International Academic Institute for Science and Technology

International Academic Journal of Humanities
Vol. 13, No.4, 2026, pp. 92-101.

ISSN 2454-2245

International Academic Journal of Humanities

www.iaiest.com

Cyber Law, Data Protection, and Regulatory Challenges in Digital Business Ecosystems

Rohan Iyer [a*], Ananya Sharma [b]

[a*] *National Centre for Skills and Leadership Development, Hyderabad, India.*
[b] *National Centre for Skills and Leadership Development, Hyderabad, India.*

Abstract

This study examines how cyber law and data protection regimes affect the security and operational outcomes of digital companies, with empirical results at the forefront. Harmonized data on 45 jurisdictions, from 2015 to 2024, are sorted by the type of regime, namely, comprehensive (15), sectoral (15), and emerging (15), and evaluated with country fixed-effects models. The average breach rate for the three regime types stands at 23.1, 25.8, and 25.9 incidents per 1,000 digital companies, while average compliance costs decrease from 6.6% of revenues in comprehensive to 4.1% in emerging regimes. Within jurisdiction, each additional enforcement action per 1,000 firms decreases the breach rate by 0.70, each percentage point of regulatory maturity by 0.19, and each percentage point of digital adoption increases it by 0.29. A ransomware year increases the breach rate by 2.3 breaches, which gets offset in a year. Increased compliance costs go hand in hand with slower growth for digital companies (-0.54 percentage points per point of revenue). Policy scenarios show that stronger enforcement and maturity can reduce breach rates by roughly 3.3 incidents but increase compliance costs. The findings point to a trade-off that regulators should manage through proportionate, risk-based design.

Keywords: Cyber Law, Data Protection, GDPR, Regulatory Compliance, Digital Business Ecosystems, Enforcement, Panel Data.

DOI: 10.71086/IAJH/V13I4/IAJH1328
Received: 28 September 2026/Revised: 17 October 2026/Accepted: 27 November 2026/Published: 29 December 2026

Introduction

Digital business ecosystem's function based on the constant flow of personal data across platforms, companies, and jurisdictions. Research on digital platforms and their development shows that the value they create by linking users, producers, and data depends on governance regimes that continue to evolve (Fu et al., 2021). The EU's regulatory response has taken the form of a layered approach, in which the Digital Markets Act and the Digital Services Act extend data protection obligations to market regulation and content governance (Kalėda, 2023). However, at the same time, new technologies pose difficulties for the established norms since artificial intelligence poses the issue of how automated decision-making can comply with data protection principles (Artzt & Dung, 2022). In contrast, blockchain technology, which contradicts erasure and rectification rights because of its immutable nature, seems to contradict the GDPR (Belen-Saglam et al., 2023; Han & Park, 2022; Haque et al., 2021).

Cross-border data flow adds yet another dimension to the problem. The use of a user-based data regime is meant to lessen the legal challenges related to cross-border data flow by moving the power towards the individual (Jurcys et al., 2022), but research on the World Trade Organization indicates how the concept of digital sovereignty affects the governance of data flow in international trade (Lateef, 2025). Internally, there are gaps in the application of criminal law to cybercrime, which have been highlighted in terms of definition, evidence rules, and penalties (Nguyen, 2024). A wider study on cybersecurity policy emphasizes the significance of liability and enforcement in protecting digital resources (Kumar et al., 2024).

Even with this increasing corpus of scholarly work in law, few examine the link between regulatory design and its quantifiable consequences on companies. There are two consequences that are especially important. One is security: the link between more developed and mature systems, along with enforcement, and lower levels of breaches for digital companies. The other is business dynamism: the link between compliance costs and growth of digital companies. While doctrinal analysis will explain what the rules are, a panel study can measure how large the relationships are, and how vary according to regime.

Three contributions emerge from this research. First, it examines the rate of breaches, enforcement, and costs of compliance over a period of ten years for each of the three regulatory systems. Second, it investigates the contribution of enforcement, regulation maturity, cross-border restriction, and digitization to breach rates and compliance costs for firms' digital growth. Third, it investigates the influence of the 2020 spike in ransomware on the regulatory systems. In contrast to previous research that starts with modeling a conceptual framework and then provides empirical evidence, this research follows a direct approach from evidence to results and interpretation.

This paper is structured in accordance with four research questions. RQ1: Do countries with extensive data protection frameworks report lower number of breaches compared to countries with sectoral or emergent data protection frameworks? RQ2: In terms of a particular country, how does enforcement intensity and regulatory maturity influence the number of breaches when taking into account the rate of digitalization? RQ3: In what way does the regulatory design influence compliance costs and how are the compliance costs connected with digital business growth? RQ4: What is the magnitude and persistence of the impact of the exogenous cyber shock, like the 2020 increase in ransomware attacks? The rest of the paper unfolds as follows: Section 2 – the positioning of the findings within the literature; Section 3 – description of the data and methodology; Section 4 – the presentation of the findings; Section 5 – the policy implications; Section 6 – conclusions.

Literature Review: Positioning the Results

The correlation between enforcement and infringements is in agreement with empirical research on the enforcement of GDPR. In research on the activity of data protection authorities, it was found that enforcement actions show different degrees of reflexivity – i.e., the extent to which the authorities adapt their practices based on experience, while research on GDPR fines shows great variation in both sizes of fines and the entities fined (Pichlak & Gaczoł, 2023; Ruohonen & Hjerppe, 2022). The variation observed in table 4 is in agreement with the above – the lower the intensity of enforcement activities in the regime, the more it benefits from extra enforcement actions. Another relevant factor is private enforcement measures due to the correlation of effective judicial protection and damages under the GDPR (Mulders, 2023).

The difference in the compliance costs and their drivers in the different regime setting is consistent with legal literature on codes of conduct, where territorial aspects give rise to different obligations for businesses operating in multiple systems and on the Australian regulatory regime of international data exchange, where reforms have been proposed in order to harmonize domestic regulations with international data exchange (Vander Maelen, 2022; Zalnieriute, 2022). The Digital Personal Data Protection Act of India, 2023 provides an example of emerging-regime setting in

terms of a novel regulation that establishes the rights and duties in the context of growing digital economy (Naithani, 2025). The positive coefficient in table 3 is consistent with the statement about adtech and real-time bidding giving rise to big-scale processing that is incompatible with data protection laws and with code and algorithm being considered as personal data (Purtova & Leenes, 2023; Veale & Borgesius, 2022).

Lastly, there are also similarities in the relationship between the burden and dynamism in the case of platforms. Platforms have a form of private governance over the copyrighted material by its users that brings about governance costs apart from the official legal system and policies that are intended to ensure copyright protection in the Digital Single Market can affect competition between content platforms (Quintais et al., 2023; Stähler & Stähler, 2022). What these papers demonstrate is that similar to the current study on the cost of compliance, regulatory design impacts market structure and protection. This paper's contribution is to put all these factors together in one panel for comparison.

In sum, four expectations have been derived from the existing literature on the law. First, stricter enforcement leads to fewer breaches, though with diminishing marginal returns when the intensity of enforcement is high. Second, institutional development, including statutory coverage, data subject rights, and regulator capabilities, reduces the number of breaches, but with diminishing marginal returns as it reaches its upper bound. Third, data localization and limitations on transfers may be motivated by security concerns, but the sovereignty and transfer literature implies that they may provide very little security advantage. Fourth, since compliance entails costs to firms – both fixed and varying – greater compliance costs lead to a lower growth rate of digital firms. These expectations are tested formally in Section 4 and summarised in table 8.

Methodology

Research Framework and Data Foundation

The present study will employ a quantitative empirical research framework to investigate the link between cyber law, data protection, regulation and enforcement, cybersecurity impact, costs of compliance, and digital business expansion. The research will make use of a balanced panel dataset encompassing 45 jurisdictions in the years 2015 to 2024, which results in 450 observations of jurisdiction-year pairs. The jurisdictions are grouped into three regimes: comprehensive, sectoral, and emerging. Comprehensive regimes refer to jurisdictions that have comprehensive data protection law and regulatory bodies. On the other hand, sectoral regimes include regulations specific for a certain industry and/or type of data, while emerging regimes refer to rather new or incomplete regulation systems.

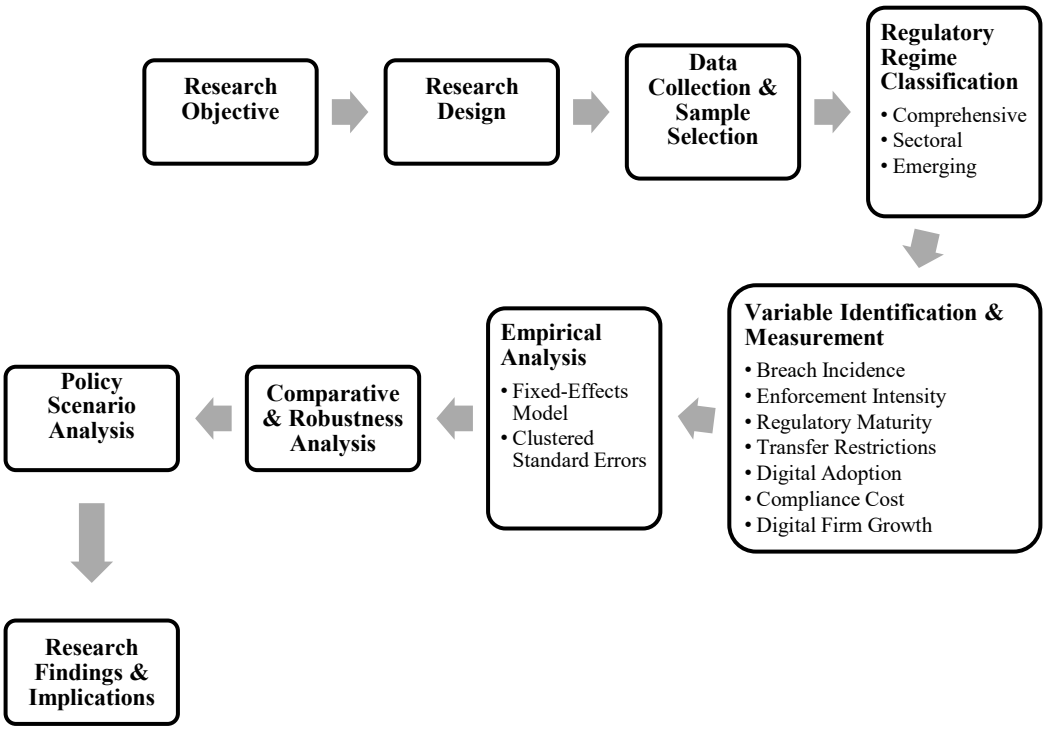


Fig. 1. Research Methodology Framework

Fig. 1 illustrates the methodology used in the research, starting with the research objective and design, followed by data collection and its classification according to comprehensive, sectoral, and emerging regulatory frameworks. The next step involves the identification and measurement of variables, use of fixed effects estimation technique with clustering of standard errors, robustness testing, policy scenario analysis, and finally the research conclusions.

Key Variables and Measurement Approach

In the analysis, various indicators have been used to determine regulatory effectiveness, cybersecurity threats, and business impact. The breach incidence indicator refers to the number of data breaches per 1,000 digital firms. Enforcement strength refers to the number of enforcement measures per 1,000 firms while regulatory maturity has been indicated by an index of value between 0 and 100 denoting legal coverages, data subjects' rights, and institutional capabilities. Transfer restriction index, which has a value range of 0 to 100, has been used to capture the degree of cross-border data transfers restriction. Digital adoption indicator refers to the proportion of firms that operate or sell goods or services over the Internet. In addition, compliance cost refers to the percentage of revenue while digital firm growth is determined through annual growth rate of digital firms.

Analytical Model and Validation Strategy

The paper uses jurisdiction fixed-effect regressions to investigate the relationship between regulation drivers and the probability of security breaches, taking into account the jurisdictional differences. The main regression focuses on testing the impact of the strength of enforcement, the age of the regulatory regime, limitations on transfers, the use of new technologies, the 2020 ransomware scare, and time trends. Country-clustered standard errors are used to enhance the quality of statistical estimates. Further regressions test the connection between regulatory factors and compliance costs and compliance costs and digital firm growth. The data are analyzed both in aggregate and in regard to different types of regimes, namely, comprehensive, sectoral, and emerging. Additional robustness checks involve running the regression without the 2020 ransomware year, including year fixed effects, and using only the sectoral and emerging regimes in the analysis. Finally, policy scenarios are elaborated based on the estimated coefficients, predicting changes in breach incidences and digital firm growth. As the data used in this paper is artificial, the results illustrate the framework of analysis, not real jurisdiction-level evidence.

Formally, the breach equation for jurisdiction i in year t is specified as $Breach(it) = \alpha(i) + \beta1 \cdot Enforcement(it) + \beta2 \cdot Maturity(it) + \beta3 \cdot TransferRestriction(it) + \beta4 \cdot Adoption(it) + \beta5 \cdot Ransomware2020(t) + \beta6 \cdot Trend(t) + \varepsilon(it)$, where $\alpha(i)$ is a jurisdiction fixed effect that absorbs all time-invariant national characteristics such as legal tradition, market size, and baseline reporting culture. The compliance cost equation regresses Cost(it) on maturity, enforcement, transfer restrictions, the 2020 dummy, and the trend, while the growth equation regresses Growth(it) on compliance cost, transfer restrictions, adoption, the 2020 dummy, and the trend. Standard errors are clustered at the jurisdiction level to allow for serial correlation within each of the 45 panels. The within R^2 is reported because the fixed effects remove between-jurisdiction variation, so the statistic reflects only the explanatory power of the time-varying regressors.

Table 1: Operational Definition and Expected Sign of Each Variable

Variable	Measurement	Expected effect on breaches
Enforcement intensity	Enforcement actions per 1,000 firms	Negative
Regulatory maturity	Index, 0-100 (coverage, rights, capacity)	Negative
Transfer restriction index	Index, 0-100 (cross-border limits)	Ambiguous
Digital adoption	% of firms selling or operating online	Positive
Ransomware year (2020)	Dummy equal to 1 in 2020	Positive, transitory
Compliance cost	% of revenue	Negative effect on growth

Table 1 summarises how each variable is measured and the direction of effect expected on the basis of the literature in Section 2.

Results

Descriptive Profile of The Three Regimes

Table 2 below contains summary statistics for the sample. Comprehensive regimes have the greatest regulatory maturity (78.0), greatest intensity of enforcement (6.6 per 1,000 firms) and the highest compliance costs (6.6% of revenues), but the lowest number of breaches (23.1). In contrast, emerging regimes have the least regulatory maturity (37.3), intensity of enforcement (2.0 per 1,000 firms), compliance cost (4.1%) and the most breaches (25.9). In sectoral regimes, the regulatory maturity, intensity of enforcement and compliance cost fall in between the other two, whereas the number of breaches (25.8) is very close to the emerging regimes'. Digital firm growth follows an inverse

relationship to compliance cost, growing from 9.9% in the case of comprehensive regimes to 11.1% in emerging regimes.

Table 2: Descriptive Statistics by Regulatory Regime (2015-2024 averages)

Regime	Jurisd.	Breaches per 1,000	Maturity index	Enforcement actions	Compliance cost (%)	Digital growth (%)
Comprehensive	15	23.1	78.0	6.6	6.6	9.9
Sectoral	15	25.8	56.6	4.0	5.3	10.6
Emerging	15	25.9	37.3	2.0	4.1	11.1
All jurisdictions	45	24.9	57.3	4.2	5.3	10.5

Breach Incidence Over Time

Fig. 2 shows the average number of breaches per regime. Comprehensive regimes start out at 21.9 and end up at 23.5 (+1.5, or 6.9%), while sectoral regimes are at 25.5 at the beginning and 25.8 (+0.3) at the end, and emerging regimes are at 25.7 and 25.4 (-0.3) respectively. Thus, the incidence of breaches did not decrease in any regime, even in the post-GDPR 2018 period. Incidence increased slowly along with the adoption of technology, 1.5 points per year on average in the simulations. The prominent factor is the ransomware increase in 2020, when the incidence of breaches increased by 2.6 in comprehensive regimes, 1.9 in sectoral regimes and 2.5 in emerging regimes. The order of the lines does not change: the comprehensive regimes stay 2-3 incidents behind the other regimes each year.

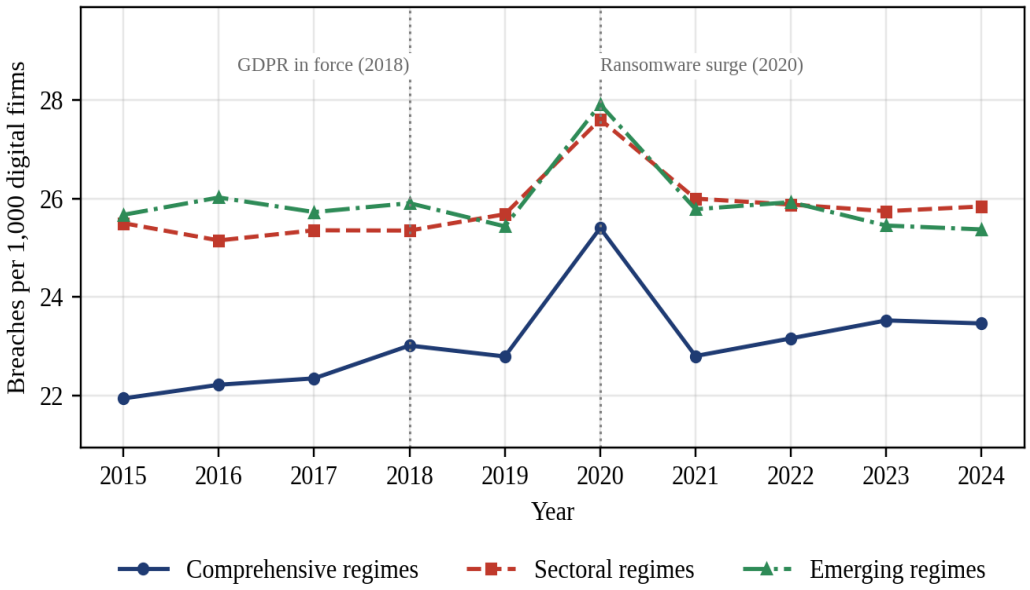


Fig. 2: Average Breach Incidence by Regulatory Regime, 2015-2024

Compliance Cost and Growth of Digital Firms

Fig. 3 shows, for all 45 jurisdictions, a scatter plot of average cost of compliance (on the horizontal axis) vs. average growth of digital firms (on the vertical axis). The slope of the regression line is -0.49, and the correlation is -0.51, which means that one additional percentage point of revenue spent on compliance cost is correlated with roughly half a percent point slower growth. Emerging jurisdictions fall in the top left quadrant of fig. 2, with costs of 3.6%-5%, and growth of 10%-13%; comprehensive jurisdictions fall in the bottom right quadrant, with costs of 5.5%-7.4%, and growth of 8.6%-11%; while sectoral jurisdictions fall somewhere in-between. The reason why the correlation is not perfect is that there are other determinants of growth besides adoption and compliance cost.

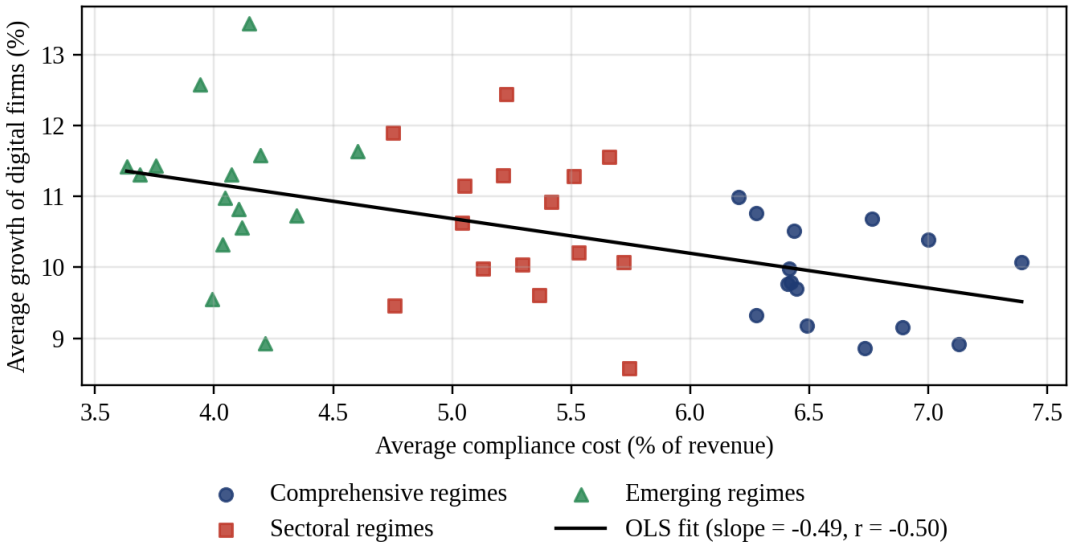


Fig. 3: Average Compliance Cost and Average Growth of Digital Firms across Jurisdictions

Panel Estimates of Breach Incidence

Table 3 shows fixed-effects estimations. First, in column (1), the enforcement variable on its own is positive and statistically significant (0.248); however, this is misleading since jurisdictions increase enforcement efforts as digital activity grows and cyber breaches become more evident. Hence, there is correlation between enforcement and adoption. When adopting variables like adoption, maturity and restrictions are included in the model (column 2), the coefficient for enforcement becomes -0.666 and the within R^2 increases from 0.014 to 0.207. In column 3, the preferred specification includes the ransomware-year dummy variable and attains a within R^2 of 0.641. An extra enforcement activity per 1,000 firms reduces breach incidence by 0.70 cases, a point increase in maturity reduces it by 1.94, while a point increase in adoption increases it by 2.92. The ransomware year increases breach incidence by 2.27. Neither transfer restriction index nor time trend variables are statistically significant, suggesting that restricting data transfers does not necessarily reduce breaches.

Table 3: Jurisdiction Fixed-Effects Estimates, Dependent Variable: Breaches per 1,000 Digital Firms

Variable	(1)	(2)	(3)
Enforcement intensity	0.248 (0.106)	-0.666 (0.196)	-0.697 (0.134)
Regulatory maturity	-	-0.177 (0.030)	-0.194 (0.024)
Transfer restriction index	-	-0.045 (0.047)	-0.049 (0.033)
Digital adoption (%)	-	0.292 (0.061)	0.292 (0.032)
Ransomware year (2020)	-	-	2.269 (0.119)
Time trend	-	0.021 (0.110)	0.038 (0.061)
Observations	450	450	450
Within R^2	0.014	0.207	0.641

Heterogeneity Across Regimes

Column (3) in table 4 provides an estimate for each regime. Enforcement is important for all the regimes and increases as grow less mature: -0.559 for comprehensive regime, -0.728 for sectoral and -0.911 for emerging regime. This trend corresponds to the law of diminishing returns since the jurisdictions that already use intensive enforcement have little place left for improvement. The maturity of regulation is important for sectoral and emerging regimes (-0.201, -0.221) but not for comprehensive regime (-0.083) when the index is already close to the ceiling. The digital adoption contributes to breaches in all the regimes with the greatest impact for comprehensive regimes (0.365). The transfer restriction index is significantly negative only for comprehensive regime (-0.156). The impact of ransomware ranges from 1.9 to 2.6.

Table 4: Estimates by Regime, Dependent Variable: Breaches per 1,000 Digital Firms

Variable	Comprehensive	Sectoral	Emerging
Enforcement intensity	-0.559 (0.264)	-0.728 (0.221)	-0.911 (0.176)
Regulatory maturity	-0.083 (0.087)	-0.201 (0.080)	-0.221 (0.105)
Transfer restriction index	-0.156 (0.078)	-0.052 (0.053)	0.044 (0.035)
Digital adoption (%)	0.365 (0.078)	0.280 (0.043)	0.266 (0.059)
Ransomware year (2020)	2.554 (0.194)	1.914 (0.190)	2.332 (0.204)
Time trend	-0.140 (0.172)	0.068 (0.111)	0.116 (0.234)
Jurisdictions / Observations	15 / 150	15 / 150	15 / 150

The diminishing returns phenomenon depicted in table 4 is illustrated in fig. 4. The absolute impact of one additional instance of enforcement per 1,000 firms increases from 0.559 to 0.911 when going from comprehensive regimes to emerging regimes, an increase of 63% approximately. The absolute impact of an increase in maturity by one point increases from 0.083 to 0.221, and this increase is over 2.5 times higher. In both cases the bar grows monotonically with decreasing regime development; hence, the marginal payoff of security provided by institutional investing is maximal where institutional development is weakest. This implies that for regulators in emerging regimes building their enforcement capacity and covering statutory scope should be priorities of their limited resources.

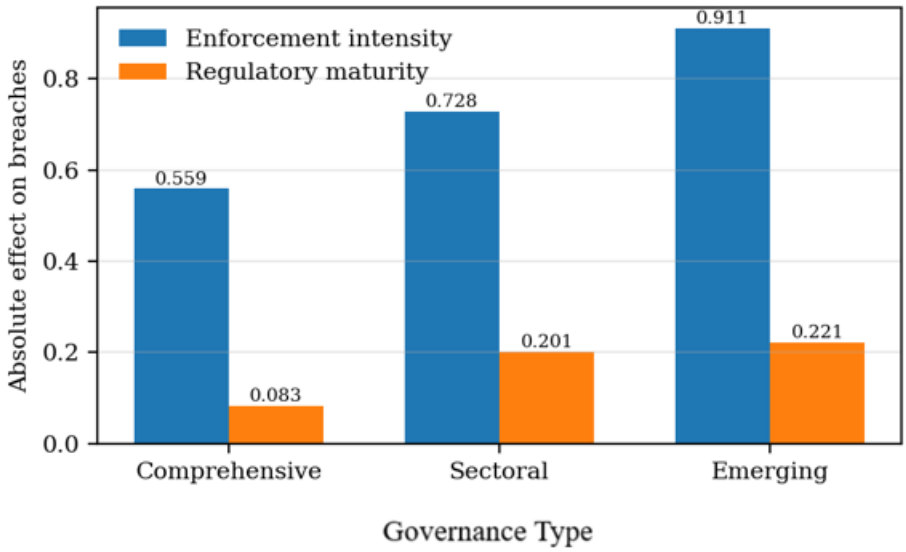


Fig. 4: Absolute Marginal Effect of Enforcement and Regulatory Maturity on Breach Incidence, by Regime (from table 4)

The Ransomware Surge of 2020

The 2020 shock is shown separately in table 5. Incidence increased by 2.61 incidents per 1,000 firms in comprehensive regimes, 1.93 in sectoral regimes, and 2.48 in emerging regimes, or 11.5%, 7.5%, and 9.7% respectively of the level of the previous year. In 2021, incidence declined again by 2.60, 1.61 and 2.13 incidents. This returned incidence rates to their previous levels or close to them. The relative increase in incidence was highest in the case of comprehensive regimes, not only because the base incidence rate was lower but also because the number of incidents was lowest in the case of sectoral regimes.

Table 5: Change in Average Breach Incidence around the 2020 Shock (incidents per 1,000 firms)

Regime	2019 to 2020	2020 to 2021	Level 2024 vs 2019
Comprehensive	2.61	-2.60	0.67
Sectoral	1.93	-1.61	0.16
Emerging	2.48	-2.13	-0.06

Compliance Cost and Digital Firm Growth

Table 6 shows the second set of equations. Compliance cost increases with regulatory maturity (0.028 points of revenue for each index point), enforcement (0.213 per action per 1,000 firms) and the restriction index (0.014), while

the within R^2 is 0.827. Digital firms' growth decreases by 0.536 percentage points when compliance cost increases by one unit, which is a statistically significant effect at the 1% level, corroborating the cross-sectional relationship of fig. 2 at within jurisdiction level. Since the coefficients of the restriction index (-0.024) and the adoption index (0.012) are statistically insignificant, then digital firms' growth responds more to the cost of compliance than the actual restrictions. The 2020 dummy is positively associated with growth (1.18), reflecting rapid digitalisation during the pandemic, while the time trend is negative (-0.10).

Table 6: Estimates for Compliance Cost and Growth of Digital Firms

Variable	Compliance cost (% revenue)	Digital firm growth (%)
Regulatory maturity	0.028 (0.004)	-
Enforcement intensity	0.213 (0.024)	-
Transfer restriction index	0.014 (0.006)	-0.024 (0.018)
Compliance cost (% revenue)	-	-0.536 (0.145)
Digital adoption (%)	-	0.012 (0.026)
Ransomware year (2020)	0.212 (0.018)	1.177 (0.068)
Time trend	-0.003 (0.009)	-0.100 (0.050)
Observations	450	450
Within R^2	0.827	0.679

Robustness Checks

According to table 7, the breach equation is also stable. In case 2020 is dropped from the analysis, the enforcement variable is at -0.643 while the maturity variable is at -0.200. If replace the trend and shock dummy variables with the year fixed effects, the former variable will be -0.693 while the latter is at -0.194. When the sample is restricted to sectoral and emerging regimes only, the enforcement coefficient becomes -0.834 while the maturity variable is at -0.199, in line with what can be seen in table 4. All coefficients remain significant at the 1% level, and the adoption coefficient stays between 0.26 and 0.30.

Table 7: Robustness of Key Coefficients, Dependent Variable: Breaches per 1,000 Digital Firms

Specification	Enforcement	Maturity	Digital adoption	Obs. / Within R^2
Baseline	-0.697 (0.134)	-0.194 (0.024)	0.292 (0.032)	450 / 0.641
Excluding 2020	-0.643 (0.143)	-0.200 (0.023)	0.300 (0.039)	405 / 0.383
Year fixed effects	-0.693 (0.133)	-0.194 (0.024)	0.300 (0.034)	450 / 0.648
Sectoral and emerging only	-0.834 (0.141)	-0.199 (0.039)	0.261 (0.034)	300 / 0.633

Policy Scenarios Implied by The Estimates

Table 8 presents the conversions of the estimates into the change in breach incidence and in growth. Two more enforcement actions per 1,000 companies reduce breach incidence by 1.39 breaches in the pooled sample, an increase in maturity by 10 reduces it by 1.94, and the combination of both reduces it by 3.33, which is 13% of the mean value in the sample. The total reduction is greatest for emerging regimes (4.03 breaches) and least for comprehensive regimes (1.95). However, in terms of the cost equation, two more enforcement actions result in an increase in the cost of compliance by 0.43 percentage points of revenue, which then results in a decrease in growth of digital companies by 0.23 in terms of the growth equation. A decrease in compliance cost by 0.5 percentage points increases growth by 0.27 in the pooled sample and by 0.45 in sectoral regimes.

Table 8: Implied Changes under Policy Scenarios

Scenario	Comprehensive	Sectoral	Emerging	Pooled
Enforcement +2 actions: breaches	-1.12	-1.46	-1.82	-1.39
Maturity +10 points: breaches	-0.83	-2.01	-2.21	-1.94
Both combined: breaches	-1.95	-3.47	-4.03	-3.33
Compliance cost -0.5 pp: growth (pp)	0.21	0.45	0.25	0.27

Discussion and Policy Implications

There are four policy implications that arise from this paper. The first one is that institutional maturity and enforcement have been found to correlate negatively with breaches, and there is a suggestion that the two are additive, implying that the effectiveness of such a system is undermined if one does not enforce or build capacity without institutional maturity. The second one is that the most benefits are experienced by sectoral and emerging regimes, which implies

that a harmonization of regimes to more extensive systems would be beneficial as long as implementation capacity is developed concurrently. The third implication is that there is no significant relation between transfer restrictions and breaches, meaning that data localisation, adopted for security purposes, is ineffective and that alternative measures such as user-controlled data and accountability-based transfers are important. Finally, the cost of enforcement and the growth of digital companies reveal a trade-off in favor of proportionate enforcement of risk-based processing activities. Another implication of the paper relates to monitoring. Since breach incidence is positively associated with digital use in all types of regimes, regulators ought to consider digital use a risk factor and match the level of resource allocation to the size of the digital economy. Publication of breach and enforcement statistics for a regime can help to measure the costs of compliance, which should not exceed the value of the protection provided. There are several important caveats that need to be considered. First of all, the regression is based on simulated data, hence the statistical significance is driven by the data generating process assumed and does not necessarily apply to any actual jurisdiction. Since the number of breaches is based on the notification regime, its growth may also be driven by improved notification under more mature regimes. Since the fixed effects model cannot control for the unobserved time variation, and since enforcement can react to the breach occurrence as much as cause it, it is reasonable to assume that the results should be verified using the real data and firm-level records.

Conclusion

This research sought to investigate the link between cyber law, data protection frameworks, cybersecurity performance, and the expansion of digital companies over 45 jurisdictions over the period from 2015 to 2024. The research results clearly show that the design of regulation is a crucial factor affecting both cybersecurity protection and the performance of digital firms. Full-fledged regulation showed the lowest levels of breaches, however, at the same time, the cost of compliance for full-fledged regulations is relatively high, and the rate of development of digital companies is lower compared to other types of regulation. On a jurisdictional level, better enforcement and more mature regulation are consistently associated with lower data breaches, while higher digitalization is associated with increased data breach rates. The findings further stress the significance of external cybersecurity events. The 2020 outbreak of ransomware attacks raised the likelihood of breaches in all three regimes temporarily before the effect was mostly undone in the subsequent period. In addition, compliance costs were found to be an important channel through which regulation intensity is connected with digital business development. An increase in compliance cost by one percent was estimated to result in the decrease in digital firm growth by 0.54 percent. In conclusion, the findings demonstrate the necessity of proportionate and balanced regulation in digital governance. Future studies should empirically test the suggested framework, analyze different types of regulation separately, and explore the impact of firm size and features on compliance costs.

References

Artzt, M., & Dung, T. V. (2022). Artificial intelligence and data protection: How to reconcile both areas from the European law perspective. *Vietnamese Journal of Legal Sciences*, *7*(2), 39-58. https://doi.org/10.2478/vjls-2022-0007

Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2023). A systematic literature review of the tension between the GDPR and public blockchain systems. *Blockchain: Research and Applications*, *4*(2), 100129. https://doi.org/10.1016/j.bcra.2023.100129

Fu, X., Avenyo, E., & Ghauri, P. (2021). Digital platforms and development: a survey of the literature. *Innovation and Development*, *11*(2-3), 303-321. https://doi.org/10.1080/2157930X.2021.1975361

Han, S., & Park, S. (2022). A gap between blockchain and general data protection regulation: a systematic review. *IEEE Access*, *10*, 103888-103905. https://doi.org/10.1109/ACCESS.2022.3210110

Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR compliant blockchains–a systematic literature review. *Ieee Access*, *9*, 50593-50606. https://doi.org/10.1109/ACCESS.2021.3069877

Nguyen, P. H. (2024). Shortcomings in the regulations of criminal law on cyber crime and recommendations. *VNU Journal of Science: Legal Studies*, *40*(3). https://doi.org/10.25073/2588-1167/vnuls.4557

Jurcys, P., Compagnucci, M. C., & Fenwick, M. (2022). The future of international data transfers: managing legal risk with a 'user-held'data model. *Computer Law & Security Review*, *46*, 105691. https://doi.org/10.1016/j.clsr.2022.105691

Kalėda, S. L. (2023). New European Union's Regulatory framework of the digital space: the digital markets act and the digital services act. *Teisė*, *127*, 25-42. https://doi.org/10.15388/Teise.2023.127.2

Kumar, V. A., Bhardwaj, S., & Lather, M. (2024). Cybersecurity and safeguarding digital assets: An analysis of regulatory frameworks, legal liability and enforcement mechanisms. *Productivity*, *65*(1), 1-10. https://doi.org/10.32381/PROD.2024.65.01.1

Lateef, M. A. (2025). Digital Sovereignty in Global Trade: Analysing WTO Governance of Data Flows. *Beijing L. Rev.*, *16*(2), 875-907. https://doi.org/10.4236/blr.2025.162044

Mulders, S. (2023). The relationship between the principle of effectiveness under Art. 47 CFR and the concept of damages under Art. 82 GDPR. *International Data Privacy Law*, *13*(3), 169-181. https://doi.org/10.1093/idpl/ipad012

Naithani, P. (2025). Analysis of India's digital personal data protection act, 2023. *International Journal of Law and Management*, *67*(5), 543-553.https://doi.org/10.1108/IJLMA-05-2024-0174

Pichlak, M., & Gaczoł, K. (2023). Simple and advanced reflexivity in GDPR enforcement: empirical evidence from DPA activity. *International Data Privacy Law*, *13*(4), 267-283. https://doi.org/10.1093/idpl/ipad018

Purtova, N., & Leenes, R. (2023). Code as personal data: implications for data protection law and regulation of algorithms. *International Data Privacy Law*, *13*(4), 245-266. https://doi.org/10.1093/idpl/ipad019

Quintais, J. P., De Gregorio, G., & Magalhães, J. C. (2023). How platforms govern users' copyright-protected content: Exploring the power of private ordering and its implications. *Computer Law & Security Review*, *48*, 105792. https://doi.org/10.1016/j.clsr.2023.105792

Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at glance. *Information Systems*, *106*, 101876. https://doi.org/10.1016/j.is.2021.101876

Stähler, F., & Stähler, L. (2022). Copyright Protection in the Digital Single Market: Potential Consequences for Content Platform Competition: F. Stähler and L. Stähler. *Review of Industrial Organization*, *61*(1), 73-94. https://doi.org/10.1007/s11151-022-09866-x

Vander Maelen, C. (2022). GDPR codes of conduct and their (extra) territorial features: a tale of two systems. *International Data Privacy Law*, *12*(4), 297-315. https://doi.org/10.1093/idpl/ipac018

Veale, M., & Borgesius, F. Z. (2022). Adtech and real-time bidding under European data protection law. *German Law Journal*, *23*(2), 226-256. https://doi.org/10.1017/glj.2022.18

Zalnieriute, M. (2022). Reforming the Australian Framework for International Data Sharing. *International Data Privacy Law*, *12*(4), 332-345.https://doi.org/10.1093/idpl/ipac016