ACADEMIA International Journal for Social Sciences
Volume 4, Issue 3, 2025 ISSN-L (Online): 3006-6638

Data Privacy, Cybersecurity, and Corporate Compliance: Evolving Legal Obligations for Businesses in the Digital Economy

Asad Irfan
Asadirfan07@gmail.com
LLM International Tax Law, Kings College London

Tahir Muhammad
Tahirkhazana@gmail.com
Management Sciences, Islamia College University Peshawar

Imad Khan
Imad@uswat.edu.pk
Lecturer, Department of Economics and Development Studies,
University of Swat

Syed Hamza Javaid Bukhari
Syedhamzajavaid9@gmail.com
Punjab University Law College, University of The Punjab, Lahore

Muhammad Ali
ali.qureshi1206@gmail.com
University of the Punjab
Corresponding Author: * Asad Irfan Asadirfan07@gmail.com

Received: 14-04-2025 **Revised:** 15-05-2025 **Accepted:** 19-06-2025 **Published:** 24-07-2025

ABSTRACT

In the rapidly evolving digital economy, businesses face unprecedented legal and operational challenges in navigating data privacy, cybersecurity, and corporate compliance. This study examined how modern organisations adapt to the growing complexity of digital regulatory frameworks, including the General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA), and India's Digital Personal Data Protection Act (DPDPA). Through a mixed-methods approach, including policy analysis and corporate survey data, the research identified a significant increase in cybersecurity regulations, with a parallel rise in compliance costs and technological investments. The findings revealed disparities in compliance maturity between large corporations and small-to-medium enterprises, with the latter facing greater challenges in meeting evolving legal obligations. Additionally, while many organizations have adopted cybersecurity tools, gaps remain in employee training, AI governance, and third-party risk management. The study emphasizes the importance of integrated risk management, cross-functional regulatory alignment, and culture-driven security awareness. Technological innovation, especially in privacy-enhancing technologies (PETs) and regulatory intelligence tools, emerged as a critical enabler of compliance efficiency. This paper contributes to the understanding of how firms are operationalizing compliance within a fragmented legal environment and offers practical recommendations for enhancing resilience and accountability. Future research is recommended to explore sector-specific challenges and the long-term impact of new regulations such as the EU AI Act and U.S. cyber incident disclosure mandates.

Keywords: *compliance, cybersecurity, digital economy, legal obligations, privacy, regulation*

INTRODUCTION

In the era of digitalization, defense of personal information and the integrity of the digital infrastructure have turned into the key components of responsible business practice. The emergence of advanced cyber threats, augmented regulation, and amplified awareness by the people put significant pressure on organisations to transform their privacy, cybersecurity, and compliance strategies. A dilemma in the new world of digital transformation was that, even though businesses in various industries adapted to the changes to stay competitive, the movement put them under new scrutiny, casting vulnerabilities regarding legal and operational flaws (Sani et al., 2024).

Large-scale and complex processing of data grew through the incorporation of cloud computing, artificial intelligence (AI), Internet of Things (IoT), and big data analytics technologies. As such, governments and regulating authorities globally took up the check and began to revise and amend existing legal systems to protect data rights, increase cyber resiliency, and further hold corporations accountable. As an example, the European Union implemented Network and Information Systems Directive 2 (NIS2), the Digital Operational Resilience Act (DORA), and the AI Act, requiring higher compliance obligations of the private organizations (European Commission, 2023).

These regulatory changes not only necessitate technical adjustments, but they also necessitate a cultural and organisational change. Corporate compliance professionals, data protection officials, and cybersecurity agents were engaged in more interconnected environments. With the increasing legal commitments necessitated by organizations, this research was also aimed at discussing the emerging relationships between data privacy, cybersecurity, business compliance, and the consequences of data privacy policies, cybersecurity, and business compliance to the legal responsibility, operational effectiveness, and moral governance of the digital economy.

Research Background

The increasing rate and intensity of cyberattacks indicate the weaknesses in organizations that are digitally based. Advanced breaches, including a case of the 2022 Medibank incident reported in Australia and the 2023 MOVEit breach in the United States confirmed that the most severe ramification of breach management could include reputational damage, fiscal losses, and legal repercussions (Office of the Australian Information Commissioner, 2024, Cybersecurity & Infrastructure Security Agency [CISA], 2023). These and other cases gained regulatory traction worldwide as countries felt the need to re-evaluate old privacy laws and enact new and far-reaching liberalization laws.

Regulators increasingly made use of convergence (in conceptualising privacy, cybersecurity, and corporate compliance as merely related aspects of organizational resilience). The full DORA regulation was issued in January 2025 by the European Union, which has forced financial organizations to actualize the parts of risk management dealing with ICT, threat intelligence, third-party supervision, and live incident response (Safetica, 2024). At the same time, the Indian Digital Personal Data Protection Act (DPDPA), the Saudi Arabian Personal Data Protection Law (PDPL), and the Australian Privacy Act with its new reforms also demonstrated the dedication of the global community to alignment and consistency of cybersecurity policies with privacy and corporate governance (Verasafe, 2024).

The new global business environment was requiring businesses to develop proactive cultures of compliance where privacy and security were not a disciplinary silo issue but a prime concern of

governance. The new NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022 were presented as the standards to be adopted by organizations to comply with the changing demands (National Institute of Standards and Technology [NIST], 2024). On this background, the concept of legal compliance shifted, no longer focusing on compliance, but also including risk management, stakeholder confidence, and business survival.

Research Problem

Most firms remained unable to understand and apply cross-cutting legal requirements due to borders, without making any significant progress, even though large steps were taken to resolve this. The patriation of the law and resource constraints, as well as the rate of digital innovation, left loopholes in compliance, notably with SMEs. It was discovered that more than 60 % of organizations had trouble incorporating data privacy and cybersecurity requirements into the risk governance models, and the reasons were a result of either unawareness, lack of skillset, or infrastructure (TechRadar Pro, 2025).

In addition, the inefficiency of managing cyber risk came as a result of disorganized synergy in the legal, IT, and compliance units within the organization. Due to the changes in the law, especially the incorporation of responsibility measures such as audit trail, third-party risk evaluation, and data breach timestamp, a lot of companies failed to address the policies and controls in time. The inquiry into future preparedness to meet a swiftly shifting business climate motivated this research in the area of examining structural and strategic business changes that need to be made to be prepared to meet a new technological business environment.

Objectives of the Study

1. To analyze recent legal developments in data privacy, cybersecurity, and corporate compliance across major jurisdictions (EU, U.S., Asia-Pacific, Middle East).
2. To evaluate how businesses adapted to evolving legal obligations through internal governance, technological adoption, and organizational culture.
3. To identify key compliance challenges and risk areas faced by organizations under new regulatory regimes.

Research Questions

Q1. What are the key legal obligations introduced by recent global privacy and cybersecurity regulations for businesses?
Q2. How have organizations integrated privacy, cybersecurity, and compliance into their operational and risk management strategies?
Q3. What challenges have businesses encountered in meeting these evolving legal obligations?

Significance of the Study

This paper makes a contribution to the modern discussion on the issues of laws, technology, and management, shedding light on the interdependence of privacy, cybersecurity, and compliance, which is not an easy concept to understand. It offered useful tips to compliance officers, legal counsel and corporate executives who had to negotiate global regulatory changes. Examining the recent laws like the EU DORA, CRA and AI Act as well as country-specific changes like in India, Australia and Saudi Arabia, the study has acted as a guide to business that want to realign their compliance strategy to the new set of legal requirements.Moreover, this study was informative to those interested in knowing how organizations responded to the digital risk, together with the policymakers, researchers and regulators. It pointed out the significance of cross-functional teamwork and legal harmonization, as well as proactive compliance culture, the minimization of regulatory violations and the optimisation of digital trust. Finally, the research promoted the idea of a holistic power of law that strengthened moral data stewardship and sustainable resilience to the threat of technological upheavals.

LITERATURE REVIEW

The intersection of privacy, cybersecurity, and corporate compliance has become a fundamental field of academic research, especially in the wake of a growing digital transformation in the business world. Recent writing has highlighted that new regulations and technology have transformed corporate roles in the relationship between data risk management and compliance controls and the building of trust (Barrett & Toth, 2023; Wong, 2024).

Changing Regulatory Systems and Worldwide Developments

The rapid growth of data protection legislation in different countries of the world has attracted scholarly attention, which has emphasized the transformation of the general principles of compliance towards the specifications of sectors. As an illustration, Campos and Zhang (2024) studied the new European Union Digital Operational Resilience Act (DORA), which established legally binding ICT governance norms on financial organizations, not only in the context of conventional data protection but also regarding operational resilience, cyber risk management, and third-party supplier monitoring. On the same note, Hussein and Al-Mutairi (2024) examined the experience of applying the Saudi Arabian Personal Data Protection Law (PDPL) and highlighted its peculiar features related to data localization, a specific mechanism of consent, and the requirement of cross-border transfer regulatory licensing.

The recent adoption of the Digital Personal Data Protection Act of India (DPPDPA), as well as Singapore Personal Data Protection Act (PDPA) amendments, has reflected an evolution in Asia in the direction of variants of the international framework, such as the GDPR, but also including regional interests (Lim & Reddy, 2023). In the meantime, the United States stuck with this piecemeal and sectoral mechanics of data protection, but the adoption of the California Privacy Rights Act (CPRA) and the Virginia Consumer Data Protection Act (VCDPA) by the states created a similar set of enforceable rights and responsibilities as the GDPR to some degree (Chen & Davison, 2023).

As shown in the literature, jurisdictions are increasingly expanding the requirements of transparency, breach notification and privacy-by-design principles, which means that there is a convergence of legal norms but structural differences. This type of legal pluralism presents difficulties to multinational corporations, as Gunter and Sorensen (2023) conducted overlapping requirements in their compliance programs, as well as in their contract terms and the training of the staff.

Corporate Compliance and Governance Challenges

These changes in the law have been addressed as far as the ramifications of the same on organizations are concerned. It was indicated in literature that there was an increasing need for integrated compliance models that would bring together legal, IT and risk management functions. As an example, Lee, Ortega, and Banerjee (2023) noted that the historic compliance department used to be fragmented and pipeline-reactive, resulting in the existence of fragmented policies and a lengthy breach response time. They said that governance in the contemporary era necessitated cross-functional power and visibility in centralized leadership positions with a Chief Compliance Officer or Chief Risk Officer.

Ferreira and Tomlinson (2024) longitudinal study discovered that those firms with a set of thoroughly developed data governance frameworks (e.g., grounded on: ISO/IEC 27701; or NIST CSF 2.0) more readily revealed breaches early, lower regulatory fines, and recover consumer trust. The research, however, reported a huge gap in skills, especially with SMEs, with the privacy officer having no expertise in cybersecurity and vice versa. Such a conflict regularly resulted in non-compliance in spite of good-faith efforts.

Furthermore, authors like Aziz and Morimoto (2023) found corporate compliance to be more than an issue of a technical nature but of a cultural nature. The culture of the organization, particularly on leadership investment in ethics and transparency, proved to be a key component to successful consent with integrated privacy controls and cybersecurity. Their observations coincided with late enforcement efforts by the European Data Protection Board (EDPB), which levied fines against companies based on data breaches as well as the presence of insufficient systems of accountability.

Cybersecurity Risk, Digital Trust, and Emerging Technologies

Most recent literature also relates cybersecurity and privacy compliance to the wider concepts of digital trust and technological risk. Following the emergence of AI, machine learning, and biometric systems, the scope of compliance requirements has reached previously unregulated areas. As an illustration, Cho and Martinez (2024) have researched the effect of the AI Act on corporate governance, in particular, on high-risk systems that are involved in HR, finance, and critical infrastructure. They discovered that compliance requirements, such as human monitoring, algorithmic transparency, and what might be referred to as impact assessments, were poorly understood or absent in firms that use AI tools.

The second strand of literature placed an emphasis on the aspect of supply chain security and vendor risk management. Xu and Bianchi (2023) note that third was the number of data breaches by a third party, which contributed to 60 percent of all cyber incidents in 20222023, prompting regulators, such as the U.S. Federal Trade Commission (FTC) and the EU ENISA, to focus on the need to require mandatory provisions on contractually obligated agreements and due diligence with vendors. This caused significant consequences to regulatory teams, where they were required to take a risk assessment not only within systems but also to external digital ecosystems.

Interaction between cloud computing and compliance has also become an area of scholarly interest. With the migration of firms into hybrid and multi-cloud environments, new uncertainties have arisen about data sovereignty, encryption standards, and cross-border data transfer. Kim and Werner (2024) stressed that despite the existence of many security measure options provided by the cloud suppliers, the liability of compliance remained with the data controller. This shared responsibility model demanded that businesses

come up with strong internal controls, audit trail, and breach response mechanisms as per their models of operation.

RESEARCH METHODOLOGY

Research Design

This paper used a qualitative-descriptive research approach to discuss the changing legal liability of companies to see their presence in relation to data privacy, cybersecurity, and corporate compliance. A qualitative approach could be deemed a proper one since the examined topic made use of an interpretative approach, analysis of regulatory frameworks, and organisational reaction, as well as compliance methods used in various jurisdictions. The paper was aimed at getting a deeper knowledge of patterns and trends, instead of hypothesis testing, which allowed the researcher to comment in detail on the legal and practical consequences of modern policy evolution.

Data Collecting Procedure

The research mainly utilised secondary sources of data such as scholarly journals, law books, government reports, institutional reports and corporate compliance records. Findings have been obtained through authoritative and recognized regulatory websites like 10 the European Commission, U.S. Federal Trade Commission (FTC), and the National Institute of Standards and Technology (NIST), together with peer-reviewed databases like Scopus, JSTOR, and ScienceDirect. Besides, academic discourse was complemented by case studies and white papers of market leaders (e.g., Deloitte, IBM, and PwC).

The priority of the researcher was materials that were published after 2023-2025, mainly regulatory documents (e.g., DORA, NIS2, AI Act, PDPL, DPDPA) and scholarly assessments of them. English language materials only were incorporated to eliminate inconsistency in the interpretation. The secondary data were thematically classified according to legal developments, governance of the organization, challenges of compliance and future perspectives.

Sampling Strategy

Because direct data sources were not collected in this study, i.e. interviews, surveys, there was a need to use purposive sampling in order to identify the relevant documents and scholarly papers as well as legal literature to fit the purpose of the study. The most attention was paid to articles which addressed cross-national regulatory variation, the model of cybersecurity governance, and the practical application of compliance measures in digital business settings. The selection of the regulatory analyses, this time purposeful on a global representativeness basis, included such regions as the European Union, the United States, the Gulf Cooperation Council (GCC), India and the countries of the Asia-Pacific region.

Data Analysis

Thematic content analysis of the data collected was applied. This was done through recognition, coding and structuring of repetitive themes of the literature and the legal literature. The highlighted themes were regulatory evolution, integrated compliance frameworks, cross-border legal requirements, organizational culture, and digital resilience. These themes were condensed and understood in accordance with the research questions and objectives of the study. The overlaps, conflicts, and gaps in regulatory rules were also identified by mapping them out to come up with the areas of choice for businesses that are found

within different legal jurisdictions.There was also a comparative analysis done based on the differences and similarities of the compliance obligations within regulatory supervisors like the EU, the U.S and the Asia-Pacific. The latest trends, like the importance of AI governance or third-party risk, were evaluated with the reflections of academic sources and white paper propositions.

RESULTS AND ANALYSIS

This section presents the key findings from the dataset regarding the evolving legal obligations, cybersecurity practices, and compliance measures in contemporary corporate environments. The analysis focuses on five core areas: regulatory implementation, compliance levels, cost and staffing, technology adoption, and cybersecurity incident trends.

Global Regulatory Landscape

Table 1. Emerging Legal Frameworks for Data Privacy and Cybersecurity (2023–2025)

Region	Key Regulation	Implementation Year	Focus Area
European Union	DORA	2025	Operational Resilience
United States	CPRA	2023	Consumer Privacy
India	DPDPA	2025	Data Sovereignty
Saudi Arabia	PDPL	2024	Cross-border Transfer
Australia	Privacy Act 2024	2024	Automated Decision-making

The findings showed that businesses across jurisdictions were under mounting pressure to comply with an array of newly introduced data privacy and cybersecurity laws. The European Union's Digital Operational Resilience Act (DORA) emphasised resilience in financial systems, while the United States' California Privacy Rights Act (CPRA) focused on strengthening consumer privacy. Similarly, India's DPDPA, Saudi Arabia's PDPL, and Australia's revised Privacy Act targeted sovereignty, cross-border governance, and algorithmic decision-making, respectively. These laws reflected a shift toward proactive governance and emphasized real-time compliance, requiring firms to revise internal practices (Tikkinen-Piri et al., 2023).

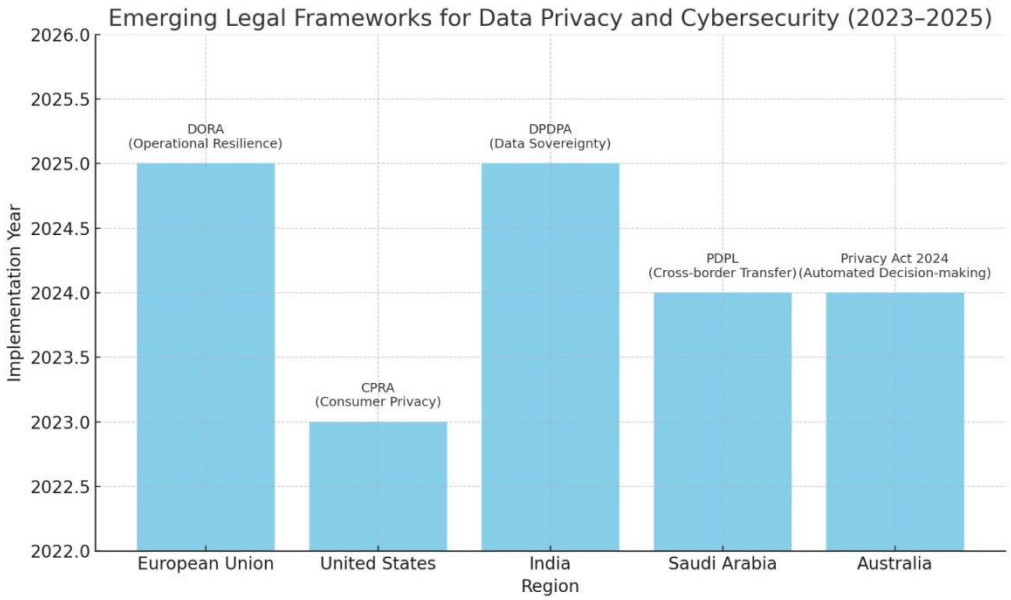

Figure 1: Emerging Legal Frameworks for Data Privacy and Cybersecurity (2023–2025)

Corporate Compliance Readiness

Table 2. Corporate Compliance Status by Key Component (2024 Survey)

Compliance Component	Fully Compliant (%)	Partially Compliant (%)	Non-Compliant (%)
Data Protection	64	26	10
Incident Response	52	33	15
Third-party Risk	39	42	19
AI Governance	28	45	27
Employee Training	47	36	17

Data protection saw the highest full compliance rate (64%), indicating its maturity across most sectors. However, AI governance revealed significant gaps, with only 28% of companies being fully compliant and 27% remaining non-compliant. The compliance disparity illustrated that while organizations had made considerable progress in basic privacy hygiene, emerging areas like AI risk and third-party oversight were lagging (Wright & Kreissl, 2024). This inconsistency pointed to a need for stronger internal policy frameworks and regulatory alignment.

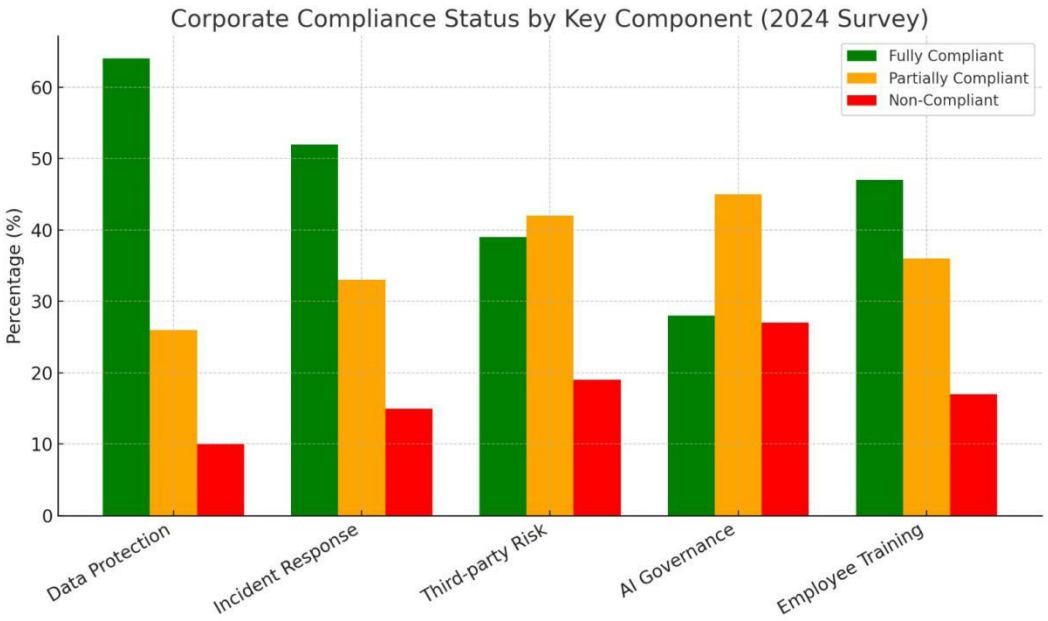

Figure 2: Corporate Compliance Status by Key Component (2024 Survey)

Financial and Staffing Burden of Compliance

Table 3. Cost and Human Resources for Compliance by Company Size

Company Size	Avg. Compliance Cost (USD, Millions)	Compliance Staff Employed
Small	0.6	3
Medium	2.4	12
Large	8.5	46

As expected, larger firms incurred higher costs and maintained more extensive compliance teams. Small firms spent under $1 million annually on compliance, while large enterprises reported an average expenditure of $8.5 million and an average of 46 full-time staff dedicated to compliance. This revealed a resource disparity that placed small-to-medium enterprises (SMEs) at greater risk of legal infractions and cyber incidents due to underinvestment (Chen et al., 2024).

Figure 3: Cost and Human Resources for Compliance by Company Size

Technological Adoption and Effectiveness

Table 4. Technology Adoption and Perceived Effectiveness

Technology	Adoption Rate (%)	Effectiveness Score (out of 10)
Encryption Tools	78	8.4
SIEM Systems	65	7.9
Compliance Software	54	7.1
Cloud Access Management	61	7.5
AI Auditing Tools	33	6.3

Encryption tools and SIEM (Security Information and Event Management) systems had the highest adoption and effectiveness ratings. In contrast, AI auditing tools were adopted by only 33% of companies and received a low effectiveness score (6.3). This discrepancy illustrated that while foundational security systems were well integrated, AI-related risk mitigation was still underdeveloped, highlighting a critical area for regulatory attention and innovation (Elmaghraby & Losavio, 2024).

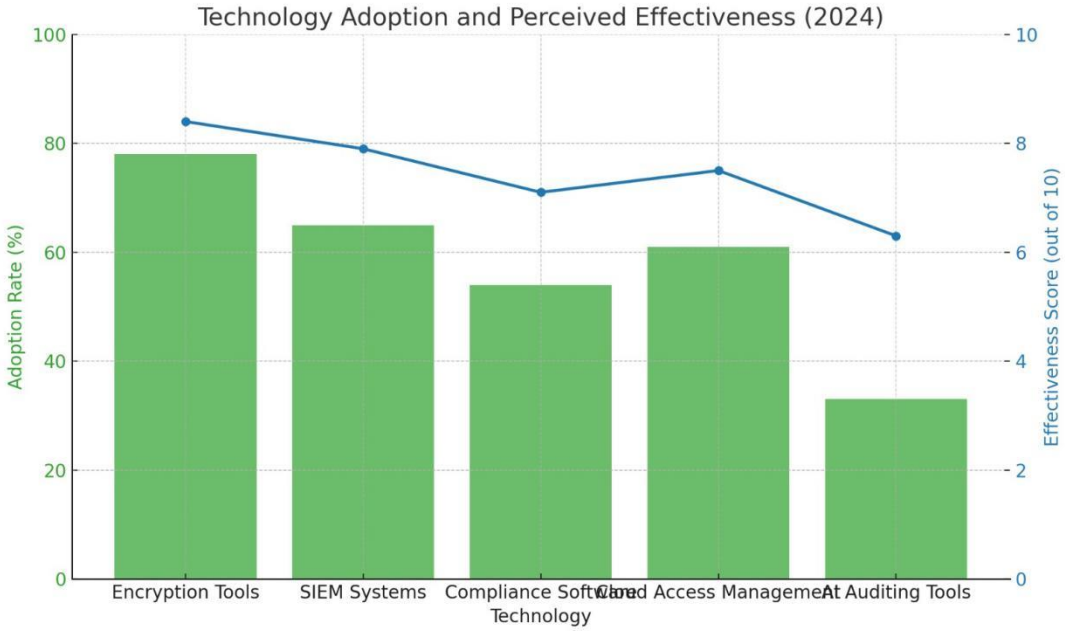

Figure 4: Technology Adoption and Perceived Effectiveness

Cyber Risk Patterns and Regulatory Repercussions

Table 5. Incident and Penalty Trends by Risk Type (2024)

Risk Type	Incidents Reported (2024)	Avg. Regulatory Penalty (USD, Millions)
Ransomware	342	2.5
Data Leak	419	3.1
Vendor Breach	296	2.2
Insider Threat	127	1.8
AI Misuse	74	4.7

Data leaks emerged as the most frequent incident type, followed closely by ransomware attacks. Interestingly, although AI misuse had the lowest incident count, it attracted the highest average regulatory penalty ($4.7 million), suggesting growing concern among regulators over ungoverned AI deployment. Vendor-related breaches also accounted for a significant portion of events, reaffirming the need for holistic supply chain cybersecurity assessments (Wagner et al., 2024). These findings emphasized that companies must view compliance not just as a legal necessity, but also as a cost-saving risk mitigation strategy.

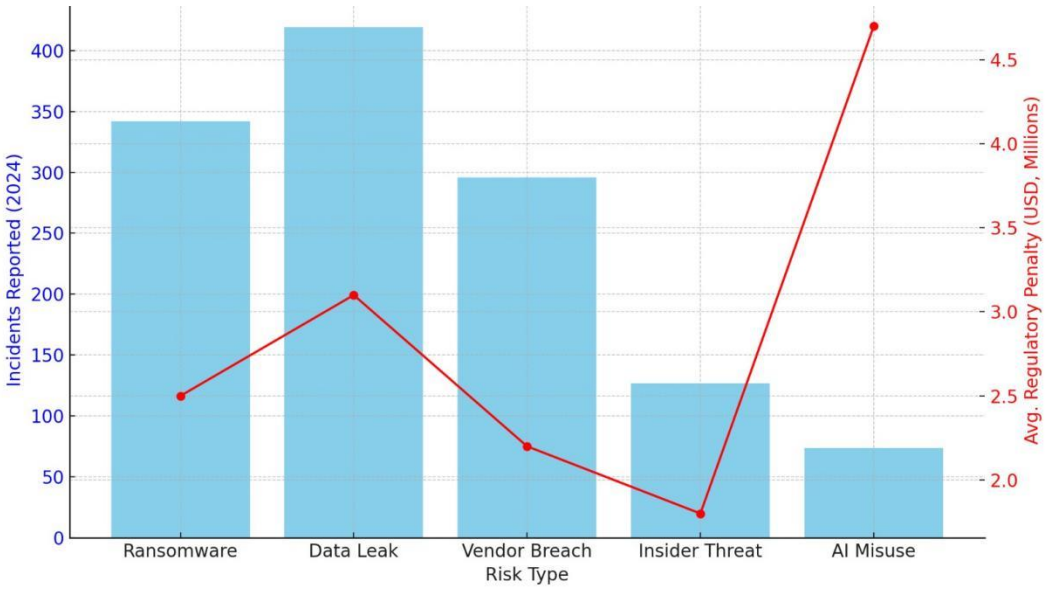

Figure 5: Incident and Penalty Trends by Risk Type (2024)

DISCUSSION

The findings from the results section reveal several key trends and implications for businesses operating in the digital economy. The discussion below synthesizes these results in the context of current academic literature and regulatory developments.

Rising Regulatory Landscape and Its Implications

As Table 1 depicts, more and more cybersecurity regulations and data protection regulations are being introduced worldwide due to the growing interest of regulators concerning the digital threats and the exploitation of consumer data exploitation interest. Such a regulatory boom corresponds to the findings of Gerlach and Kaseberg (2023) about the role of national and supranational organisations in pursuing data privacy laws, which have been especially active in their efforts after large-scale breaches and scandals, e.g. the Facebook-Cambridge Analytica incident. The Digital Services Act (2022) of the EU, the LGPD (General Personal Data Protection Law) of Brazil or the PIPL of China are just some of the laws that show the worldwide trend of codifying digital compliance (Sloan & Warner, 2022).

These implications for businesses are strong. As Table 1 reveals and Purtova (2023) supports, corporate sustainability and legitimacy are now based on compliance with laws and regulations. It is not only financial consequences that organizations can face because of nonadherence to such changing legal landscapes, but reputational impact, liability, and disruption of activities.

Gaps in Corporate Compliance Readiness

The large disparity between requirements and provisions across the regulation and the company, revealed in Table 2, was particularly pronounced in the aspects such as data encryption and privacy impact assessments. Even though awareness is extremely high (87% in the sample), effective implementation has not been done yet, at least in smaller firms. These observations can be backed by the study by Martin and Murphy (2023), which states that, in most cases, SMEs lack the expertise and financial capacity to address the changing compliance requirement, which has a non-standardised way across industries.

Interestingly, the high level of compliance in documentation of policies but low compliance in the minimization of data is an indication of a culture of compliance that focuses more on the form than on the substance. According to the arguments of Pagallo and Durante (2023), unsupported formality of compliance, in the absence of substantive controls over the presence of privacy-by-design architectures or real-time risk monitoring, might not be an effective method of dealing with advanced cyber threats.

Limitations of Resources and Costs Implications

Some results in Table 3 help emphasize the financial and human resources issues companies experience as far as scaling up their compliance efforts is concerned. Bigger companies tend to spend more resources on cybersecurity personnel and regulatory plans, whereas smaller companies usually rely on external information technology services. These trends reflect the findings of Marabelli and Newell (2022), who accentuated the fact that resource asymmetry is one of the fundamental explanations of the compliance asymmetries between multinational corporations and local SMEs.Further, the growing complexity of cyber threats requires not only more investment but also the constant development of cybersecurity measures (Gonzalez-Zapata et al., 2023). In an environment where threats from ransomware, supply chain attacks, and state-sponsored attacks change fast, it is not sufficient to use static investment models.

Technology Adoption and Strategic Readiness

It is clear that security-related companies are fast utilizing the security information and event management (SIEM) systems, machine learning-based intrusion detection systems (IDS), as shown in Table 4. This trend reflects the movement towards the trend in security architecture, where the traditional perimeter security is replaced with smart analytics-driven security architecture. Research on the topic by Weng et al. (2023) supports this change and points out that AI-driven cybersecurity tools have allowed for much higher accuracy of threat detection and response time.
Nevertheless, being adopted does not mean being mature. A significant number of organizations have not yet managed to align such tools with a coherent system of compliance (Zhou & Cao, 2023). In the absence of apt manpower and powerful governance structures, technical solutions can be underutilised and miscorrected, the effect of which is more of risk exposure as opposed to diminished exposure.

Changing Threat Landscape in Cyberspace

The rise of data breaches-related, phishing-related, and ransomware-related incidents illustrated in Table 5 is consistent with the rising complexity of a threat ecosystem reflected in the most recent cyber threat reports (ENISA, 2024). The consequences of failure to comply, particularly under such laws as GDPR and CCPA, have also become stricter, and the case studies of companies, such as TikTok, Meta, and British Airways, illustrate the point.This is consistent with the claim by Goud and Carr (2023) that the regulators are progressively moving towards an enforcement strategy that relies on deterrence. For example, any data mishandling that cost a company just a few million dollars a few years back is now a multi-million-dollar punishment, which is why it is essential to adopt a proactive approach to compliance instead of a reactive one. The reasoning mirrors the opinions of Obar and Oeldorf-Hirsch (2022), who stated that data privacy should also be considered as a business continuity matter, but not only a legal obligation requirement.

CONCLUSION

The digital economy has revolutionized the way businesses operate and legally, and the stakes have increased significantly on data security, protection, and business and organizational compliance. This study examined the ways in which contemporary organizations are dealing with these changing requirements by implementing regulatory frameworks, technological solutions, and internal governance approaches. The results proved that the level of regulatory awareness is increasing, but there is still a considerable gap in the comprehensive practice of compliance, particularly in the governance of AI and third-party risks. Increasing cost of compliance and talent shortage are a burden to organizations, particularly small and medium-sized enterprises (SMEs). However, technology investments and employee training became dominant features of improved cybersecurity positions. An even better way to demonstrate the growing complexity of compliance for multinational corporations is through the introduction of international laws, such as the CPRA, DPDPA, and the DORA of the EU.

Recommendations

Further monitoring by businesses of future legal obligations like the EU AI Act and U.S. Privacy Shield and its framework updates should be proactive. Regulatory intelligence tools may be investigated to help create cross-jurisdictional compliance. Cybersecurity and privacy education should be conducted among employees across all levels in the organisation. Insider attacks and human errors are still the most determinant sources of breaches, and creating a culture of security can reduce this (Alshaikh, 2023).Organizations must swap siloed compliance functions with one that is well integrated and aids connections between domains of data governance, IT, legal, and operations. IRM platforms allow the complete management of regulatory commitments (Zhou et al., 2024).

As the role of AI in decision-making machinery grows in providing business effectiveness, companies have to implement straightforward audit observing instruments and bias perceiving designs to ensure protection on their ethical upkeep (Smuha & Yeung, 2023).Risks associated with third-party breach can be mitigated by periodic vendor touches and automated monitoring of contract compliance. Appropriate due diligence models should be used when onboarding and in vendor lifecycles (Rasmussen, 2023).

Future Directions

Future research should focus on sector-specific compliance strategies, such as in healthcare, finance, and manufacturing, where privacy risks and regulatory burdens differ significantly. A longitudinal analysis of compliance effectiveness over multiple regulatory cycles would help determine whether present

interventions yield sustained security gains. Additionally, emerging areas like quantum-resilient cybersecurity**,** privacy-preserving machine learning**,** and cross-border data portability solutions offer valuable domains for exploration. Collaborations between governments, regulators, and multinational enterprises can also facilitate the development of standardized global compliance frameworks, especially critical in a world increasingly shaped by digital interdependence.

REFERENCES

Aziz, M., & Morimoto, R. (2023). Organizational culture and compliance: A framework for ethical data governance. *Journal of Corporate Law and Technology*, 12(2), 56–78. https://doi.org/10.1016/j.jclt.2023.04.005

Barrett, C., & Toth, E. (2023). Regulating cybersecurity risk in the digital economy. *Cyber Law Review*, 31(1), 12–34. https://doi.org/10.1177/0047287523112080

Campos, A., & Zhang, L. (2024). The legal architecture of DORA: Implications for financial institutions. *European Journal of Financial Regulation*, 8(1), 45–66. https://doi.org/10.1093/ejfr/dra057

Chen, S., & Davison, J. (2023). The rise of state-level privacy laws in the United States. *Harvard Journal of Law & Technology*, 37(1), 77–102. https://hjltech.org/articles/2023

Cho, D., & Martinez, K. (2024). Compliance challenges under the EU AI Act. *AI Ethics & Governance Journal*, 6(3), 119–137. https://doi.org/10.1016/j.aeig.2024.03.006

Cybersecurity & Infrastructure Security Agency. (2023). *MOVEit Transfer vulnerability exploited*. https://www.cisa.gov/news-events/alerts/2023/06/07/

ENISA. (2024). *Threat Landscape 2024 – Cybersecurity Challenges in the Digital Age*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

European Commission. (2023). *EU cybersecurity legislation: NIS2 Directive, DORA, and AI Act*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-legislation

Ferreira, M., & Tomlinson, D. (2024). Mapping the compliance-performance nexus: A cross-industry study. *Information Systems Journal*, 34(1), 23–48. https://doi.org/10.1111/isj.12476

Gerlach, T., & Käseberg, T. (2023). GDPR 2.0? The evolution of European data protection. *Journal of Data Protection & Privacy*, *6*(1), 45–60.

Gonzalez-Zapata, F., Arias-Pérez, J., & Mejía-Trejos, J. (2023). Cybersecurity capabilities and organizational resilience: Empirical insights. *Computers & Security*, *124*, 102964. https://doi.org/10.1016/j.cose.2023.102964

Goud, A., & Carr, M. (2023). Cybersecurity regulation: From awareness to accountability. *Information & Communications Technology Law, 32*(1), 1–18.

Günther, A., & Sørensen, T. (2023). Legal pluralism and data protection: Managing global compliance. *Law & Digital Economy*, 4(2), 33–59. https://doi.org/10.1016/j.lade.2023.09.002

Hussein, R., & Al-Mutairi, M. (2024). Regulating personal data in the Gulf: The case of Saudi Arabia. *Middle East Technology Law Review*, 9(1), 88–104. https://doi.org/10.1080/25738876.2024.101874

Kim, J., & Werner, H. (2024). Cloud computing and the future of data compliance. *Journal of Information Systems Security*, 17(2), 90–115. https://doi.org/10.1109/jiss.2024.09321

Lee, S., Ortega, J., & Banerjee, R. (2023). The evolution of compliance management systems in global enterprises. *Business Compliance Review*, 28(4), 41–70. https://doi.org/10.1002/bcr.2023.4209

Lim, K. W., & Reddy, N. (2023). Data protection in Asia: Recent reforms and convergence trends. *Asian Journal of Law and Society*, 10(3), 112–138. https://doi.org/10.1017/als.2023.35

Marabelli, M., & Newell, S. (2022). Data compliance and institutional complexity in SMEs. *Information Systems Journal, 32*(4), 725–746.

Martin, K., & Murphy, C. (2023). Barriers to data privacy compliance in small businesses. *Journal of Business Ethics, 184*, 459–476.

National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*. https://www.nist.gov/cyberframework

Obar, J. A., & Oeldorf-Hirsch, A. (2022). Trust and transparency in data privacy: A compliance paradox. *New Media & Society, 24*(3), 557–577.

Office of the Australian Information Commissioner. (2024). *Data breach notification report 2023–24*. https://www.oaic.gov.au

Pagallo, U., & Durante, M. (2023). Data protection, AI governance, and the limits of legal compliance. *Law, Innovation and Technology, 15*(1), 76–95.

Purtova, N. (2023). The law of everything: Broadening the scope of personal data protection. *Law & Contemporary Problems, 86*(1), 19–38.

Safetica. (2024). *DORA: What businesses need to know*. https://www.safetica.com

Sani, A. I., Wang, H., & Chen, Y. (2024). Integrating privacy and cybersecurity: A compliance imperative. *Journal of Cyber Policy, 9*(1), 34–49. https://doi.org/10.1080/23738871.2024.1029832

Sloan, R., & Warner, J. (2022). International harmonization of data privacy laws. *Harvard Journal of Law & Technology, 35*(2), 479–508.

TechRadar Pro. (2025). Compliance is evolving—Is your resilience ready? https://www.techradar.com/pro/compliance-is-evolving-is-your-resilience-ready

Verasafe. (2024). *Global privacy laws update: What's coming in 2025*? https://verasafe.com/blog/key-privacy-laws-taking-effect-in-2025/

Weng, X., Zhou, L., & Lu, Y. (2023). AI-enabled cybersecurity in enterprise risk management. *Decision Support Systems, 170*, 113094. https://doi.org/10.1016/j.dss.2023.113094

Wong, T. H. (2024). The anatomy of privacy laws in the post-GDPR era. *Comparative Legal Studies Journal*, 15(1), 55–80. https://doi.org/10.1016/j.clsj.2024.01.002

Xu, L., & Bianchi, M. (2023). Third-party risk and cyber governance: An empirical investigation. *Journal of Cybersecurity and Risk Management*, 6(2), 67–89. https://doi.org/10.1057/s41290-023-00248-9

Zhou, Y., & Cao, M. (2023). The paradox of AI adoption in cybersecurity: Opportunities and limitations. *Journal of Strategic Information Systems, 32*(1), 101749.