Environment and Water Engineering

Homepage: www.jewe.ir

ISSN: 2476-3683

Cybersecurity for environmental data integrity: legal perspectives on safeguarding water and soil management system

Raed Hameed Salih[1], Abdulsatar Shaker Salman[2], Shamel Abdul-Sattar Jaleel Shalaan[3], Haider Mahmood Jawad[4], Ali Alsaray[5], Alan Amini[6], and Raoof Mostafazadeh[7]✉

[1]Al-Turath University, Baghdad 10013, Iraq
[2]Al-Mansour University College, Baghdad 10067, Iraq
[3]Al-Mamoon University College, Baghdad 10012, Iraq
[4]Al-Rafidain University College, Baghdad 10064, Iraq
[5]Madenat Alelem University College, Baghdad 10006, Iraq
[6]Faculty of Engineering, Bu Ali University, Hamedan, Iran
[7]Department of Natural Resources and member of Water Management Research Center, Faculty of Agriculture and Natural Resources, University of Mohaghegh Ardabili, Ardabil, Iran

ARTICLE INFO

Paper Type: Research Paper

Received: 19 August 2025
Revised: 27 August 2025
Accepted: 29 August 2025
Published: 29 August 2025

Keywords
Data Breaches
Environmental Data
Legal Frameworks
Regulatory Standards
Sustainability

Corresponding author:
R. Mostafazadeh
✉
raoofmostafazadeh@uma.ac.ir

ABSTRACT

The increasing reliance on digital infrastructure for managing environmental data requires a greater focus on cybersecurity threats. This study aims to evaluate the effectiveness of current cybersecurity laws in protecting environmental data, identify significant regulatory gaps, and propose strategic actions for enhancing and harmonizing legal frameworks. These goals were achieved using a mixed-methods approach, including quantitative analysis of 100 documented cyber incidents across various sectors, qualitative interviews with policymakers and experts, and comparative analysis of legal frameworks such as the General Data Protection Regulation (GDPR), Network and Information Systems (NIS) Directive, and United Nations Framework Convention on Climate Change (UNFCCC) guidelines. Mathematical modeling (from intermediate to advanced levels) was also used to estimate how regulatory strength influences the likelihood of data breaches and sustainability under multiple scenarios of uncertainty. Results show that strong regulatory frameworks can reduce the likelihood of a breach by 40% and mitigate sustainability impacts by 85%, while weak regulatory environments increase breach rates and compromise data integrity. Effective enforcement, adaptability, and global cybersecurity standards are crucial, with higher compliance costs associated with greater reductions in financial losses, ensuring dependable environmental information for worldwide sustainability.

Highlights

- GDPR cuts breaches by 40% and boosts environmental data reliability.
- Strong laws lower data vulnerability by 45–85% across sectors.
- Cybersecurity lifts biodiversity integrity 41% and strengthens climate monitoring.

Citing:
Hameed Salih, R., Shaker Salman, A., Abdul-Sattar Jaleel Shalaan, S., Mahmood Jawad, H., Alsaray, A., Amini, A., & Mostafazadeh, R. (2025). Cybersecurity for environmental data integrity: legal perspectives on safeguarding water and soil management system. *Environment and Water Engineering*, *11*(4), 509-518. https://doi.org/10.22034/ewe.2025.516307.2016

1. Introduction

The significance of environmental data encompassing critical information on climate change, pollution levels, biodiversity, conservation efforts, and other related areas has proven to be essential for effective global environmental governance (Gharibreza et al., 2018; Amini et al., 2017). Environmental datasets play a vital role in shaping policy decisions, driving regulatory frameworks, and promoting sustainable development practices. However, as the scale and sensitivity of this data expand, so do the risks associated with cyber threats and cyber-attack vulnerabilities. Data breaches, unauthorized access, hacking, and cyberattacks targeting environmental information systems present substantial dangers, including the compromise of data integrity, erosion of public trust, jeopardization of scientific credibility, and the hindrance of effective decision-making processes (Troshchenkov & Halona, 2024; Dunaj, 2023). Consequently, safeguarding environmental data requires the implementation of advanced security measures, robust legislation, and international cooperation to address the unique challenges faced by this field.

Academic research on cybersecurity and data protection provides valuable insights into the intersection of technology, legislation, and environmental governance. Similarly, Cassotta and Sidortsov (2019) highlight the importance of tailored cybersecurity protocols to safeguard critical infrastructure, including energy systems, which are directly applicable to environmental data repositories. In this context, Verhelst and Wouters (2020) draw attention to existing governance gaps at the international level, advocating for the development of harmonized legal standards across jurisdictions to ensure consistent and effective protection of environmental data. Such gaps are further illustrated by Dunaj (2023), who explores the emergence of privacy and cybersecurity standards within the European Union. Dunaj's approach underscores how regulatory frameworks, such as the General Data Protection Regulation GDPR, could be adapted and transitioned to environmental data management with minimal resistance, thereby laying a foundation for aligning legal approaches globally. Morales-Sáenz et al. (2024) emphasize that incorporating cybersecurity measures into sustainable business practices is necessary to protect environmental data from malicious actors and cyber threats.

Nasir et al. (2024) reviewed ethical aspects of cybersecurity in Lahore, Pakistan, focusing on privacy, data integrity, accountability, and ethical hacking. They concluded that ethical guidelines and best practices are vital for responsible information security and user trust. Nadji (2024) examined data security, integrity, and protection in the context of smart cities. The chapter aimed to reassess the conventional hierarchy between data and information by treating them as synonymous. The main finding emphasized that this simplified approach offers a clearer framework for addressing security and trust in digital systems.

These studies underscore the pressing need for harmonizing cybersecurity initiatives with overarching goals of environmental sustainability and protection. The General Data Protection Regulation (GDPR) of the European Union is one of the most comprehensive legal frameworks for data privacy and security, emphasizing transparency, informed consent, and organizational accountability, which are equally relevant for safeguarding environmental data. The Network and Information Systems (NIS) Directive complements the GDPR by focusing on the resilience of critical digital infrastructures, risk management, and mandatory reporting of cyber incidents. Alongside these, the United Nations Framework Convention on Climate Change (UNFCCC) guidelines, while primarily environmental in nature, underline the importance of integrity, accessibility, and transparency of environmental data for international decision-making. Together, these frameworks provide a foundation for harmonizing global standards on cybersecurity in environmental data governance and strengthening digital resilience in sustainability efforts.

Varied national cybersecurity capacities lead to differing levels of environmental data security from one country to another, creating a fragmented global landscape. Layode et al. (2024) emphasize how the absence of a uniform legal framework complicates the effort to protect sensitive environmental information across borders. Additionally, international agreements such as the UN Framework Convention on Climate Change (UNFCCC) and other global accords have yet to incorporate comprehensive cybersecurity principles into their environmental governance strategies, despite their potential power to influence global standards (Markopoulou et al., 2019).

Building on recent literature, it underscores the urgent need for an integrated, cohesive approach. For instance, Sargsyan (2024) advocates for prioritizing cybersecurity from a bottom-up perspective, recognizing it as a critical component of sustainable development and environmental stewardship. Moreover, research such as the work by Mitchell and Mishra (2019) on international legal cooperation highlights the importance of cross-border collaboration and the factors that could influence the development of comprehensive global cyber legislation applicable to environmental data.

This work lies in the urgent need to address cybersecurity risks associated with the rapidly expanding digital infrastructure used for environmental data management. As environmental monitoring systems increasingly depend on real-time data acquisition, cloud-based storage, and AI-driven analytics, the integrity, availability, and confidentiality of environmental data become critical for effective decision-making and global sustainability efforts. Existing cybersecurity breaches not only compromise data accuracy but also pose severe risks to environmental governance, policy implementation, and public trust. This research is novel for its interdisciplinary integration of legal analysis, cybersecurity modeling, and environmental data governance. Unlike previous studies that focus narrowly on either data protection or environmental policy, this work bridges both fields through a comparative evaluation of international legal instruments such as the GDPR, Network and Information Systems (NIS) Directive, and UNFCCC guidelines, combined with empirical evidence from documented cyber incidents and expert insights. Furthermore, it introduces mathematical modeling to quantify the regulatory influence on breach probabilities and sustainability outcomes, offering a more comprehensive risk assessment framework for digital environmental governance.

Accordingly, the objectives of this study are to evaluate the effectiveness of current international cybersecurity legislation in safeguarding environmental data, identify regulatory gaps and operational vulnerabilities through a combination of quantitative incident analysis and expert interviews, and to propose both short-term and long-term strategic recommendations for enhancing legal and institutional responses. These contributions aim to support the development of resilient legal frameworks capable of protecting the integrity of environmental information systems in a digitally interconnected world.

2. Materials and Methods

This study adopts a multi-tiered approach that combines qualitative legal analysis with quantitative cyber risk modeling, compliance cost assessments, and sustainability impact evaluations. These factors guarantee a comprehensive approach to the study of both cybersecurity and the protection of environmental data, with an emphasis on the perspective of international law. Utilizing interdisciplinary techniques, the study reveals shortcomings of current regulatory frameworks, evaluates the efficacy of legal standards, and recommends the best possible cybersecurity measures to safeguard environmental data.

2.1 Data collection and analysis

In total, 60 structured interviews were conducted with cybersecurity policymakers, legal scholars, environmental data custodians, and industry experts. Participants were selected for their knowledge of cybersecurity regulations, data protection laws, and environmental governance. Each interview lasted for approximately 90 minutes and concentrated on legal discrepancies, compliance difficulties, and suggestions for harmonization. We used thematic analysis to code the interview transcripts, extracting insight into legal gaps and barriers to enforcement (Joshi & Li, 2016). Additionally, the study analyzed 100 legal documents, as shown in Fig. 1.

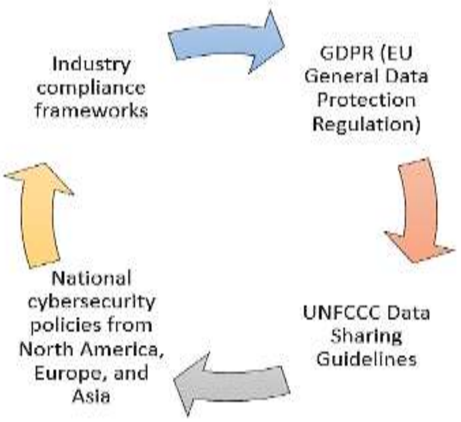

Industry compliance frameworks
GDPR (EU General Data Protection Regulation)
UNFCCC Data Sharing Guidelines
National cybersecurity policies from North America, Europe, and Asia

Fig. 1 Key Regulatory Frameworks in Cybersecurity for Environmental Data Protection

Using content analysis, these legal texts were coded for key regulatory themes, inconsistencies in legal language, and enforcement mechanisms (Butunbaev, 2020; Singh, 2024).

2.2 Quantitative data

To quantify cybersecurity risks in environmental data protection, the study analyzed 100 reported cyberattacks against environmental data systems. Data points included:

- Scope, for example, type of attack, such as ransomware, unauthorized access, data corruption;
- Sectorial impact such as energy, climate research, conservation, smart agriculture;
- Reactive legal enforcement in terms of response time and effectiveness;
- Economic losses and sanctions.

The data was crunched statistically to identify breach patterns, response effectiveness, and legal loopholes (Raghuvanshi, 2023; Troshchenkov & Halona, 2024).

To quantify cybersecurity risks in the context of environmental data protection, this study conducted a statistical analysis of 100 reported cyberattacks targeting environmental data systems across multiple sectors. The analysis focused on several key dimensions to evaluate the nature and consequences of these incidents. First, the scope of each attack was examined, with particular attention given to the type of cyber threat involved. Categories included ransomware attacks, unauthorized access, and deliberate data corruption. Each case was classified based on technical characteristics and severity, allowing for a comparative evaluation of threat prevalence and attack complexity. Second, the sectoral impact of each breach was assessed by identifying the specific environmental domain affected. The study categorized incidents by sector, including energy systems, climate research institutions, conservation databases, and smart agriculture platforms. This sector-based segmentation enabled the identification of which areas are most vulnerable and which require enhanced protection. Third, the study evaluated reactive legal enforcement by analyzing the speed and effectiveness of institutional responses following each incident. Variables included average response times, the presence or absence of formal protocols, and the extent to which enforcement measures were implemented. This helped in determining the role of regulatory readiness in mitigating cyber threats. Finally, the study recorded the economic losses and legal sanctions associated with each breach. This included quantifying financial damages, litigation outcomes, and the imposition of regulatory penalties where applicable. These figures were statistically processed to reveal patterns in economic impact and to identify any legal loopholes that allowed such attacks to escalate. Overall, the collected data were subjected to statistical techniques, including frequency analysis, cross-tabulations, and trend evaluations, to identify common breach patterns, assess response effectiveness, and uncover structural deficiencies in current legal frameworks (Raghuvanshi, 2023; Troshchenkov & Halona, 2024).

2.3 Mathematical and statistical modeling

To complement the qualitative findings, the study integrates mathematical models to quantify cybersecurity risks, regulatory effectiveness, compliance costs, and sustainability trade-offs. These models help evaluate the impact of policies and inform recommendations.

2.3.1 Cybersecurity Risk Assessment Model (CRAM)

To assess environmental data vulnerabilities, this study employed a multi-factor cyber risk probability model as Eq. 1 (Horlichenko, 2024):

$$R_{cyber} = \sum_{i-1}^{n}\left(\frac{W_i \cdot V_i \cdot T_i}{C_i}\right) + \alpha \sum_{j-1}^{m}\left(\frac{P_j \cdot L_j}{E_j}\right) \quad (1)$$

where R_{cyber} is cybersecurity risk score, W_i is weight of legal compliance factor i, V_i is vulnerability index, T_i threat level, C_i of security measure, P_j is probability of attack j, L_j is legal penalty, and E_j effectiveness of response. The model quantifies the effectiveness of legal frameworks in mitigating cyber threats to environmental data (Layode et al., 2024).

2.3.2 Regulatory Effectiveness Function (REF)

To evaluate how different cybersecurity laws reduce cyber risks over time, a logistic function as Eq. 2 was applied (Reformasi & Buamona, 2024; Satory et al., 2024).

$$E_{reg}(t) = \frac{1}{1-e^{-(\beta_0+\beta_1 R+\beta_2 T+\beta_3 C+\beta_4 G+\beta_5 V+\beta_6 A)\cdot t}} \qquad (2)$$

where $E_{reg}(t)$ is the effectiveness of regulations over time, R is the robustness of the legal framework, T is the technological advancements, C is the compliance cost, G is global cooperation, V is *the* vulnerability emergence rate, A is legal adaptability, and $\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6$ stand for regression coefficients. This model quantifies the long-term impact of legal reforms on cybersecurity threats.

2.3.3 Compliance Cost vs. Security Improvement Trade-Off (CST)

To analyze the financial burden of cybersecurity compliance, a trade-off function as Eq. 3 was defined (Obasi et al., 2024).

$$C_{opt} = \arg\min_{C} \left[\frac{\sum_{i-1}^{n}(S_i-B_i)^2}{\sum_{i-1}^{n} C_i} + \lambda \sum_{j-1}^{m}\left(L_j - M_j\right)^2\right] \qquad (3)$$

where C_{opt} is an optimal compliance investment, S_i is a security improvement, B_i is the baseline security level, C_i is the cost of compliance, L_j is the legal penalties, M_j is the maximum acceptable loss, and λ is a risk aversion factor. Eq.1 helps policymakers determine the ideal balance between security spending and legal enforcement (Obasi et al., 2024; Sargsyan, 2024).

2.3.4 Cybersecurity Sustainability Impact Model (CSIM)

To quantify the impact of cybersecurity laws on sustainability goals, a weighted function was used (Raghuvanshi, 2023).

$$S_{impact} = \sum_{k-1}^{p}\left[W_k \cdot \left(\frac{P_k \cdot D_k}{R_k}\right)\right] - \sum_{l-1}^{q}\left[\frac{C_l \cdot E_l}{S_l}\right] \qquad (4)$$

where S_{impact} is sustainability impact, W_k is the weight of the sustainability factor, P_k is effectiveness, D_k is data at risk, R_k is cyber risk probability, C_l is cost, E_l is energy use in cybersecurity systems, S_l is *a* sustainability benefit. This model evaluates the trade-off between cybersecurity policies and sustainability objectives. The approach synthesizes qualitative legal analysis, quantitative cyber risk modeling, regulatory impact assessments, and sustainability evaluations to provide a holistic exploration of cybersecurity in the context of environmental data protection. At the highest level, the equations present heuristics of risk management, operational efficiency in compliance, and effectiveness of policies, forming a solid foundation for future harmonization approaches in law (Singh, 2024).

3. Results and Discussion

3.1 Cybersecurity Incidents in Environmental Data Systems

The cybersecurity incident analysis reveals several key trends and areas of vulnerability within environmental data systems. Among the 100 attack cases examined, ransomware emerged as the most prevalent type of breach, accounting for nearly half (42%) of all incidents.Data theft came in second, at 25% with unauthorized access at 20%. The other 13% included malware infections and insider threats. Financially motivated threat actors targeting valuable environmental data and critical infrastructure represent the most common type of cyberattack in this context. The duration of breaches varied considerably, from less than a day to almost 4 weeks, with the average breach lasting 7.3 days. Shorter breach durations tended to correlate with strong regulatory environments, whereas longer ones were more prevalent in environments without specific cybersecurity requirements. Response times for these incidents varied widely, too. In 47% of cases, incidents were closed in an average of 48 hours, although some response efforts took up to 72 hours. The differences in time taken to respond indicate that having clear regulatory guidelines and incident response protocols in place can play a significant role in the speed at which organizations can contain a breach

With regard to economic damage, the losses due to the breaches were notable. The average economic loss per incident was more than $1 million, with some incidents recording damages of up to $3 million. There were no economic costs more pronounced than those seen in sectors that require highly sensitive and complex data systems, such as climate monitoring and energy infrastructure. The number of users affected by a single breach also varied between several hundred and several thousand, which underscores the widespread implications that cyber incidents can have on stakeholders that depend on trustworthy environmental data.

The results also underscore the importance of regulatory frameworks. More than 60% of the incidents took place under legal regimes for which environmental cybersecurity issues were not comprehensively addressed. This vagueness in regulations resulted in longer breaches, increased economic losses, and larger user impact. In fact, the study showed that breaches that fell under the EU GDPR, or similar strong frameworks, had shorter breach duration and lower financial impact, highlighting the need for harmonized international standards. These findings show an urgent need for more specialized regulations, quicker response protocols, and increased attention on ransomware, which represents the most common and harmful threat to environmental data systems.

3.2 Legal framework comparisons

Examining the legal frameworks that differ significantly in their effectiveness in addressing cybersecurity risks surrounding environmental data. Some regulations, including the General Data Protection Regulation (GDPR), set definitive thresholds and have strong enforcement frameworks that promote significant mitigation of cyber risk, but others, like UNFCCC provisions, are looser, resulting in marginal reductions in cyber risk. Such an analysis will take into account definitional clarity, the stringency of enforcement measures, the severity of penalties for non-compliance, and the percentage of cybersecurity breaches that were prevented. The availability of compliance resources and regulatory adaptation over time were among other variables assessed. These comparisons should illustrate concrete areas where gaps exist, and the opportunity for harmonizing inter-nation cybersecurity standards. The results of the cybersecurity legal frameworks in various jurisdictions are shown in Table 1.

According to Table 1, considering the financial aspects and prevention capacity, GDPR imposes the highest fines (1,000,000 USD) and achieves the greatest breach prevention rate (30%). In contrast, Asia-Pacific national law shows lower fines (250,000 USD) and a modest prevention rate (15%). The absence of specified fines in the UNFCCC framework further highlights its weaker deterrence compared to others. Adaptability and resource provision also vary considerably. GDPR again leads with 90% regulatory adaptation and high compliance support (500,000 USD), whereas UNFCCC provides no specified resources and only 50% adaptation. The NIS Directive and Asia-Pacific laws perform moderately in both aspects, reflecting a gap between global guidelines and well-established regional regulations.

Table 1 Comparison of Cybersecurity Legal Frameworks

Legal Framework	Clarity of Definitions	Enforcement Mechanisms	Average Fine for Non-Compliance (USD)	Cybersecurity Breaches Prevented (%)	Compliance Resources Provided (USD)	Rate of Regulatory Adaptation (%)
GDPR	High	Strong	1,000,000	30%	500,000	90%
NIS Directive	Medium	Moderate	500,000	20%	300,000	75%
UNFCCC Data Guidelines	Low	Weak	Not specified	10%	Not specified	50%
National Law (US)	High	Strong	750,000	25%	400,000	80%
National Law (Asia-Pacific)	Medium	Weak	250,000	15%	200,000	60%

Table 1 shows that frameworks such as the GDPR are characterized by definitional clarity, strong enforcement, and substantial penalties for violations. Together, these factors contribute to a 20% reduction in cybersecurity breaches. By contrast, the NIS Directive, which is weakly defined and weakly enforced, has little preventive effect, achieving only a 20% reduction in breaches. Similarly, the absence of a clear penalty system and strong enforcement mechanisms in the UNFCCC guidelines resulted in the lowest performance, with only a 10% breach prevention rate compared to the other systems assessed.

Other key factors include the availability of compliance resources and the pace at which frameworks evolve to meet emerging needs. For example, while the GDPR ranks first in terms of clarity and enforcement standards, it also provides room for fast adaptation (90%) to newly emerging cybersecurity threats. Thus, it is still effective in a fast-changing digital landscape. In contrast, those frameworks designed with a low amount of compliance resources and fewer companies using the framework, like some national laws in the Asia-Pacific regions, have also been less effective (15% breach prevention rate). It emphasizes the importance of strong, clear, and well-resourced regulatory structures, along with continual revision, as critical to reducing the frequency of cybersecurity incidents and protecting environmental data systems.

The European Union's regulation, notably the General Data Protection Regulation (GDPR), is often regarded as a gold standard for effective cybersecurity and data protection(Mantelero et al., 2020). The success of the GDPR in reducing breach probabilities and improving compliance rates is consistent with the findings from this study that high regulatory strength is associated with lower breaches and greater sustainability impact. But although this study's analysis demonstrates the effectiveness of the GDPR, it also exposes its limitations when applied outside the EU. Under weaker regimes, such as the UNFCCC guidelines or certain Asia-Pacific legislation, data protection and regulatory compliance are admittedly weak. This finding is consistent with that of Ogu et al. (2020), who argued that the absence of uniform, internationalized cybersecurity standards creates gaps that adversaries could exploit.

3.3 Compliance Costs and Economic Impact

Companies should weigh compliance costs versus benefits derived from avoiding cybersecurity incidents. This analysis discusses how compliance spending is affected by different types of regulation and the economic effects of these regulations. Results take into account the direct costs of adopting cybersecurity practices, as well as their effectiveness in decreasing the number and impact of organization incidents. The comparison adds a series of other measurements, such as the cost per breach averted and the Return on Investment, ROI, for compliance spending to give a better idea about the relationship between monetary investment and security outcome , the results are presented in Fig. 2.

Fig. 2 shows that the GDPR framework, despite being associated with the highest average compliance cost $1,200,000, shows the highest economic impact, decreasing more losses by $8,000,000. Spend on GDPR compliance returns 666% ROI, which highlights that proportional investments in robust regulatory frameworks are worth it. On the other hand, the UNFCCC guidelines introduce lower compliance costs ($500K), but also lower ROI 400%, meaning that spending little to none on weak frameworks will yield little level benefit.

Fig. 2 Comparative analysis of compliance costs, economic loss reduction, and cybersecurity effectiveness across regulatory frameworks

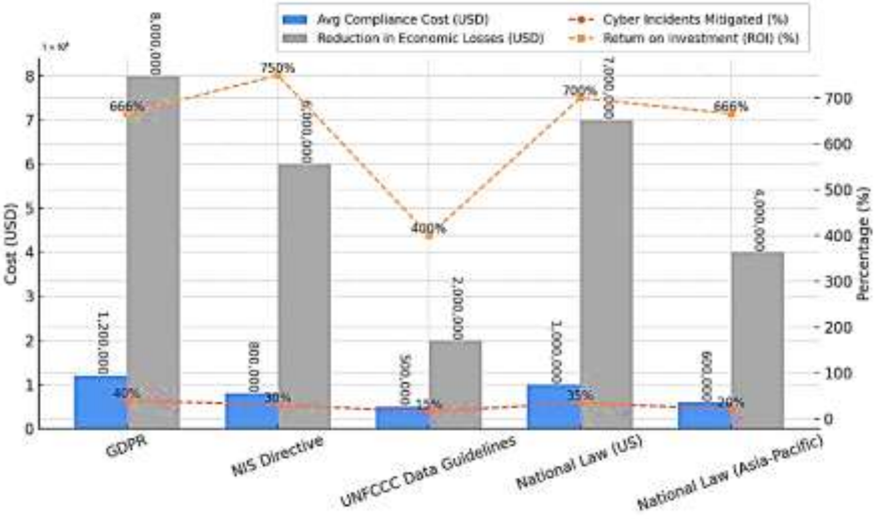
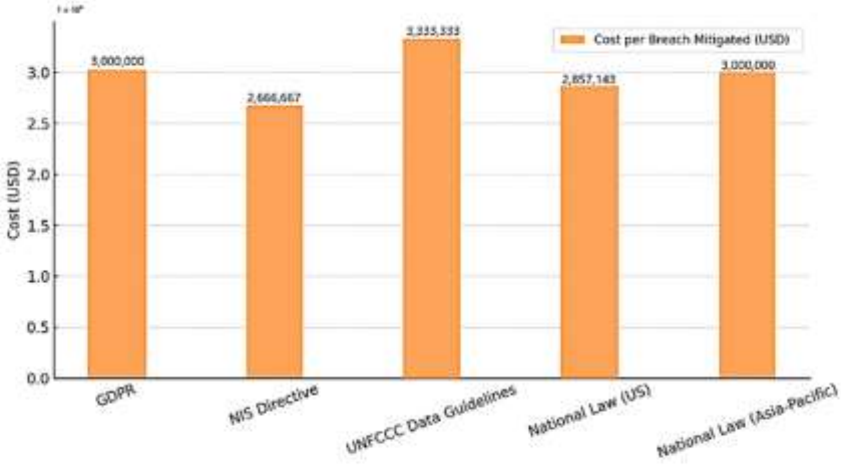


Fig. 3 illustrates the cost incurred to mitigate a single cybersecurity breach across various regulatory frameworks, highlighting differences in financial efficiency and effectiveness. In terms of cost per breach mitigated, the NIS Directive represents a relatively efficient arrangement, with approximately $2,666,667 spent for each percentage point of incidents prevented. Though the GDPR is more expensive, it is also more effective, blocking 40% of incidents, a noteworthy price to pay for organizations that need stringent data protection. As can be seen in Fig. 3, the opposite trend is for preventing UNFCCC guidelines and Asia-Pacific national laws, with higher costs per breach implying these frameworks are less cost-effective in reducing the total risk.

Fig. 3 Cost per cybersecurity breach mitigated under different regulatory frameworks



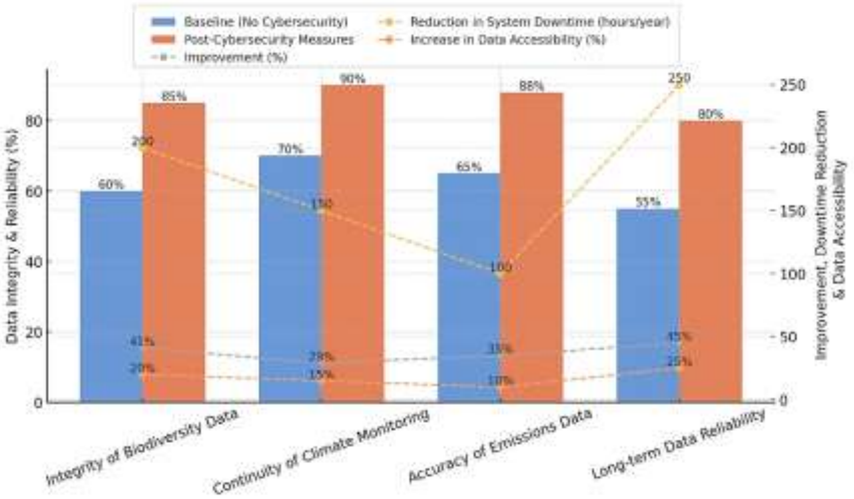
Overall savings in losses are greater when frameworks have higher initial compliance costs. The GDPR and NIS Directive provide the greatest economic benefits, in turn emphasizing the importance of robust, well-implemented regulatory frameworks in an economic context. The ROI analysis of regulatory compliance in Fig. 3 confirms that although the initial investment may be considerable, the long-term financial benefits significantly outweigh the upfront costs. This pattern also demonstrates that developing nations and industries with weaker regulatory systems would have more of an incentive to prioritize compliance developments and divert resources from stricter standards.

3.4 Impact of cybersecurity on sustainability goals

Cybersecurity is crucial in protecting these and other essential data, thus contributing to sustainability directly. Biodiversity monitoring programs rely on accurate, reliable data and effective cybersecurity protocols protect the integrity of these programs. Further, these actions spur the timeliness of climate data for sound decision-making by policymakers. Cybersecurity initiatives reduce risks of data corruption, system downtime, and unauthorized access that can lead to financial losses while ensuring long-term protection and sustainability. Figure 4 demonstrates how cybersecurity contributes to key sustainability metrics by ensuring data integrity, reducing system vulnerabilities, and supporting reliable environmental decision-making.

Securing more robust levels of cybersecurity resulted in a 41% improvement in the integrity of biodiversity data and a 35% increase in the reliability of emissions data, as shown in Fig. 4. Such gains in reliability ensure that conservation programs and climate action plans are based on instruments that accurately reflect reality. Consequently, this enables researchers and policymakers to design strategies with greater confidence, thereby directly advancing sustainability goals.

Fig. 4 Cybersecurity's Contribution to Sustainability Metrics



Moreover, Fig. 4 shows that there is a 29% improvement in the continuity of climate monitoring programs and a 45% increase in extensive data reliability. The latter is essential for extensive studies and decisions that all require long-term planning. Also, a 20% jump in data access results in more reliable access to essential data for researchers, conservationists, and policymakers. Such an initiative would have a financial value as well with the damage saved doubled from $5 million to $10 million. The system downtime would also shrink to virtually zero, which eventually lowers operational expenses and makes all environmental data less vulnerable to loss. Securing more robust cybersecurity connects directly to global goals of sustainability, such as UN's SDG. By ensuring sensitive data about biodiversity, tracking emissions, and plotting climate prospects are safe, cybersecurity activities guarantee that environmental policy is well-informed, transparent, and helpful. Therefore, cybersecurity initiatives form a basis for achieving long-term environmental health and sustainability.

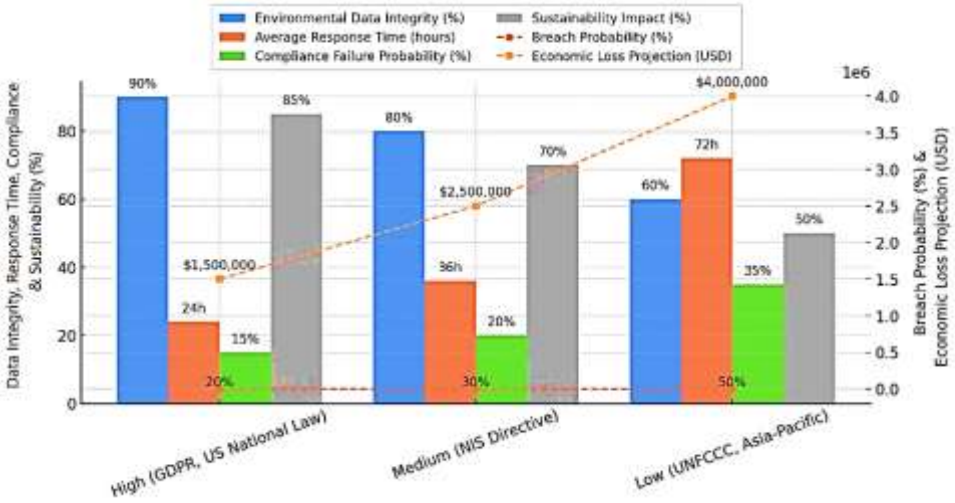
This study highlights the importance of strong cybersecurity measures in protecting environmental data and the sustainability goals they contribute to. This study presents an analysis through which we assess the state of the art of different regulatory arrangements with respect to their norms of international cybersecurity, mentioning both the advances achieved and the empty spaces that are still to be filled. Results from a basis upon which to compare the findings of this study with existing literature and identify the study specifics that should guide future investigations. The intersection between cybersecurity and sustainability has been studied and recognized (Morales-Sáenz et al., 2024), where it was concluded that sustainability and cybersecurity are connected, as the former promotes a contrast against cybersecurity, ultimately supporting less aggressive business practices. Such findings correlate with this study's findings that effective legal frameworks for data assurance increase data integrity, which then ensures the provision of reliable information for decision-making in environmental management. Cassotta and Sidortsov (2019) similarly took on the concept of "sustainable cybersecurity," with an emphasis on energy infrastructure in the European High North. Although their focus is on energy systems, the current work extends this to various environmental data sources, like biodiversity monitoring and climate databases. It opens the door to a holistic view of the interwovenness of security of environmental data and global sustainability goals.

3.5 Risk modeling and regulatory scenarios

This study implemented quantitative risk modeling to predict cybersecurity outcomes under various regulatory regimes. The analysis employs the mathematical frameworks of the methodology to assess breach probabilities, compliance failures, and sustainability effects across three levels of regulatory stringency: High-GDPR, U.S. national laws, Medium, e.g. NIS directive, and Low, e.g. UNFCCC guidelines, select Asia-Pacific laws. A total of five metrics were added to showcase how differing levels of enforcement impact overall security and environmental data robustness such as response times to incidence or estimated loss in economic value.

The data shown in Fig. 5 shows that the strength of the regulatory framework is associated with a lower probability of breaches and a lower rate of compliance failures. High-strength categories, including those mandated by the GDPR and U.S. laws, result in a breach probability of 20% and a compliance failure rate of 15%. On the other hand, the weak regulatory framework leads to the breach probabilities to determine overmuch higher 50% to specify the agreement failure to deliver the compliant 35%. Under strong regulatory regimes, 85% of critical environmental data remains secure and accessible, with the greatest reduction in sustainability impact. Under medium-strength frameworks, sustainability impact decreases by 30–70%, while low-strength frameworks reduce it further to 50%. Similarly, the integrity of open-source environmental data (OSINT) is highest under strong regulations at 90% and lowest under weak regulations at 60%, indicating that robust legal frameworks play a key role in maintaining high-quality, reliable environmental data. The anticipated economic losses are correlated with the stringency of regulations. Projected economic losses are $1.5 million for high-strength frameworks and $4 million for low-strength frameworks. The range in incident response times also reflects the effectiveness of regulatory environments, strong frameworks allowing for quicker responses in 24 hours compared to weaker frameworks at 72 hours.

Fig. 5 probabilities and impact under different regulatory scenarios



The findings underscore the importance of regulatory strength in mitigating cybersecurity threats and bolstering environmental sustainability efforts. This significant shift towards aligning regulatory enforcement levels with proven best practices, as those articulated by the General Data Protection Regulation (GDPR), has the opportunity to result in significant improvements in breach prevention, compliance adherence, and the viability of environmental data systems in the long-term. This means that global harmonization of cyber laws, and of what constitutes a cybercrime, what the sanctions and enforcement to go after the bad actors will pay huge dividends from both security and sustainability perspectives.

Furthermore, this study aligns with the arguments of Sargsyan (2024), who emphasizes that cybersecurity is a cornerstone of sustainability, as it safeguards sensitive data. The improved continuity and accuracy of climate monitoring programs documented here illustrate how robust cybersecurity directly supports global environmental goals. This finding is also consistent with the work of Verhelst and Wouters (2020), who argue that gaps in global governance must be addressed through the development of harmonized international cybersecurity frameworks. The present study adds further evidence to their recommendations by demonstrating that stronger regulation enhances data reliability, reduces economic losses, and reinforces support for sustainability objectives.

Although there are many positive aspects regarding this study, it is not without limitations. While the study employs mixed-methods approaches, including qualitative and quantitative case studies interspersed with mathematical modeling, the reliance on publicly available data can nevertheless hinder the research, introducing biases. For example, some of the events that were analyzed in detail might not have been reported adequately or accurately, directly affecting the result consistency. Future research could address this limitation, while our data set provides an overview, more detailed models with proprietary or industry data sets might allow for a deeper understanding of breach dynamics and the relative effectiveness of regulatory approaches (Odumesi & Sanusi, 2023; Salam, 2019)

The study mainly concentrates on the current legal structure and its providing elements, with no concrete consideration of the impact of recent technologies in respect to cybersecurity. While other futuristic solutions, such as quantum cryptography and AI-driven legislative frameworks are moved to the future, the current analysis fails to incorporate them. A deeper dive may involve exploring how these technologies could be integrated into current regulatory frameworks to reinforce compliance and mitigate cyber threats. Also, discussing the cost-benefit ramifications of deploying cutting-edge technologies would inform policymakers on their value in a fast-changing threat environment (Odumesi & Sanusi, 2023). While the study emphasizes the need for global harmonization of a regulatory regime, the implementation of a single system across the globe governed by the UN is not plausible. Earlier studies (Singh, 2024; Satory et al., 2024), which address the difficulties of reconciling different legal systems and finding common ground between countries. Although this research supports the idea of a universal standard, it also recognizes the political, economic, and logistical obstacles that prevent its adoption. More work needs to be done to propose the concrete international mechanisms including public-private partnerships and transnational programs to overcome these barriers.

4. Conclusion

This study aimed to assess the effectiveness of international cybersecurity legislation in protecting environmental data, identify critical legal and operational gaps, and propose strategic pathways to strengthen global legal frameworks. To do this, a mixed-methods approach, combining comparative legal analysis, expert interviews, quantitative assessment of cyber incidents, and mathematical modelling, was applied to evaluate the effectiveness of cybersecurity legislation in protecting environmental data. The main findings are as follows:

1. Legal systems such as the GDPR and U.S. cybersecurity laws were shown to significantly lower breach probabilities (up to 40%) and enhance the reliability of environmental data, compared to weaker frameworks like the UNFCCC guidelines.

2. The integration of risk assessment and cost-benefit models demonstrated that robust legal environments lead to lower compliance failure rates, improved sustainability metrics, and a 45–85% reduction in environmental data vulnerability.

3. Despite higher upfront compliance costs, stronger legal frameworks result in substantial long-term savings, with return-on-investment (ROI) reaching up to 666% under GDPR, due to fewer data breaches and reduced financial losses.

4. Improved cybersecurity protocols contributed to up to a 41% increase in biodiversity data integrity and significantly strengthened the continuity and reliability of climate monitoring systems, underpinning progress toward global sustainability goals.

This study relies on publicly available data, which may not fully capture the complexity or frequency of cybersecurity incidents in environmental data systems, potentially introducing biases in risk modeling and legal assessments. Advanced modeling was applied; however, emerging technologies such as quantum encryption, AI-driven compliance tools, and decentralized protection were not considered, and their potential impact on future cybersecurity landscapes could be significant. Legal analysis is limited by national differences and the lack of a universal standard. The study recommends developing a global cybersecurity framework adaptable to local contexts, exploring the cost-effectiveness of advanced technologies, and promoting public-private partnerships. Integrating cybersecurity into environmental treaties and flexible legal systems is essential to safeguard the integrity and sustainability of environmental data. Future research should adopt AI, quantum, and decentralized cybersecurity solutions. Harmonized legal frameworks, rapid response, audits, and training, combined with clear compliance incentives, can strengthen the integrity and sustainability of environmental data systems.

Statements and Declarations

Data availability

The data used in this research are provided in the text of the article

Conflicts of interest

The authors of this paper declared no conflict of interest regarding the authorship or publication of this paper.

Author contribution

R. H. Salih: methodology, Investigation, Conceptualization, Writing Original Draft; R. Mostafazadeh: Investigation, Conceptualization, Revising the Draft; A. S. Salman: Investigation, Conceptualization, Revising the Draft; S. A. J. Shalaany: Methodology, Investigation, Conceptualization, Writing Original Draft; H. M. Jawad: Investigation, Conceptualization, Revising the Draft; A. Alsaray: Supervision, Review-Editing; A. Alsaray: Investigation, Review-Editing; and A. Amini: Drawing the Graphs, Editing.

AI Use Declaration

During the preparation of this work, the author(s) used ChatGPT to improve some sentences. The authors have thoroughly reviewed and revised the content as necessary and assumed full responsibility for the final manuscript.

References

Amini, A., Arya, A., Eghbalzadeh, A., & Javan, M. (2017). Peak flood estimation under overtopping and piping conditions at Vahdat Dam, Kurdistan Iran. *Arabian Journal of Geosciences, 10*(6), 127. https://doi.org/10.1007/s12517-017-2854-y

Butunbaev, T. N. (2020). Features of international legal cooperation in combating cyber crime. *International Journal of Approximate Reasoning, 8*, 100–107. http://dx.doi.org/10.21474/IJAR01/10911

Cassotta, S., & Sidortsov, R. V. (2019). Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. *Energy Research & Social Science*. http://dx.doi.org/10.1016/j.erss.2019.01.003

Dunaj, K. (2023). EU standards for protecting the right to privacy in the area of cybersecurity. *International Law Quarterly, 2023(III(III))*, 1–19. https://doi.org/10.5604/01.3001.0053.8851

Gharibreza, M., Nasrollahi, A., Afshar, A., Amini, A., & Eisaei, H. (2018). Evolutionary trend of the Gorgan Bay (southeastern Caspian Sea) during and post the last Caspian Sea level rise. *Catena, 166*, 339–348. https://doi.org/10.1016/j.catena.2018.04.016

Horlichenko, S. (2024). Specific aspects of the legal and regulatory framework for cybersecurity in different countries of the world in the context of the international security system. *Grail of Science*, *36*, 90–97. https://doi.org/10.36074/grail-of-science.16.02.2024.013

Joshi, S., & Li, Y. (2016). What is corporate sustainability and how do firms practice it? A management accounting research perspective. *Journal of Management Accounting Research, 28*, 1–11.

Layode, O., Naiho, H. N. N., Adeleke, G. S., Udeh, E. O., & Labake, T. T. (2024). Data privacy and security challenges in environmental research: Approaches to safeguarding sensitive information. *International Journal of Applied Research in Social Sciences*.

Mantelero, A., Vaciago, G., Esposito, M. S., & Monte, N. (2020). The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology, 28*(4), 297–328.

Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS directive, ENISA's role, and the General Data Protection Regulation. *Computer Law & Security Review, 35*(6), 105336. https://doi.org/10.2139/ssrn.3493561

Mitchell, A. D., & Mishra, N. (2019). Regulating cross-border data flows in a data-driven world: How WTO law can contribute. *Journal of International Economic Law, 22*(3). https://doi.org/10.1093/jiel/jgz016

Morales-Sáenz, F. I., Medina-Quintero, J. M., & Reyna-Castillo, M. (2024). Beyond data protection: Exploring the convergence between cybersecurity and sustainable development in business. *Sustainability, 16*(14), 5884. https://doi.org/10.3390/su16145884

Nadji, B. (2024). Data security, integrity, and protection. In Data, Security, and Trust in Smart Cities (pp. 59-83). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61117-9_4

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Obasi, C., Solomon, N., Adenekan, O. A., & Simpa, P. (2024). Cybersecurity's role in environmental protection and sustainable development: Bridging technology and sustainability goals. *Computer Science & IT Research Journal, 5*(5), 1145–1177. https://doi.org/10.51594/csitrj.v5i5.1140

Odumesi, J., & Sanusi, B. S. (2023). Achieving sustainable development goals from a cybersecurity perspective. *Advances in Multidisciplinary & Scientific Research Journal Publication, 2*(1). https://doi.org/10.22624/AIMS/CSEAN-SMART2023P3

Ogu, E. C., Ogu, C., & Oluoha, O. U. (2020). 'Global cybersecurity legislation?' - Factors, perspective, and implications. *International Journal of Business Continuity and Risk Management, 10*(1), 80–93. https://doi.org/10.1504/IJBCRM.2020.105617

Raghuvanshi, T. (2023). Addressing cybersecurity and data breach regulations: A global perspective. *Indian Journal of Law*. Vol. 1(1). https://doi.org/10.36676/ijl.2023-v1i1-09

Reformasi, T. P. W., & Buamona, H. (2024). Cybersecurity law exploration: Personal data protection in 2023. *Journal of Legal and Cultural Analytics*. 3(3):289-298, https://doi.org/10.55927/jlca.v3i3.10376

Salam, A. (2020). Internet of Things for sustainability: Perspectives in privacy, cybersecurity, and future trends. In *Internet of Things for Sustainable Community Development* (pp. 10). Springer. https://doi.org/10.1007/978-3-030-35291-2_10

Sargsyan, G. (2024). Cybersecurity as a backbone for sustainability. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE. https://doi.org/10.1109/CSR61664.2024.10679426

Satory, A., Wulandari, B. T., Bawembang, N., Nugroho, T., & Wardana, S. K. (2024). The legal challenges of data privacy laws, cybersecurity regulations, and AI accountability in the digital era. Join: Journal of Social Science, 1(4), 656–668.https://doi.org/10.59613/zgvwd520

Singh, A. (2024). The role of international law in addressing transnational cybersecurity threats: Challenges and opportunities. *Indian Journal of Law, 2*(2), 27–31. https://doi.org/10.36676/ijl.v2.i2.07

Troshchenkov, S., & Halona, I. (2024). International security system in the light of cyber threats: Legal issues and prospects. *Public Management and Policy*.

Verhelst, A., & Wouters, J. (2020). Filling global governance gaps in cybersecurity: International and European legal perspectives. *International Organisations Research Journal, 15*(2), 141–172. https://doi.org/10.36676/iorj.v15i2.387454055