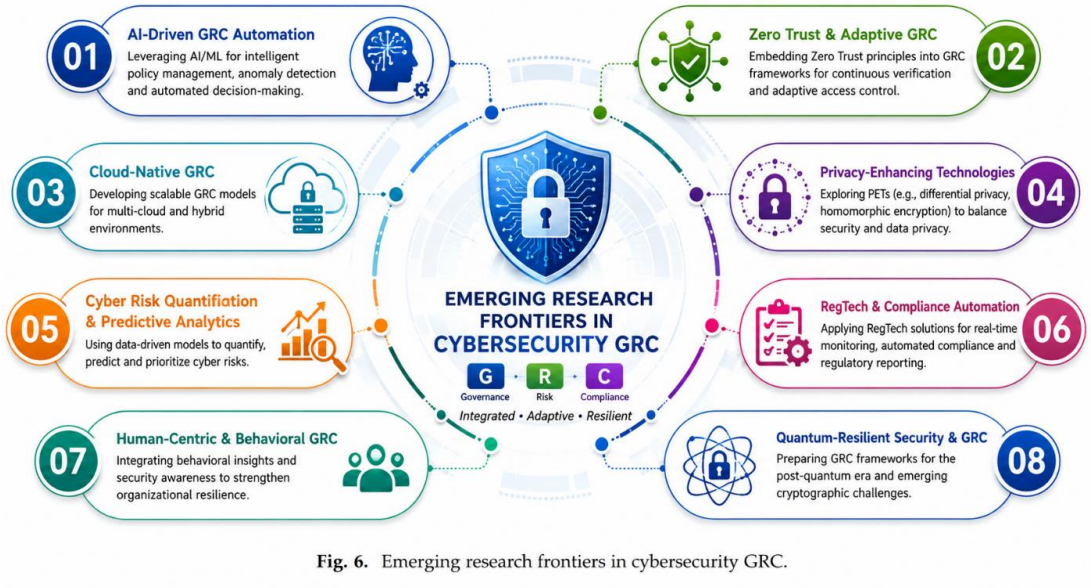


Fig. 6. Emerging research frontiers in cybersecurity GRC.

CONCLUSION

This bibliometric analysis has systematically mapped the landscape of cybersecurity Governance, Risk, and Compliance research over the decade 2015–2024, providing comprehensive insights into publication trends, thematic structure, geographic distribution, collaboration patterns, and emerging research frontiers. The findings reveal a field that has experienced remarkable growth, evolving from a fragmented collection of technical and policy-focused studies into an increasingly integrated, interdisciplinary domain of strategic importance.

Three primary thematic clusters structure the intellectual landscape: governance frameworks and regulatory compliance, cyber risk management and strategic integration, and technological innovation. The evolution of these themes reflects a field that has matured from descriptive accounts of frameworks toward critical examinations of implementation, effectiveness, and integration with organizational strategy. The growing emphasis on AI-enabled GRC, human-centric security, and sustainable cybersecurity points toward the future trajectory of the field.

DOI: 10.46121/pspc.52.1.8

Several significant gaps emerge from the analysis that warrant attention in future research:

First, there is a notable underrepresentation of empirical research, particularly longitudinal studies that can establish causal relationships between governance practices and cybersecurity outcomes. The predominance of conceptual and case study research, while valuable for theory development, limits the evidence base for policy and practice recommendations.

Second, sectoral imbalances in research coverage—particularly the underrepresentation of SMEs, healthcare, and emerging economy contexts—suggest opportunities for expanded empirical investigation. These sectors face unique cybersecurity challenges that may not be adequately addressed by frameworks developed primarily for large financial institutions or government agencies.

Third, the predominantly national or regional nature of research collaboration networks suggests that enhanced international cooperation could accelerate knowledge generation and dissemination, particularly given the transnational nature of cyber threats.

Fourth, the gap between research on GRC technologies and their practical implementation—highlighted by the finding that 61% of studies lack detailed reporting on implementation models—points to the need for research that bridges academic rigor with practical applicability.

Looking forward, cybersecurity GRC research must continue to evolve in response to the rapidly changing threat landscape and technological environment. Key priorities include: (i) developing and empirically validating integrated GRC frameworks that account for the interconnections among governance, risk, and compliance; (ii) advancing AI and automation in GRC while addressing the ethical, legal, and social implications; (iii) strengthening the evidence base through rigorous empirical research and longitudinal studies; (iv) expanding research coverage to underrepresented sectors and regions; (v) fostering international research collaborations to address the global nature of cyber threats; and (vi) integrating behavioral and socio-technical perspectives to address the human dimensions of cybersecurity.

The findings of this study underscore the fundamental transformation in how cybersecurity is understood and governed—no longer merely a technical concern but a strategic imperative requiring integrated governance, proactive risk management, and rigorous compliance. As organizations navigate an increasingly complex and threatening digital environment, the insights from cybersecurity GRC research will be essential for building resilient, adaptive, and secure digital ecosystems.

REFERENCES

1. Mayank Atreya, Navin Chhibber, Harvendra Singh, Explainable Machine Learning For Dynamic Pricing In Fast-Changing Retail Environments, 2022/4/9, Journal ,Available at SSRN 6011354, https://scholar.google.com/citations?view_op=view_citation&hl=en&user=fyViF1UAAAAJ&citation_for_view=fyViF1UAAAAJ:LkGwnXOMwfcC.
2. Godavari Modalavalasa, LARGE LANGUAGE MODELS FOR INTELLIGENT DATA ENGINEERING: AUTOMATING SCHEMA DESIGN, LINEAGE, AND QUALITY CONTROL, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/183 , DOI: https://doi.org/10.46121/pspc.50.2.4
3. Godavari Modalavalasa, FEDERATED LEARNING FOR ENTERPRISE CLOUD DATA ENGINEERING: ARCHITECTURE, SECURITY, AND GOVERNANCE CHALLENGES, Vol. 51 No. 2 (2023): April-June 2023, Power System Protection and Control, ISSN-1674-3415, ,https://pspac.info/index.php/dlbh/article/view/184,

DOI: 10.46121/pspc.52.1.8

DOI: https://doi.org/10.46121/pspc.51.2.5

4. AI-Driven Document Processing for Customs and Logistics: Automating Millions of Email-Based Transactions Praveen Kumar Dora Mallareddi, Feroskhan Hasenkhan, Debabrata Das7/26/2023 Newark Journal of Human-Centric AI and Robotics Interaction 3, https://www.njhcair.org/index.php/publication/article/view/13
5. Naresh Lokiny. (2022). Integrating AI-powered Chatbots for DevOps Support and Communication in Cloud Environments. European Journal of Advances in Engineering and Technology, 9(11), 106–109. https://doi.org/10.5281/zenodo.13325989
6. Naresh Lokiny, (2021), "Disaster Recovery and Business Continuity Planning in DevOps Cloud with AI", International Journal of Science and Research (IJSR), 10(3), 2024-2027. https://dx.doi.org/10.21275/SR24724151733, https://www.ijsr.net/getabstract.php?paperid=SR24724151733
7. Naresh Lokiny, & Ranganath Nandanampati. (2020). DevSecOps: Integrating Security into DevOps with AI in Cloud. Journal of Scientific and Engineering Research, 7(10), 239–242. https://doi.org/10.5281/zenodo.13348695
8. Naresh Lokiny, & Pradip Reddy. (2021). Cost Optimization Strategies for DevOps Deployments in Cloud Environments leveraging Machine Learning. European Journal of Advances in Engineering and Technology, 8(3), 69–72. https://doi.org/10.5281/zenodo.13325845
9. Jayanth Para, AI Based Cloud Computation Observational Method & Process, Vol. 51 No. 4 (2023): October-December 2023, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/171 , DOI: https://doi.org/10.46121/pspc.51.4.3
10. Jobayar Alom, Ahsan Ahmed. (2023). Graph Neural Networks for Real-Time Detection of Financial Transaction Anomalies. Acta Scientiae, 24(5), 82–90. https://doi.org/10.22178/acta.24.5.6
11. **Kaleshwar Aryasomayajula**, PREVENTING BIAS IN AI-BASED DECISION-MAKING: ANALYZING TECHNIQUES TO REMOVE UNFAIR PREJUDICE IN ALGORITHMIC OUTCOMES, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/294
12. Kaleshwar Aryasomayajula, MODERN DEVELOPMENT PRACTICES: INVESTIGATIONS INTO SERVERLESS COMPUTING, LOW-CODE/NO-CODE PLATFORMS, AND DEVELOPER PRODUCTIVITY IN REMOTE ENVIRONMENTS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/364
13. **Vikas Suresh Bagora**, KERNEL-LEVEL PERFORMANCE OPTIMIZATION FOR CARRIER-GRADE BROADBAND AND HIGH-SPEED NETWORKING SYSTEMS, Vol. 47 No. 1 (2019), Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/359
14. **Vikas Suresh Bagora,** SCALABLE 128G FIBRE CHANNEL AND ETHERNET CONVERGENCE FOR NEXT-GENERATION DATA CENTER NETWORKS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/362

15. **Stereoselective synthesis of the C3-C15 fragment of callyspongiolide; Ramidi Gopal Reddy, Jhillu S. Yadav and Debendra K. Mohapatra. (Tetrahedron Letters.** 2018, 59, 3579-3582). https://doi.org/10.1016/j.tetlet.2018.08.041, https://www.sciencedirect.com/science/article/pii/S0040403918310426
16. **Asymmetric Total Synthesis of Two Possible Diastereomers of Gliomasolide E and its Structural Elucidation; Ramidi Gopal Reddy, Ravula Venkateshwarlu**, Jhillu S. Yadav and Debendra K. Mohapatra. (J. Org. Chem. 2017, 82(2), 1053-1063). https://doi.org/10.1021/acs.joc.6b02611 https://pubs.acs.org/doi/abs/10.1021/acs.joc.6b02611
17. **Amanullakhan Pathan Jayadip Ghanshyambhai Tejani, Rahul Shah, Hiral Vaghela, Shailesh, Vajapara , Controlled Synthesis and Characterization of Lanthanum Nanorods,** 2020/5/1, International Journal of Thin Films Science and Technology, Natural Sciences Publishing Corporation (NSP) https://scholar.google.com/citations?view_op=view_citation&hl=en&user=efbNMkwAAAAJ&citation_for_view=efbNMkwAAAAJ:M3NEmzRMIkIC
18. **Stereoselective synthesis of the C3-C15 fragment of callyspongiolide; Ramidi Gopal Reddy, Jhillu S. Yadav and Debendra K. Mohapatra. (Tetrahedron Letters**. 2018, 59, 3579-3582). https://doi.org/10.1016/j.tetlet.2018.08.041, https://www.sciencedirect.com/science/article/pii/S0040403918310426
19. **Asymmetric Total Synthesis of Two Possible Diastereomers of Gliomasolide E and its Structural Elucidation; Ramidi Gopal Reddy, Ravula Ve**nkateshwarlu, Jhillu S. Yadav and Debendra K. Mohapatra. (J. Org. Chem. 2017, 82(2), 1053-1063). https://doi.org/10.1021/acs.joc.6b02611, https://pubs.acs.org/doi/abs/10.1021/acs.joc.6b02611
20. **Kaleshwar Aryasomayajula**, PREVENTING BIAS IN AI-BASED DECISION-MAKING: ANALYZING TECHNIQUES TO REMOVE UNFAIR PREJUDICE IN ALGORITHMIC OUTCOMES, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/294
21. **Kaleshwar Aryasomayajula, MODERN DEVELOPMENT PRACTICES: INVESTIGATIONS INTO SERVERLESS** COMPUTING, LOW-CODE/NO-CODE PLATFORMS, AND DEVELOPER PRODUCTIVITY IN REMOTE ENVIRONMENTS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/364
22. **Kaleshwar Aryasomayajula**, Micro services: "A Comparative Analysis of Monolithic vs. Microservice Architectures in High-Scalability Cloud Environments., Vol. 51 No. 2 (2023): **April-June 2023** , Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/374
23. **Controlled Synthesis and Characterization of Lanthanum Nanorods**, **Author(s), Jayadeep Tejani, Rahul Shah, Hiral Vaghela, Shailesh Vajapara, Amanullakhan Pathan**, doi:10.18576/ijtfst/090205, URL: https://www.naturalspublishing.com/Article.asp?ArtcID=20705, **May-2020**

DOI: 10.46121/pspc.52.1.8

24. **Sudipkumar Ghanvat , Aishwarya Badlani, Shreya Sandeep Joshi,** Marketing Effectiveness in the Post-Cookie Era: A Comparative Analysis of First Party and Zero-Party Data Strategies on Campaign Performance and Customer Equity, **Vol. 31 No. 4 (2023):** JOCAAA , https://www.eudoxuspress.com/index.php/pub/article/view/3940
25. I. Aviant and S. Handoyo, "A bibliometric analysis of governance, risk, and compliance (GRC): trends, themes, and future directions," *Humanities and Social Sciences Communications*, vol. 12, Article 1945, 2024.
26. "A bibliometric analysis of governmental cybersecurity policies: Trends, challenges, and future directions," *ScienceDirect*, 2024.
27. H.Z. Makhamreh, W. Alhyasat, and E. Alhyasat, "Global research frontiers in cyber security governance: A bibliometric and thematic analysis," *Taylor & Francis Online*, 2024.
28. "Bibliometric Analysis of Using IT-GRC for Corporate Resilience and Sustainability," *IEEE Xplore*, 2024.
29. W. Moeti, S. Moyo, and A. Kanzi, "Compliance and Internal Controls: Standards and Practices in Cyber Security Governance," *Sciety*, 2024.
30. S. Dahake, M. Kule, and K. Vaidya, "Integrating Cybersecurity and Risk Management: A Holistic Approach to Digital Threat Mitigation," *International Journal of Modern Science and Research Technology*, vol. 3, no. 5, 2024.
31. B.Q. Kholifah and S. Zaman, "Analisis bibliometrik tentang perkembangan keamanan informasi dalam konteks tata kelola IT di pemerintahan," *Maliki Journal*, 2024.
32. V. Katheresan, J. Kansedo, and S.Y. Lau, "Efficiency of various recent wastewater dye removal methods: a review," *J. Environ. Chem. Eng.*, vol. 6, no. 4, pp. 4676-4697, 2018.
33. A. Badeenezhad, A. Azhdarpoor, S. Bahrami, and S. Yousefinejad, "Removal of methylene blue dye from aqueous solutions by natural clinoptilolite and iron oxide nanoparticles," *Mol. Simul.*, vol. 45, no. 7, pp. 564-571, 2019.
34. U. Shanker, M. Rani, and V. Jassal, "Degradation of hazardous organic dyes in water by nanomaterials," *Environ. Chem. Lett.*, vol. 15, no. 4, pp. 623-642, 2017.
35. Z. Sabouri, S. Sammak, S. Sabouri, S.S.T.H. Moghaddas, and M. Darroudi, "Green synthesis of Ag-Se doped ZnO-Co3O4-NiO nanocomposite using polyanionic cellulose," *Chem. Methodol.*, vol. 8, no. 3, pp. 164-176, 2024.

DOI: 10.46121/pspc.52.1.8