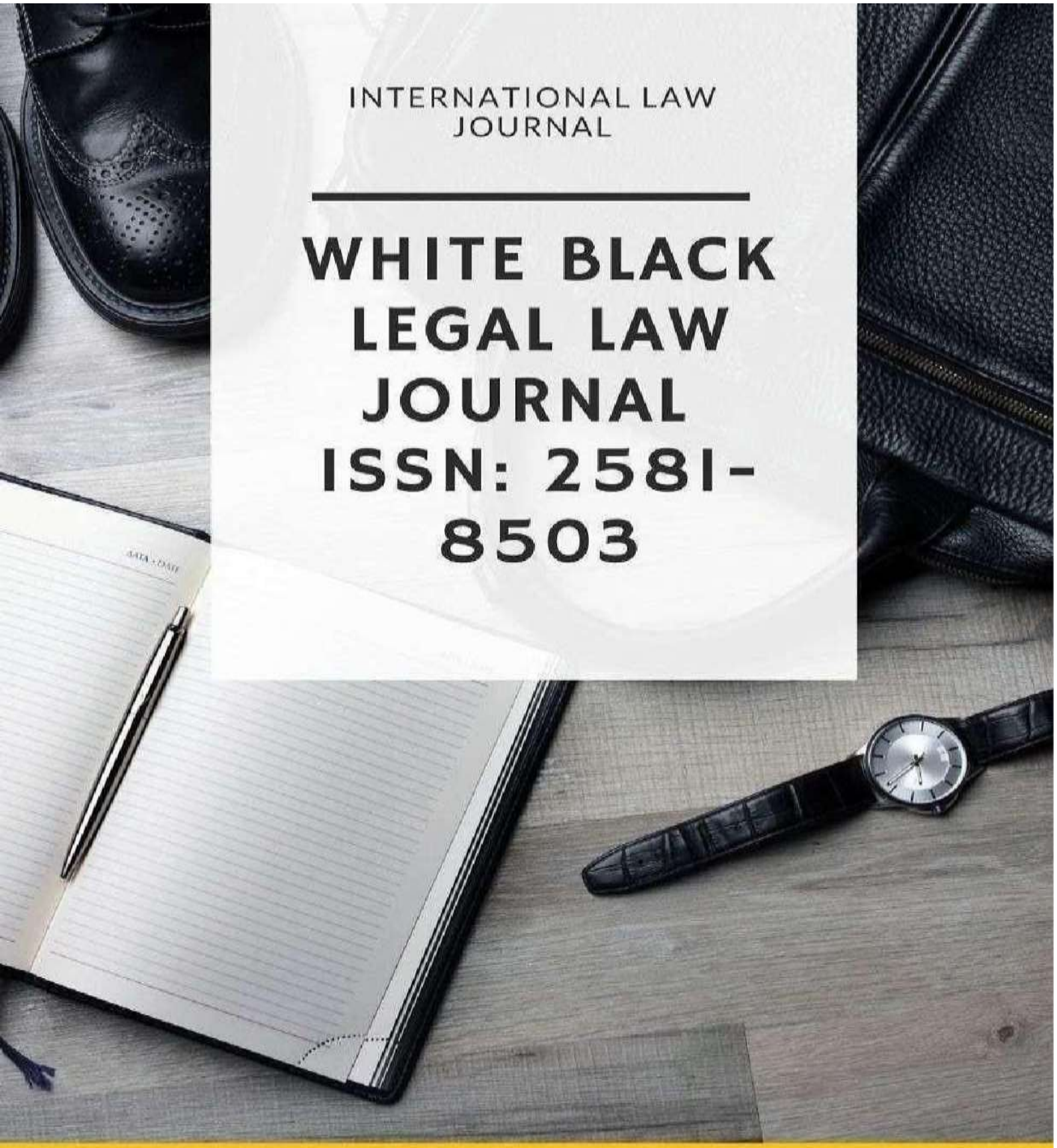

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

CYBERSECURITY AS A SOCIAL RESPONSIBILITY: ALIGNING CSR WITH DATA SECURITY PRACTICES

AUTHORED BY - SHATAKSHI DIXIT

Abstract

The globalization of the digital economy has transformed cybersecurity from a limited technical challenge into a key element of corporate social responsibility (CSR). Data breaches and cyberattacks are not only costly for entities but have far-reaching consequences for society, such as infringement of personal privacy, reduction in public confidence in digital infrastructure, mass-scale identity theft, disruption of essential services, and deepening of digital resilience inequalities. This paper argues that corporations have a duty to strategically integrate a strong data security approach into their CSR systems, not only to meet ethical commitments towards diverse stakeholders but also to contribute to building a safer and more ethical digital ecosystem. Based on stakeholder theory, signaling theory, and state of the art empirical evidence, the paper traces the historical and conceptual incorporation of cybersecurity in the CSR and wider ESG (environmental, social and governance) frameworks, reviews regulatory efforts of major bodies such as the EU, quantitatively and qualitatively analyzes the costs and societal impact of breaches on the society, reviews relevant case studies of failings and resilient approaches, and derives a multi-pillars Cybersecurity Integrated CSR (CICSR)Framework; it shows how effective and authentic CSR practices can effectively have a "reputational insurance" function against the adverse impacts of an incident, and, at the same time, provide the opportunity to improve employees' cybersecurity habits via mechanisms such as psychological safety and less job stress, while the phenomenon of Corporate Social Irresponsibility (CSIR) correlates positively to breach incidence and intensity.

Drawing on the latest industry reports and academic findings up to 2025–2026, the paper addresses emerging challenges posed by artificial intelligence (AI), shadow AI, and quantum computing threats. This paper concludes with recommendations for practitioners, policy implications for regulators and avenues for future disciplinary research and the actions they can take.

Keywords: Cybersecurity, Corporate Social Responsibility (CSR), Data Protection, Data Breaches, ESG Reporting, Digital Trust, Stakeholder Theory, and Corporate Social Ignorance (CSI)

1. Introduction

With the advancement and continuous reliance of digital technologies, the business operations, stakeholder relationships and societal structure have been reshaped. Unprecedented efficiency and innovations have paved its way through Cloud computing, Internet of Things (IoT) devices, artificial intelligence (AI) application, and interconnected supply chains. However, this rapid digital revolution also extended the attack surface for cybercriminals. Cybersecurity has emerged as one of the most pressing threats facing modern organisations and societies alike, with incidents like ransomware attacks on hospitals to large-scale exfiltration of data from consumer databases.

As per a study by IBM for Cost of a Data Breach Report, the global average cost of a single data breach hit 4.44 million USD, which represents a decrease of 9% from the previous year's average of 4.88 million USD. This decrease was a direct result of the AI powered security tools and automation with its swifter identification and containment. However, notable regional disparities have persisted, with average costs surging 9% to a record 10.22 million USD in the United States. Sectors such as healthcare, finance and critical infrastructure continue to feel the most burden, as breaches could ripple into broader societal disruptions, including postponed medical treatment, financial instability for individuals and communities, and even threats to public safety.

Historically, CSR initiatives have focused on things like environmental sustainability, fair labor practices, community development, and ethical governance. In an ever hyper-connected world, however, data and digital ecosystems have become another equally critical dimension of social responsibility. Cybersecurity malfeasances are no longer seen as mere technical/operational failures but ethical breaches that amount to a violation of social contracts with customers, employees or suppliers, regulatory bodies, and the public at large. Academia is beginning "to situate cybersecurity in the world of ESG," where proper data protection increases "social" capital through digital trust and "governance" through risk-resilient management.

In this paper, we argue that incorporating cyber security into CSR is not only helpful, but necessary for ethical business conduct, risk mitigation for long-term survival, and sustainable competitive advantage.

The research questions that this paper seeks to answer are: 1. How has cyber-security been conceptualized in CSR scholarship and practice? 2. What practical frameworks can organizations adopt to operationalize cyber-security as a key CSR element? 3. What are the challenges, practice tips, and future trends related (to the risks and opportunities) that should be anticipated with regards to the increased complexity offered by emerging technologies?

The following sections of this paper are as follows:-

- Literature review and theoretical foundations
- Multiple aspects of the security breach of the society, in depth
- Explaining the constantly evolving regulatory landscape of cyber-security and the resulting requirements and considerations of the CSR practice.
- Detailed case studies of negative and positive outcomes.
- A comprehensive framework for alignment has been provided.
- Finally a confluence of implementation challenges, way forward and future trends has been presented.

By providing a holistic, descriptive, and evidence-based treatment of the matter, we aim to help bridge the gap between the diverse technical literature of cyber security, on the one hand, and the domains, on the other, of business ethics and management studies.

2. Literature review and theoretical foundations

With the social and moral implications of digital risks gaining more attention, the CSR scholarly discourse is shifting from seeing social responsibilities as a mere "responsibility beyond profit" to encompassing a broader perspective that includes actions and decisions that serve to maximise profit while at the same time adhering to the law. Traditionally, the seminal work of Milton Friedman has dominated the CSR discourse, advancing a shareholder primacy perspective that argues organisations have no responsibility beyond that owed to their shareholders. However, the emergence of stakeholder theory posits that organisations have obligations to a far greater range of stakeholders including customers, employees and the wider

society. For the vast majority of people, organisations with which they have most direct contact are those that provide digital systems and environments that are safe and secure. This includes both the commercial organisations for whom they work and the information, communication and technology systems that facilitate their work.

Cybersecurity too has made inroads into ESG discourse. Khan (2025) establishes linkage between ESG—specifically social responsibility—outcomes and cybersecurity. Not only do cyber-mishaps make it more likely for other social responsibility practices to fail, but cyber-attacks also negatively impact a firm's share price. CSR practices therefore carry insurance-like characteristics that generate moral capital. Bamita et al. (2023) found that firms with strong CSR practices prior to a cyber-data breach faced less damage from the incident post breach. Their sample of breached firms found that firms with superior CSR performance prior to a breach experienced only a short-term stock price drop (around 30 days). In the long run, their moral capital helped them to offset negative stakeholder reactions and regain their operating footing.

The academic literature on cybersecurity and CSR has rapidly grown in recent years, reflecting increasing awareness of digital risks' social and moral implications. Prior CSR scholarship, from Milton Friedman's shareholder primacy perspective, often framed social responsibilities as limited to profit maximization within legal parameters. On the other hand, stakeholder theory (Freeman, 1984; extended by Matten & Crane, 2005) suggests organizations have obligations to a wider range of parties, including customers who trust them with personal data, employees who rely on safe systems, and society that depends on reliable digital infrastructure. When organizations fail to safeguard this data, their stakeholders are hurt, and data security therefore cannot be dismissed as just a technological or operational problem but must be framed as a moral and social duty.

New empirical and theoretical scholarship has also integrated cybersecurity more squarely into ESG discourse. Khan (2025) provides validity to such claims by finding that cybersecurity breaches not only increase the risk of other forms of social responsibility violations but also correlate with stock price drops, positioning robust cybersecurity management practices as a quantifiable measure of corporate responsibility. Bamita et al. (2023) add to this discourse by demonstrating the "insurance-like characteristics of CSR" -firms with strong pre-breach CSR performance are significantly less severely punished upon breaches. In particular, the authors'

examination among breached firms showed that firms with high CSR benefit from "moral capital" gained over years of responsible behavior, allowing them to better withstand stakeholder anger and recover more quickly.

Meanwhile, Rezae (2024) finds a statistically significant positive correlation between CSIR levels and data breach incidence, with environmental and the product dimension of CSIR correlating with external breaches, and governance/employee issues more likely to cause internal ones. The authors also show that CSIR intensifies negative stock market reactions, and that following breaches, firms create new CSR committees that can prevent this irresponsible behavior.

Behaviorally, Kim & Lee (2025) use an integrative model influenced across social identity theory, social exchange theory, and the job demands-resources (JDR) model. Their research reveals CSR initiatives directly and indirectly affect cybersecurity behaviors through increased psychological safety and reduced job stress. By nurturing a robust CSR culture, organizations foster an environment where employees feel confident to report anomalies and perceive security as a collective ethical duty.

While several theoretical models have been developed to address these issues as well, this research builds on Maastricht University's Data Protection as a Corporate Social Responsibility (UM-DPCSR) model. The UM-DPCSR model offers a broader framework of applying the GDPR principles and demonstrates how data protection is implemented through 'data protection by design, default' by including systems to promote transparency and 'ethical data processing' throughout the entire enterprise life cycle. Insights can be gained from studies on GDPR compliance and how this has made cybersecurity the number one priority for industry executives – a priority that intersects with ESG reporting and addressing stakeholder expectations.

This is not the only area in which signalling theory may have some relevance - the way in which senior individuals in organisations involved in information systems invest in cyber security and signal that investment to customers, suppliers, press and bloggers etc may be seen as a way of demonstrating greater organisational ethics in the face of increasing criticism.

Despite significant research on this topic, there are several gaping holes in the extant literature.

Although there are many studies which focus on a reactive and utilitarian interpretation of corporate web sites, few have attempted to examine long term effects or conducted cross cultural research including organizations from emerging economies (e.g. small-medium enterprises in Europe and Asia). This paper seeks to address some of this shortfall by integrating a number of the above perspectives and present a practical, managerial and conceptual framework.

While the financial cost of a cybersecurity failure may be contained within a corporation's bottom line, the broader societal implications of such an event have far-reaching and deeper repercussions that impact people's lives and the fabric of society as a whole. For example, many individuals affected by a data and identity Theft breach will experience identity theft, financial fraud, and may be subjected to long-term psychological harm as a result of a single breach incident. They may spend years remedying errors with their credit score or grapple with the trauma of a cyber-attack. Moreover, certain industries, like healthcare, possess information of a uniquely personal and sensitive nature, and breaches involving this information can lead to dire consequences for patients, including delays in treatment, discrimination, and a crisis of faith in the very institutions responsible for their care.

The economic cost of these incidents is nothing short of alarming; according to IBM's 2225 whitepaper Costs of a Data Breach, the global average cost per breach is USD 4.144 million. According to the Identity Theft Resource Center's 2025 Annual Data Breach Report, there were a record 3,322 data compromises in the U. S. in 2025, an increase of 5% over 2024, representing three years in a row where over 3,000 incidents have occurred. While the number of records exposed decreased due to a decrease in the number of mega-breaches, the number of notifications decreased from 2024 to 2025 to around .8278 million. However, attacks are increasingly well-targeted, with higher impact than in the past, and credential theft is a growing factor in such incidents.

From an enterprise perspective critical infrastructure breaches can pose significant risks including impact to critical services and safety of people, in addition to an overall erosion of trust in digital systems. Cyberattacks are ranked as the top global risk by the World Economic Forum, and can have lasting effects on vulnerable populations recovering at different speeds than technology early adopters, potentially widening the emerging digital gap.

From a CSR perspective organisations, as guardians of vast amounts of personal data, fail in their social responsibilities either due to embedded vulnerabilities or missed opportunities caused by a desire to maximise profit. This behaviour constitutes corporate social irresponsibility and undermines an organisation's social licence to operate. However, those organisations that invest in data awareness campaigns and initiatives such as digital literacy, as well as those that adopt open-source solutions that contribute to the digital commons, can be seen to be performing a positive role.

Staff of organisations under cyber attack experience elevated levels of stress and decreased morale. General consumer turbulence and decreased participation in e-commerce can also impact organisations with a digital strategy and cause them to fail to launch "crazier" innovations. Given that cyber security is in part a public good, its absence results in negative externalisation whereas its provision creates positive spillovers and is in line with the shared value mandate of CSR.

3. Societal Impacts of Cybersecurity Failures

While the financial cost of a cybersecurity failure may be contained within a corporation's bottom line, the broader societal implications of such an event have far-reaching and deeper repercussions that impact people's lives and the fabric of society as a whole. For example, many individuals affected by a data and identity Theft breach will experience identity theft, financial fraud, and may be subjected to long-term psychological harm as a result of a single breach incident. They may spend years remedying errors with their credit score or grapple with the trauma of a cyber-attack. Moreover, certain industries, like healthcare, possess information of a uniquely personal and sensitive nature, and breaches involving this information can lead to dire consequences for patients, including delays in treatment, discrimination, and a crisis of faith in the very institutions responsible for their care.

The economic cost of these incidents is nothing short of alarming; according to IBM's 2225 whitepaper Costs of a Data Breach, the global average cost per breach is USD 4.144 million. According to the Identity Theft Resource Center's 2025 Annual Data Breach Report, there were a record 3,322 data compromises in the U. S. in 2025, an increase of 5% over 2024, representing three years in a row where over 3,000 incidents have occurred. While the number of records exposed decreased due to a decrease in the number of mega-breaches, the number of

notifications decreased from 2024 to 2025 to around .8278 million. However, attacks are increasingly well-targeted, with higher impact than in the past, and credential theft is a growing factor in such incidents.

From an enterprise perspective critical infrastructure breaches can pose significant risks including impact to critical services and safety of people, in addition to an overall erosion of trust in digital systems. Cyberattacks are ranked as the top global risk by the World Economic Forum, and can have lasting effects on vulnerable populations recovering at different speeds than technology early adopters, potentially widening the emerging digital gap.

From a CSR perspective organisations, as guardians of vast amounts of personal data, fail in their social responsibilities either due to embedded vulnerabilities or missed opportunities caused by a desire to maximise profit. This behaviour constitutes corporate social irresponsibility and undermines an organisation's social licence to operate. However, those organisations that invest in data awareness campaigns and initiatives such as digital literacy, as well as those that adopt open-source solutions that contribute to the digital commons, can be seen to be performing a positive role.

Staff of organisations under cyber attack experience elevated levels of stress and decreased morale. General consumer turbulence and decreased participation in e-commerce can also impact organisations with a digital strategy and cause them to fail to launch "crazier" innovations. Given that cyber security is in part a public good, its absence results in negative externalisation whereas its provision creates positive spillovers and is in line with the shared value mandate of CSR.

4. Regulatory landscape and compliance as CSR

Cybersecurity has become an important aspect of "Ethical Corporate Behavior" in the laws and regulations in many countries around the world. The European Union's General Data Protection Regulation (GDPR) laid down the principle of "data protection by design and by default," with strict requirements concerning any processing of data for consent and transparency, and even laid down a penalty of up to 4% of global sales in the event of any breach of personal data. The NIS2 Directives currently scheduled to come into effect in 2026 expand the scope of the cybersecurity requirements to 18 areas of industry and commerce,

requiring the systematic management of risk, the prompt reporting of major cyber incidents 24/7, the assessment of the security of supply chains, and the appointment of a director on the company's board with responsibility for cybersecurity. In the United States, the Securities and Exchange Commission issued a rule concerning the timely disclosure of material cybersecurity incidents, while many states and cities have enacted laws regulating cybersecurity such as data breach notification, cybersecurity standards for contractors, and social media surveillance bans. These laws include the California Consumer Privacy Act (CCPA/CPRA), which grants a wide range of rights to consumers in relation to their personal data. Voluntary international standards such as ISO 27001, the NIST Cybersecurity Framework, and CISA's Cyber Essentials and other guidance are widely adopted to ensure best-practice cybersecurity.

Compliance is the minimum requirement for corporate social responsibility with respect to data privacy and security. Indeed, going beyond the minimum requirement and fostering a culture of ethical leadership is key to building credibility with the public and the market. The UM-DPCSR framework calls on organizations to embed fairness in their strategy, to promote societal education about data rights and to incorporate data and information security and protection into the product development process as well as into their supplier relationships. Open reporting of incidents, as well as of positive experiences and key statistics, is also crucial for earning legitimacy and standing out from the crowd in terms of responsible business practices. In sum, regulations that require organizations to respect the privacy and security of data serve as a floor but also as a springboard for innovation with respect to social responsibility with respect to data. By viewing compliance with data privacy and information security regulations not as a cost of doing business but rather as a CSR opportunity, organizations can transform a legal requirement into a strategic differentiator, lowering the risk of costly litigation and reputational damage over the long term.

5. Case Studies: Lessons from Breaches and Resilient Responses

With recent high-profile incidents laying bare the links between CSR and cybersecurity failures, companies are now scrambling to understand their exposure.

A vulnerability in the Apache Struts web application that Equifax used to process customer applications remained unpatched for 76 days until attackers exploited the vulnerability to steal the sensitive information including social security numbers and other data related to 147 million

individuals. The company's delayed disclosure of the breach, inadequate engagement with stakeholders, and perceptions of prioritizing shareholders' returns over consumers' data led to Congressional hearings. In the end, the company agreed to a settlement of over $1.38 billion and the resignation of its CEO. The Equifax case study illustrates how a governance failure and inadequate engagement with stakeholders, can have very negative consequences to society. Furthermore, it illustrates the importance of being proactive in protecting customers' information as a CSR activity to avoid greater harm, and how something as simple as a patch could have prevented the worst data breach in history. The case study of Uber from 2017 also speaks to the ethics of such failures. In that case, the company not only paid hackers to delete the stolen data of 57 million users and drivers, but covered up the breach for over a year, until finally, in late 2017, it was exposed. Although the company has since improved how it reports breaches, the incidents at Uber highlight the opposite end of the spectrum, and how a "cover-up" approach to breaches can lead to increased social irresponsibility and erosion of trust in integrity of corporations. The 2022 breach at Uber also highlights the need for increased awareness on both a corporate and societal level, as the breach was the result of simple social engineering.

Evidence shows that Yahoo did not disclose breaches in 2013-2016, and that delayed disclosure of data breaches had cost Yahoo in terms of lower price Verizon paid for Yahoo during acquisition process, and the damage done to public trust. The problem seems rooted in underinvestment in information security to pursue growth and other business goals. In contrast, organizations with CSR-oriented cultures are better protected and managed in the face of security crises. The empirical evidence provided by academic studies, including the 2023 study by Bamiatzi et. Al. and others, documents positive effects of CSR on security, namely, the fact that organizations with high CSR scores suffer milder drops in stock price after a breach, and also enjoy faster recovery. Companies like Cisco include security and the raising of security awareness within CSR programs and community education initiatives. By doing so, companies not only can improve information security but also strengthen name reputation. This paper addresses the need for improved information security in light of evidence of underinvestment and delayed disclosure of data breaches. The dual benefits of the CSR security approach are discussed, particularly how security is enhanced while reinforcing social responsibility, especially in community education initiatives. A number of recent incidents, for example, a 2017 software company breach of financial institutions suppliers such as SitusAMC, demonstrate the increasingly relevant nature of corporate responsibility within an enterprise-

wide framework. The proposed framework extends the CSR approach to information security management for an enterprise-wide approach to corporate responsibility.

6. Proposed framework for the alignment of CSR with cybersecurity

For a successful translation of these theories to practice, this paper develops the Cybersecurity-Integrated CSR (CICSR) Framework. This is structured around four pillars, each with measurable components.

Pillar 1: Governance and Ethical leadership.

Board-level oversight of cyber risks is treated as a material ESG matter. This includes: (i) implementing cross-functional CSR-cyber committees; (ii) incorporating security aspects into codes of ethics; and (iii) implementing executive accountability measures. Empirical evidence confirms that the formation of CSR committees after a breach helps mitigate CSIR.

Pillar 2: Risk Management and Technical Excellence.

Principles of security-by design, zero-trust architectures, default-encryption, regular penetration testing, and integration of AI-assisted threat detection with human oversight should be in place. Security measures should be extended to supply chains and third parties. These measures align with internationally recognized standards such as ISO 17799, NIST and NIS2. Shadow AI is a particular concern as it has been linked to higher expected breach costs.

Pillar 3: Stakeholder Engagement and Transparency.

The implementation of clear, easily accessible privacy communications, and timely and empathetic breach notification with a clear road-map is essential. Furthermore there should be tools to assist users in understanding their obligations in the use of technology (such as privacy icons). The development of an internal environment of psychological safety, enabling the reporting of threats and incidents, is also necessary. There are also opportunities to enhance data protection through dialogue with external stakeholders, eg., around the use of surveillance technologies and the use of AI models in data collection and processing. This needs to include impact assessments with all stakeholders in a transparent manner.

Pillar 4: Society contribution and Shared value.

The framework suggests investing in public digital literacy programmes, supporting open-

source security projects such as cover, participating in public private threat-sharing initiatives; and measuring success in terms of privacy and data security (PDS) indices and cyber trust scores.

The contribution to society is expressed in terms of societal impact metrics (eg., availability of digital resources for the most-vulnerable groups) as well as through cybersecurity incident prevention, mitigation and response measures. This framework makes a substantial contribution to the literature and to business practice. In terms of contributions to theory, it enables a more nuanced approach to the debate about the nature of CSR and the relationship between business and society. In terms of practice, it provides a coherent roadmap for the translation of the principles that underpin CSR theory into action.

Implementation of the framework requires the integration of several metrics across these four pillars (for example, the correlation between CSR ratings and frequency/departure of breaches), the establishment of regular audits and cultural change initiatives. In terms of implications, the framework emphasizes the importance of integrating cybersecurity into their strategy and ensuring accountability for both the board and executive management. The framework also highlights the need for a shift in the perception of cybersecurity as a cost center to that to see it as a strategic enabler of responsible business.

7. Implementation Challenges, Best Practices, and Future Trends

Aligning cybersecurity with CSR is not without challenges, and organizational resource constraints are often significant obstacles to realizing value. SMEs lack the resources of the larger corporation. Cultural resistance may assign cybersecurity to the IT department in isolation from the rest of the organisation, and the rapid evolution of threat actor techniques in the wake of increasingly sophisticated AI powered attacks pose real challenges to organisations without legacy data and with a skills shortage. Moreover, there is the problem of 'Cyber-Washing', where organisations give the appearance of being committed to Cybersecurity in a similar way to green washing and risk being targeted by those they perceive to be weak.

Protecting your organization from emergent threats such as Shadow AI must be a top priority. IBM's 2025 Cyber Risk Report found that 20% of breaches involved Shadow AI, resulting in an average of $670,000 more damage per incident. Additionally, 97% of organizations faced with an AI-related security incident had inadequate access controls in place and 63% lacked mature AI governance policies. In addition to malicious insider threats and supply

chain attacks (averaging $4,920,000 and $4,910,000 respectively), organizations must develop a holistic approach to risk management. In the U.S., breach costs, regulatory penalties and detection costs all place significant pressure on organizations. In a rapidly changing threat landscape, ITRC's 2025 report found that there were 3,322 data compromises in the U.S. alone, a record high. These breaches are becoming more frequent and targeted rather than simply 'mega breaches'.

To address these challenges, organisations can employ integration, authenticity and pro-activity. For instance, ensuring comprehensive security training is embedded within an existing CSR remit can capitalize on the psychological safety and social exchange mechanisms at play. Cross-functional decision-making groups consisting of CISOs, CSR leads, in-house counsel and other relevant operations staff are also essential in balancing security concerns with broader ethical and business considerations. This extends to integrating and rolling out third-party audits, penetration testing or the adoption of industry-wide frameworks such as ISO 27001 and NIST guidelines for cybersecurity and privacy. Companies should also 'build security into products by design', such as during the product development stages, and use mechanisms such as trust-enabling tools like transparency platforms (e.g. privacy icons) to effectively communicate its cybersecurity posture and practices to relevant stakeholders.

Leaders must also ensure that cybersecurity investments are properly aligned with other ESG objectives. Adopting energy efficient solutions, such as open-source based security tools, is one example of how this can be achieved. The literature has also shown that authenticity in reporting incidents is key to ensuring that any defensive posturing is perceived positively by stakeholders such as investors or consumers. For SMEs, the pressure to ensure that cybersecurity is properly addressed may actually reduce as collaborative technology platforms and public and private partnerships become more established. Leaders should also keep an eye on upcoming developments as the European Union has proposed a raft of improvements to the NIS Directive in the 2026 amendments known as NIS2.

Looking down the lane, future trends will radically alter the cybersecurity and CSR landscape in the next decade. The confluence of AI and cybersecurity will fundamentally change the nature of defense as a whole. According to IBM, organizations that have implemented significant amounts of AI in their security operations saved an average of $1.8 million against breaches. However, there are also risks of attacks using AI, such as phishing (37%), deepfakes

(35%) or automated adversarial tactics. Moreover, there are risks of "shadow AI" or "ungoverned AI" creating an entirely new surface for attack with 13% of respondents indicating they have been attacked on an AI model or application. As quantum computing emerges as a viable future threat, "harvest now, decrypt later" is already a reality. It is time to act now by moving to post-quantum cryptography and developing an ethical framework for the use of dual-use AI technologies.

Regulatory consolidation will continue to concentrate down on supply-chain and product security issues, including through the forthcoming EU Cyber Resilience Act that will apply to all relevant manufacturers across Europe. Once common framework for minimum NIS requirements is also very likely at a European level (in line with new NIS2 recommendations). Requirements for AI to demonstrate explainability, a significantly upskilled cybersecurity workforce and increased public/private collaboration (including threat information sharing) are also expected to grow in significance. Consideration of environmental factors such as the security-related carbon footprint – particularly where processes are energy-intensive – will also become increasingly relevant, driving the development of what has been termed 'green cybersecurity'.

Future research directions might include: employing a more causal or longitudinal lens to study the relationship between ESG issues and outcomes in different contexts and sectors (such as emerging economies or SMEs); examining the intersections and trade-offs across the ESG pillars, including both short- and long-term effects (using mixed-methods approaches); and advancing research that foregrounds the long-term societal implications of trends in business and management. An interdisciplinary approach that integrates insights from behavioral sciences, ethics, and technological forecasting would also yield important new perspectives.

Business is facing new challenges and trends when it comes to cybersecurity. By integrating Cybersecurity into CSR, businesses can become more resilient and demonstrate future-situational responsibility. By treating cybersecurity as a public good rather than a cost center, businesses can help promote trustworthiness in the digital world and create sustainable competitive advantages in a world fraught with cybersecurity risks.

Conclusion

Cybersecurity is today a form of social responsibility. Data security practices can not only fulfill an ethical company behavior preventing systemic risks and damage to brand reputation but also turn information security into a public good and a common resource, creating value and fostering digital trust. The transformational effect of CSR in the data era can gain momentum by adopting the CICSR Framework, which looks at security from a holistic perspective embedding strong governance, security standards and communication protocols into business practices and inspiring companies to take responsibility towards society while creating opportunities for individual transformation.

As cyber threats evolve with technology, those in policy making positions must evolve as well and implement measures such as improved reporting requirements, better collaborative platforms for information sharing, and more inclusion of small and medium-sized enterprises in global initiatives. Also necessary is a shift in the way business leaders perceive cybersecurity: from a pure defensive investment to one that promotes the health and security of the global citizen.

Aligning digital futures with our best interests is essential to building a safe, just and trustworthy future online.

References

- Bamiatzi, V., et al. (2023). Are the goods spared? Corporate social responsibility as insurance against cyber security incidents. Risk Analysis.
- IBM (2025). Cost of a Data Breach Report 2025.
- Identity Theft Resource Center (2026). 2025 Annual Data Breach Report.
- Khan, W.N. (2025). Is Cybersecurity a Social Responsibility? Information Systems Frontiers.
- Kim, B.J., & Lee, J. (2025). The impact of corporate social responsibility on cybersecurity behavior. Humanities and Social Sciences Communications.
- Rezaee, Z. (2024). Corporate social irresponsibility and the occurrence of data breaches. Relevant journal.
- Additional sources: NIS2 Directive and 2026 amendments, stakeholder theory classics, and case analyses.