SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2026
ORGANIZATION AND MANAGEMENT SERIES NO. 243

CYBERSECURITY AS A COMPONENT OF CORPORATE GOVERNANCE IN ESRS REPORTING: DISCLOSURE PRACTICES IN THE TRANSITION TO MANDATORY CSRD REPORTING

Aleksandra FERENS

Uniwersytet Ekonomiczny w Katowicach; aleksandra.ferens@ue.katowice.pl, ORCID: 0000-0003-2346-9904

Purpose: The aim of the article is to examine how companies, listed on the Polish Stock Exchange in the energy sector disclose cybersecurity issues in Management Board Reports and Sustainable Development Reports before and after the implementation of mandatory reporting in accordance with the European Sustainability Reporting Standards (ESRS 2), "General Disclosures" and "Business Conduct" (ESRS G1). The study focuses on identifying changes in the transparency, scope and quality of disclosures.
Design/methodology/approach: An analysis of the content of the Management Board Reports and Sustainable Development Reports of companies from the energy sector for 2023 **(**the period before the implementation of the CSRD) and for 2024 (the period after the implementation of the CSRD) was used**.** Based on the ESRS guidelines, the company's an author-developed Cybersecurity Disclosure Index was developed**,** covering four areas: Governance, Strategy, Risk Management and "Metrics and Targets".
Findings: The results of the study showed that most of the analysed companies increased the amount and scope of reported information on cybersecurity after the introduction of mandatory ESRS reporting requirements. However, the disclosures still lack several key elements considered essential in this area.
Originality/value: The study contributes to expanding the understanding of governance in social responsibility reporting, encompassing cybersecurity. The study analyzes information security in non-financial reporting before and after the implementation of the mandatory provisions of the CSRD Directive and the ESRS standards. To the author's knowledge, this is the first study in Poland on this topic.
Keywords: cybersecurity, risk management, CSRD Directive, ESRS standards.
Category of the paper: Research paper.

1. Introduction

Global challenges such as environmental pollution, the depletion of natural resources, and biodiversity loss have become urgent realities, requiring businesses to take greater responsibility for their impact on the environment (Nicolò et al., 2024, Szadziewska et al.,

2021). In response to these challenges, the concept of corporate social responsibility (CSR) has begun to play a key role in shaping corporate strategies. Organizations are now assessed not only through their financial performance but also in the context of their environmental, social, and ethical activities.

In parallel with the growing importance of environmental, social and ethical considerations, the modern economy is experiencing a rapid expansion of technology-driven business processes. Contemporary digital solutions provide organizations with significant opportunities for development and innovation, yet they also introduce serious and entirely new types of risks (Strupczewski, 2021). These risks may have financial, economic, environmental and social consequences. Although the original concept of corporate social responsibility primarily focused on reducing the negative environmental impact of business activities and supporting local communities, in the era of digitalization it should also encompass responsible information management, the security of technological processes, and the protection of data. Information collected and processed in cyberspace is exposed to leakage, loss of availability or integrity, and breaches of privacy, which may occur either accidentally or intentionally (Frank et al., 2021). Cybersecurity incidents lead to reputational damage as well as financial consequences resulting from such breaches (Khan et al., 2025). According to the World Economic Forum (2023), cybercrime and the lack of digital security currently rank among the ten most severe global risks in both the short and long term. In the era of digital transformation and the rapid advancement of artificial intelligence (AI), "information" has become one of the most valuable organisational assets, and its protection is a critical condition for maintaining stakeholder trust. Considering the rapid evolution of AI, ethical considerations have become paramount for businesses and are expected to gain even greater significance in the future, particularly with respect to issues such as deprofessionalisation, the responsibility gap and the expectation gap (Arena, Mazzitelli, 2025).

From a CSR perspective, a properly designed and reported cyber risk management system in place within an enterprise, encompassing identification, measurement, assessment, and response processes, not only protects information assets but also strengthens stakeholder trust. This assumption is consistent with the Corporate Sustainability Reporting Directive (CSRD) (2022/2464/EU) and the European Sustainability Reporting Standards (ESRS) developed by the European Financial Reporting Advisory Group (EFRAG). From a corporate governance perspective, cybersecurity is an important category of corporate responsibility, combining social (protecting stakeholder privacy and data), environmental (effective use of IT infrastructure), and management (building trust and organizational resilience) dimensions.

In accordance with the requirements of ESRS 2 and ESRS G1, companies are obliged to disclose information on the policies, processes, strategies and oversight systems that enable effective risk management and ensure information security. These requirements include, among others, the description of internal control mechanisms, incident response procedures, methods for monitoring threats, as well as the links between information security and the corporate risk

management system. In the author's view, an important aspect of this framework is the inclusion of cybersecurity within sustainability reporting structures in line with ESRS requirements. Against this background, the aim of the present study is to assess the scope of cybersecurity related information disclosed in Management Reports and Sustainability Reports before and after the introduction of mandatory reporting under the ESRS, with a particular focus on corporate governance aspects - ESRS 2 and ESRS G1. The study seeks to address the following research questions:

1. To what extent do companies disclose information about cybersecurity risk policies, processes, and systems in their management and sustainability reports?
2. Does reporting in this area meet the requirements of transparency and comparability?

The study is based on a content analysis of the Management Board Reports and Sustainable Development Reports published by companies for 2023 and 2024, during the period of preparation for the implementation of the CSRD and after the implementation of mandatory reporting regulations. The research sample includes selected listed companies from a sector particularly exposed to technological and information risks, i.e. the energy sector. Based on the ESRS 2 and ESRS G1 guidelines, a proprietary Index of Cybersecurity Disclosures has been developed**.** Each Management Board Report and Sustainability Report was assessed in terms of compliance with ESRS 2 and ESRS G1 (0 - no disclosure; 1 - partial disclosure; 2 - full disclosure).

The results obtained will determine the extent to which companies are prepared to report cybersecurity information in accordance with the requirements of the ESRS, as well as identify areas that require further clarification in reporting and regulatory practice. The study contributes to broadening the understanding of governance in sustainability reporting, including the aspect of information security as an integral part of transparency and accountability. This article is up-to-date and innovative, filling the research gap by providing information on the level of compliance of cybersecurity disclosures with the ESRS requirements. To the best of the author's knowledge this is the first article that offers information on the readiness to change companies not covered by the exemptions from the Omnibus Package.

2. Literature review

Growing social pressure on corporate transparency (Agostini et al., 2021), the need to rebuild public trust, the need to harmonize regulations between Member States, and a crisis of confidence in reported financial information influenced the adoption of the NFRD (2014/95/EU) by the European Parliament and the Council of the European Union on 22 October 2014. The directive required large public interest entities to disclose non-financial information regarding the environment, social affairs, respect for human rights,

anti-corruption activities, and corporate governance principles (Cuomo et al., 2024). Corporate social responsibility (CSR) ceased to be a voluntary initiative and became a subject of legal regulation. The directive contributed to an increase in the number of companies preparing and disclosing CSR reports, including their social and environmental performance (Christensen et al., 2021). However, the NFRD had significant limitations: the form and content of reports were voluntary, varied in scope, and inconsistent, and disclosures were incomparable and fragmented. This was due to the lack of a standardized reporting format. Companies could use GRI and ISO 26000 standards, and could publish them as part of their management report or in a separate non-financial report (Sethi et al., 2017). Many companies continued to use non-standard disclosure frameworks, which hindered the assessment of non-financial risks (Ho, 2022). Therefore, the EU introduced more comprehensive reporting solutions – the Corporate Sustainability Reporting Directive. The CSRD covered a broader range of entities subject to the reporting obligation and introduced references to uniform standards – the European Sustainability Reporting Standard (ESRS) developed by EFRAG. CSRD acts as a catalyst for integrating sustainability into firms' business operations and reporting practices, recognizing the interdependence between corporate actions, the regulatory environment, and sustainability goals (Kosi, Relard, 2024). The introduction of the ESRS standards aimed to increase the transparency, consistency, comparability, and verifiability of information regarding environmental, social, and governance issues. The ESRS standards are currently a key tool for implementing CSRD. They consist of ESRS 1 (general requirements), ESRS 2 (general disclosures), and thematic standards (E, S, G).

The roles of supervisory authorities, the process of identifying and assessing significant risks, policies and internal control mechanisms are defined by the ESRS G1 "Business Conduct" standards (Hummel, Jobst, 2024) and ESRS 2. In practice, this means that a company covered by CSRD must describe, among other things, its governance structure, risk identification processes, policies on ethics, compliance, data protection and, although not always explicitly mentioned, cybersecurity management. Due to its capacity and multidisciplinarity, cybersecurity is defined differently in the literature (Schatz et al., 2017). Cybersecurity refers to all actions taken to achieve the postulated state in which the risks threatening operations carried out in cyberspace are minimized as much as possible (Yang et al., 2020). Cybersecurity is the protection of cyberspace, i.e. electronic information, information and communication technologies, and cyberspace users in terms of their personal and social interests, both material and immaterial, who are vulnerable to attacks from cyberspace (Craigen, et al., 2014). The literature emphasizes that cybersecurity is linked to three pillars of corporate social responsibility: economic, environmental, and social. Research (Balboni, Francis, 2024) places cybersecurity within the ESG framework, in which digital trust serves as social capital and cyber resilience as a public good.

Economically, investments in information security systems reduce the risk of data loss, operational downtime, and reputational damage (Jerman-Blažič, 2008). Furthermore, investments in cybersecurity infrastructure (Arcuri et al., 2018) are consistent with corporate responsibility and cyber risk reduction. Information security breaches can lead to significant financial losses related to repairing damage after attacks (replacing devices that were destroyed or damaged by the attack). Another significant threat to companies is the lack of transparent information about the level of security, which can complicate investor risk assessment. This can make raising capital more costly, as investment attractiveness tends to decrease with increasing uncertainty about ESG risk (Healy et al., 2001). Increasingly, investors are considering cyber risk management as a key element of the environmental, social, and governance analyses they conduct when making investment decisions (Sherman, 2020).

In the environmental dimension, cybersecurity supports sustainable development by protecting critical infrastructure from threats resulting from cyberattacks. Technologies such as blockchain and cloud solutions, when used safely and effectively, can reduce the carbon footprint and improve the energy efficiency of IT systems (Fraga-Lamas et al., 2024). Properly designed cybersecurity technology, by optimizing the operation of computer systems, can indirectly contribute to energy savings and mitigate negative environmental impacts. Furthermore, sustainable supply chain management, supported by appropriate cybersecurity practices, can reduce emissions and improve the efficiency of transportation and logistics processes (Litvinenko, 2020). Currently, most decarbonization and CO2 emission reduction strategies are based on digital transformation and the use of intelligent technologies that monitor, manage, and distribute energy.

In the social dimension, cybersecurity strengthens stakeholder trust, protects customer privacy, and is a significant element of an organization's reputational capital (Fan et al., 2023). In the cyber context, "trust" is particularly important for users of computer hardware and software, who expect performance to be consistent with their expectations. Implementing cybersecurity measures, such as protection against data theft and service interruptions, contributes to corporate social responsibility (Morales-Sáenz et al., 2024). Axelton, Chandna's 2023) article also highlights the social responsibility aspects of cybersecurity. According to the authors, responsible data management, respect for privacy, and information protection are not only legal requirements but also a responsibility to society and stakeholders. Shackelford et al. (2016) express a similar opinion, arguing that organizations should treat cybersecurity as a component of CSR to protect their customers and society, for example by securing critical national infrastructure. In the digital world, responsibility for protecting consumer and stakeholder data, ensuring privacy, and maintaining robust cyber defenses is increasingly seen as a direct reflection of an organization's commitment to social responsibility (Khan et al., 2025). However, empirical research indicates that the level of cybersecurity disclosure is low, often general (Fortin, Héroux, 2020). At the same time, international guidelines such as

ISO 27001, NIS 1.2, and ESRS attempt to standardize expectations regarding the scope and manner of narrative (Lam, Seifert, 2023).

Cybersecurity, previously treated as a technical element of IT, should be incorporated into corporate governance and internal risk management processes (Craigen et al., 2014). A growing body of research also points to the need to incorporate cybersecurity into corporate governance. As Morales-Sáenz et al. (2024) point out, digital resilience is a prerequisite for maintaining a sustainable business model, and the lack of appropriate security measures can lead to material risks in financial, environmental, and social dimensions. In the context of corporate risk management, cybersecurity should be considered a strategic risk. Research by Smaili et al. (2023) indicates that effective cyber threat management systems are associated with higher board effectiveness and better corporate governance practices. Kluiters et al. (2023) demonstrates that the quality of cyber governance impacts the market value and risk assessment of companies. Effective cybersecurity policies increase investor confidence and can reduce the cost of capital (Frank et al., 2023). Although the ESRS does not include a separate thematic standard on cybersecurity, this topic is indirectly addressed in, among others, the ESRS 2 "General Disclosures" and the ESRS G1 "Business Conduct" corporate governance framework. The General Disclosures require descriptions of governance, risk roles and responsibilities, internal control systems, and risk identification and response processes. The analysis of the ESRS provisions enabled the author to identify key elements related to cybersecurity that should be disclosed under ESRS 2. The summary is presented in Table 1.

Table 1.
Identification of Cybersecurity Disclosure Requirements in ESRS 2

ESRS 2 GOV-1 (The role of the administrative, management and supervisory bodies)	How the administrative, management and supervisory bodies and senior executive management oversee the setting of targets related to material impacts, risks and opportunities, and how they monitor progress towards them.
ESRS 2 GOV-2 (Information provided to and sustainability matters addressed by the undertaking's administrative, management and supervisory bodies)	How the administrative, management and supervisory bodies consider impacts, risks and opportunities when overseeing the undertaking's strategy, its decisions on major transactions, and its risk management policies, including any assessment of trade-offs and analysis of sensitivity to uncertainty that may be required; and a list of the material impacts, risks and opportunities addressed by the administrative, management and supervisory .bodies, or their relevant committees during the reporting period.
ESRS 2 IRO- 1 (Description of the processes to identify and assess material impacts, risks and opportunities)	Focus(es) on specific areas due to heightened risk of adverse impacts.
ESRS 2 SBM-3 (Material impacts, risks and opportunities and their interaction with strategy and business model(s)	How the material risks and opportunities relate to the undertaking, specifying which risks and opportunities the undertaking reasonably expects could have financial effects, including affecting its business model(s) and strategy, and the reasonably expected time horizons for those effects.

Source: author's own elaboration.

Under ESRS 2 (GOV-1, GOV-2), companies are required to disclose their corporate governance structure, including the roles and responsibilities of management and the supervisory board in setting objectives and managing risks and opportunities. Therefore, corporate social responsibility aspects must also be considered. In practice, this also includes risks and opportunities related to information security, data protection, and cyber threats, if they are deemed material in the double materiality assessment. Furthermore, ESRS 2 IRO-1 and SBM-3 require entities to disclose how they identify and assess material risks and opportunities and integrate them into the company's business model and strategy, which will incorporate CSR aspects.

The ESRS G1 Standard specifies that its objective is to provide an understanding of an undertaking's strategy, processes and performance in conducting business in an ethical and responsible manner. Based on the author's own analysis, several ESRS G1 disclosure requirements were identified as relevant to the area of cybersecurity. These linkages are presented in Table 2.

Table 2.
Identification of Cybersecurity Disclosure Requirements in ESRS G1

G1-1 Corporate culture and business conduct policies	A description of the mechanisms for identifying, reporting and investigating concerns about unlawful behaviour or behaviour in contradiction of its code of conduct or similar internal rules; and whether it accommodates reporting from internal and/or external stakeholders. Details on the establishment of internal whistleblower reporting channels, including whether the undertaking provides for information and training to its own workers and information about the designation and training of staff receiving report.
G1-2 Management of relationships with suppliers	The undertaking's approach to its relationships with its suppliers, taking account of risks to the undertaking related to its supply chain and of impacts on sustainability matters.
G1-3 Prevention and detection of corruption or bribery	A description of the procedures in place to prevent, detect, and address allegations or incidents of corruption and bribery.
G1-4 Confirmed incidents of corruption or bribery	Any actions taken to address breaches in procedures and standards of anti-corruption and anti-bribery.

Source: author's own elaboration.

ESRS G1 regulations require organizations to disclose information regarding the existence of a system for reporting and analyzing legal violations, the operation of internal reporting channels, employee training policies, and procedures for handling incidents of business ethics violations. In the context of cybersecurity, these requirements cover data breaches, cyberattacks, information misuse, and the protection of individuals who report security breaches. Furthermore, ESRS G1 requirements also encompass staff training in responding to irregularities, including digital incidents. In practice, this means that a company can, and indeed should, also include a cybersecurity incident response policy and a description of the structure of data breach reporting channels. This approach strengthens transparency, organizational resilience, and stakeholder trust in the company's management system. Integrating cybersecurity with ESG reporting represents a new dimension of corporate responsibility,

where data protection, compliance with regulations such as the GDPR, and system security are perceived as significant non-financial risk factors.

Although cybersecurity has become a critical component of corporate responsibility and governance in the digital economy, prior research has largely overlooked its role within sustainability reporting frameworks. In particular, there is a lack of empirical studies assessing the compliance of cybersecurity disclosures with ESRS 2 and ESRS G1 requirements, especially in the context of the transition to mandatory CSRD reporting. risks. This study addresses this gap by providing evidence on the scope and quality of cybersecurity disclosures from a governance perspective.

3. Research methodology

Based on prior studies on corporate governance, sustainability reporting, and cybersecurity risk management as well as on the CSRD framework the key analytical constructs of the study were identified. These include cybersecurity governance, cybersecurity risk management and compliance with ESRS disclosure requirements. Following the reviewed literature and the structure of ESRS 2 and ESRS G1 the constructs were operationalized through a set of measurement variables capturing disclosures on policies, processes, oversight mechanisms and the integration of cybersecurity into the corporate risk management system. On this basis a proprietary Cybersecurity Disclosure Index was developed to assess the level of compliance with ESRS 2 and ESRS G1.

Companies from the WIG-Energia index were selected for analysis because the energy sector is a key critical infrastructure sector, meaning entities operating within it are particularly vulnerable to cybersecurity risks. In an era of digitalized operational processes, automated transmission networks, and the use of smart meters, any information security breach can lead to serious economic, environmental, and social consequences. Therefore, disclosures regarding information security management and cyberattack prevention mechanisms are particularly important for stakeholders in this sector, both investors and regulators. Furthermore, energy companies listed on the Warsaw Stock Exchange (GPW) are among the first large public interest entities to be required to report in accordance with the CSRD and ESRS standards.

According to the ESRS 2 and ESRS G1 standards, cyber risk management, data protection, and information security are among the elements of assessing corporate governance and responsible business conduct. Examining companies in the energy sector, where the level of exposure to cyber threats is particularly high, allows us to assess whether these companies reported existing risks before the introduction of the mandatory ESRS, and also to verify whether they are actually implementing the ESRS 2 and ESRS G1 requirements in their reporting practices in the year of mandatory application of the standards. Selecting companies

from the WIG-Energia index also allows for an assessment of the comparability of results, as the index includes entities with similar business profiles. This allows for a more precise capture of changes in the scope of cybersecurity disclosures before and after the implementation of the ESRS.

To assess the scope and quality of cybersecurity disclosures in energy company reports, an author-developed Cybersecurity Disclosure Index was constructed and applied.The index's design was based on an integrated approach, taking into account the requirements of ESRS 2 and ESRS G1. The index's goal was to combine key aspects of both sets of standards into a single framework to showcase companies' cybersecurity disclosures. Four key reporting areas were considered, which, in the author's opinion, best reflect the link between cybersecurity and corporate governance, strategy, and risk:

1. Governance – the system for managing and overseeing cybersecurity.
2. Strategy – the integration of information security with the business model and strategy.
3. Risk Management – processes for identifying, assessing, and responding to cybersecurity risks.
4. Metrics & Targets – disclosure of indicators and information security incidents.

Each area includes specific data points reflecting the information requirements of ESRS 2 and ESRS G1. A total of eight assessment points have been developed, as presented in Table 3.

Table 3.
Cybersecurity Disclosure Assessment Points Based on ESRS 2 and ESRS G 1

No.	Area	Link to ESRS2/ESRS G1	Data point	Refinement
1	Governance	G1-1, GOV 1, GOV 2	Information Security/Cybersecurity Policy and Accountability of Management and Supervisory Bodies	Disclosure of a formal information security or cybersecurity policy
2		G1-1	Incident and breach reporting channels	
3	Strategy	SBM-3, G1-2	Cybersecurity in Business Strategy / ESG	Describe how cybersecurity is integrated into the business strategy and sustainability strategy
4		G1-2, SBM-3	Strategic objectives and plans for information security	Disclosure of measurable information security goals and action plans
5	Risk Management	IRO-1, G1-2, G1-3, G1-4	Process of identification, assessment, response to incidents (cyber risks)	
6		IRO-1, G1-2	Risk management in the value chain (suppliers and subcontractors)	
7	Metrics & Targets	G1-4	Number and nature of cybersecurity incidents	
8		G1-1	Cybersecurity training and awareness of employees	

Source: author's own elaboration.

4. Results

Based on eight data points, we analyzed the content of energy companies' reports for 2023 and 2024 (individual reports, Management Board Reports, and Sustainability Development Reports). Companies that did not prepare a separate Management Board Reports and Sustainable Development Reports were not included. A comparison of cybersecurity disclosures in the 2023 and 2024 reports among ten energy companies listed on the Warsaw Stock Exchange (GPW) shows a clear improvement in both the scope and quality of the information presented. Data coded on a three-point scale (0 - no disclosure, information not included in the report; 1 - partial disclosure, descriptive, fragmentary information; 2 - full disclosure, complete information compliant with ESRB requirements, containing quantitative data or indicators) indicates that the number of items with a value of "0" decreased by as many as 15 cases.

This indicates that in 2024, companies significantly reduced the scope of areas that had previously been entirely disregarded in relation to cybersecurity. In turn, many disclosures previously assessed as partial were expanded and converted into full disclosures (11 such instances in total). This indicates a growing maturity of the reporting approach, consistent with the requirements of ESRS 2 and ESRS G1.

In the 2023 reports, the disclosed information was descriptive and general in nature, often lacking measurable indicators. The most significant gaps were observed in the areas of strategy, risk management across the value chain, and quantitative data. Regarding governance, companies typically referred only to the application of information security principles. They lacked a comprehensive policy framework, clear references to the role of management bodies, and information on dedicated channels for reporting cybersecurity incidents. Among the analysed companies PGE, Tauron, and Columbus presented the most comprehensive disclosures in this area, including the development of ICT systems, efforts to ensure process automation and digitisation, and the implementation of an Integrated Management System and IT infrastructure security principles (particularly within the Distribution and Railway Energy segments). However strategy-related disclosures were generally limited to emphasising the importance of digitisation, ICT system modernisation plans, strengthening infrastructure resilience, and the development of remote customer service solutions. They did not include explicit measurable indicators.

In the area of Risk Management, companies briefly referred to ensuring IT security and compliance with internal procedures, without describing response processes. There were also references to the Integrated Management System and updated security procedures, and descriptions of incident response procedures, resilience testing, and cooperation with national security structures. However, there was no description of incident management.

In the Metrics & Targets area, there were general references to occupational health and safety and ethics related training, but no dedicated cybersecurity specific training. Only PGE reported on regular cybersecurity and data protection training for employees, including e-learning initiatives and phishing simulations.

5. Discussion

Modern organizations operate in an environment where dependence on digital infrastructure creates both new development opportunities and systemic threats (Ciborra, 2007). The effects of cyberattacks damage corporate reputation, violate privacy, and lead to negative financial consequences, which can lead to disastrous consequences for long-term sustainability. Cybersecurity is therefore crucial to all three dimensions of social responsibility. Organizations should consider cybersecurity reporting at every stage of considering sustainability factors, as it is crucial to ensuring the credibility of all nonfinancial reporting.

The results of the survey of companies listed on the Warsaw Stock Exchange in the energy sector confirm that the implementation of ESRS 2 and ESRS G1 has contributed to a shift from a declarative approach to effective, data-driven reporting, particularly in terms of strategy and risk management, including cybersecurity. Our study is consistent with the findings of Fortin and Héroux (2020), who indicate that despite increasing regulatory requirements, the level of cybersecurity disclosure remains low, and information is often general, inconsistent, and poorly comparable. Although the ESRS standards do not explicitly require the inclusion of cybersecurity aspects, companies have begun to present more systematic, transparent, comparable, and transparent information in their SZ and SZR, which better reflects the actual activities, processes, and outcomes related to cybersecurity.

The largest number of new or expanded disclosures in 2024 reports concerned the following areas:

- cybersecurity training and employee awareness (an increase in the number of companies disclosing from 3 to 8) – most companies began presenting specific figures on the types of training, number of participants, and frequency of educational activities,
- incorporating cybersecurity into business strategy and ESG (also an increase from 3 to 8 companies) – detailed descriptions of the integration of cyber risks with strategic planning and value management appeared,
- disclosure of the number and nature of cybersecurity incidents (from 0 to 2 companies) – new, quantitative disclosures indicate the inclusion of metrics and targets in reports in accordance with ESRS requirements,

- risk management in the value chain – an increase from 1 to 3 disclosures, demonstrating the expansion of reporting boundaries. Governance remained consistently high – nine out of ten companies reported this area in 2023, meaning that the implementation of the ESRS did not so much compel disclosure, but rather streamlined and structured its presentation. In total, between 2023 and 2024, the number of "2" scores increased from 4 to 13, representing a more than three-fold increase in the number of full disclosures. The average score on a 0-2 scale increased from 0.48 to 0.78, confirming significant progress in reporting quality. These changes demonstrate that since the ESRS came into force, companies are no longer limiting themselves to laconic statements about the existence of a security policy, but are increasingly presenting specific figures, metrics, and a description of cybersecurity risk management processes.

This means a gradual shift from a narrative and declarative approach to reporting that effectively incorporates metrics, objectives, and strategies, increasing the usefulness of disclosures for stakeholders, including investors and regulators. However, the level of disclosure remains insufficient. However, our research findings differ from those conducted by Hashemi and Ray (2023), who found that many companies still limit themselves to declarative statements such as "we have a security policy", without presenting measurable indicators of effectiveness or the impact of cybersecurity incidents. The author believes that in the context of CSRD and ESRS, there is a need to standardize cybersecurity reporting, such as the number of incidents, the degree of security audit coverage, and the level of employee training, which can become important ESG indicators.

6. Conclusions

The findings of this study indicate a clear transition from narrative and declarative cybersecurity reporting toward disclosures that increasingly incorporate metrics, objectives, and structured descriptions of risk management processes. This evolution enhances the usefulness of sustainability reports for key stakeholders, including investors and regulators. From a regulatory and governance perspective, the results highlight the need for further standardization of cybersecurity disclosures, particularly with regard to indicators such as the number and type of cybersecurity incidents, the scope of security audits, and the level of employee training. Such indicators could serve as meaningful ESG metrics and support greater transparency and comparability across companies and sectors.

Including cybersecurity in sustainability reporting in accordance with ESRS not only increases information transparency but also strengthens the trust of investors and business partners. The regulatory framework for sustainability reporting in the European Union, shaped by the CSRD Directive and the ESRS standards, sets new standards for transparency in

environmental, social, and digital responsibility. Integrating cybersecurity into non-financial reporting is an expression of regulatory compliance and a key element of corporate governance, the disclosure of which is a tool for building trust, credibility, and organizational resilience.

References

1. Agostini, M., Costa, E., Korca, B. (2021). Non-financial disclosure and corporate financial performance under directive 2014/95/EU: Evidence from Italian listed companies. *Accounting in Europe*, *Vol. 19, Iss. 1,* pp. 78-109, doi:10.1080/17449480.2021.1979610
2. Arcuri, M., Brogi, M., Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. *Corporate Ownership & Control*, *15*(2), 70-83, doi:10.22495/cocv15i2art6
3. Arena, C., Mazzitelli, D. (2025). *Critical Considerations on the Ethical Implications of the Artificial Intelligence Integration in the Accounting Field. In The Generative AI Impact:* Reframing Innovation in Society 5.0. Emerald Publishing Limited. doi: 10.1108/978-1-83549-105-820251008
4. Axelton, Z., Chandna, V. (2023). A practical guide to SEC financial reporting and disclosures for successful regulatory crowdfunding. *Business Horizons, Vol. 66, Iss. 6,* pp. 709-719, doi:10.1016/j.bushor.2023.02.006
5. Balboni, P., Francis, K.E. (2024). Data ethics and digital sustainability: Bridging legal data protection compliance and ESG for a responsible data-driven future. *Journal of Responsible Technology, Vol. 18,* doi:10.1016/j.jrt.2024.100099
6. Christensen, H.B., Hail, L., Leuz, C. (2021). Mandatory CSR and sustainability reporting: Economic analysis and literature review. *Review of accounting studies*, *Vol. 26, Iss. 3,* pp. 1176-1248, doi:10.1007/s11142-021-09609-5
7. Ciborra, C. (2007). *Digital technologies and risk: a critical review. Risk, complexity and ICT.* Cheltenham: Edward Elgar Publishing, doi: 0.4337/9781847207005.00007
8. Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining cybersecurity. *Technology innovation management review, Vol. 4, No. 10,* pp. 13-21.
9. Cuomo, F., Gaia, S., Girardone, C., Piserà, S. (2024). The effects of the EU non-financial reporting directive on corporate social responsibility. *The European Journal of Finance, Vol. 30, Iss. 7*. doi:10.1080/1351847X.2022.2113812
10. Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU as regards corporate sustainability reporting (CSRD). doi: 10.15394/jdfsl.2017.1476; doi:10.1002/bse.3911

11. Fan, Q., Chun, D., Ban, Q., Jiang, Y., Li, H., Xu, L. (2023). Mandatory Disclosure of Corporate Social Responsibility and the Quality of Earnings Management. *Sustainability, Vol. 15, Iss. 17,* doi:10.3390/su15171130026
12. Fortin, A., Héroux, S. (2020). Cybersecurity disclosure by the companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *Vol. 19(2),* pp. 73-100, doi: 10.1111/1911-3838.12220
13. Fraga-Lamas, P., Fernandez-Carames, T.M., da Cruz, A.M.R., Lopes, S.I. (2024). An overview of blockchain for Industry 5.0: towards human-centric, sustainable and resilient applications. *IEEE Access*, *Vol. 12,* pp. 116162-116201
14. Frank, M.L., Grenier, J.H., Pyzoha, J.S., Zielinski, N.B. (2023). Implications of enhanced cybersecurity risk management reporting and independent assurance. *Current Issues in Auditing*, *17(1),* P11-P18. https://doi.org/10.2308/CIIA-2022-018
15. Frank, M., Grenier, J., Pyzoha, J. (2021). Board Liability for Cyberattacks: The Effects of a Prior Attack and Implementing the AICPA's Cybersecurity Framework. *Journal of Accounting and Public Policy, Vol. 40, No. 2,* p. 106812, doi:10.1016/j.jaccpubpol.2021.106860
16. Healy, P.M., Palepu, K.G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of accounting and economics, Vol. 31, Iss. 1-3,* pp. 405-440.
17. Ho, V.H. (2022). Modernizing ESG disclosure. *Law Review*, *No. 1.* University of Illinois, pp. 277-338.
18. Hummel, K., Jobst, D. (2024). An overview of corporate sustainability reporting legislation in the European Union. *Accounting in Europe*, *Vol. 21, Iss. 3,* pp. 320-355, doi:10.1080/17449480.2023.2295986
19. Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *Vol. 28, Iss. 5,* pp. 413-422, doi:10.1016/j.ijinfomgt.2008.02.002
20. Khan, W.N., Lee, J.K., Liu, S. (2025). Is Cybersecurity a Social Responsibility? *Information Systems Frontiers, Vol. 27,* pp. 1-25.
21. Kluiters, L., Srivastava, M., Tyll, L. (2023). The impact of digital trust on firm value and governance: an empirical investigation of US firms. *Society and Business Review*, *Vol. 18, Iss. 1,* pp. 1-23, doi:10.1108/SBR-07-2021-0119
22. Kosi, U., Relard, P. (2024). Are firms (getting) ready for the corporate sustainability reporting directive? *Sustainability Nexus Forum*, *Vol. 32, No. 1,* p. 5, doi:/10.1007/s00550-024-00541-1
23. Lam, W.M.W., Seifert, J. (2023). Regulating data privacy and cybersecurity. *The Journal of Industrial Economics*, *71(1),* 143-175, doi: 10.1111/joie.12316
24. Litvinenko, V.S. (2020). Digital economy as a factor in the technological development of the mineral sector. *Natural Resources Research*, *Vol. 29, Iss. 3,* pp. 1521-1541, doi:10.1007/s11053-019-09568-4

25. 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*, *Vol. 16, Iss. 14,* p. 5884, doi:10.3390/su16145884
26. Nicolò, G., Zanellato, G., Esposito, B., Tiron-Tudor, A. (2024). Cultural dimensions and sustainability disclosure in the banking sector: Insights from a qualitative comparative analysis approach. *Business Strategy and the Environment*, *Vol. 33, Iss. 8,* pp. 8086-8101.
27. Non-Financial Reporting Directive (NFRD, 2014/95/EU).
28. Schatz, D., Bashroush, R., Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *Vol. 12, No. 2,* pp. 8-26.
29. Sethi, S.P., Rovenpor, J.L., Demir, M. (2017). Enhancing the quality of reporting in Corporate Social Responsibility guidance documents: The roles of ISO 26000. Global Reporting Initiative and CSR-Sustainability Monitor. *Business and Society Review, Vol. 122, Iss. 2,* pp. 139-163, doi: 10.1111/basr.12113
30. Shackelford, S.J., Fort, T.L., Charoen, D. (2016). Sustainable cybersecurity: Applying lessons from the green movement to managing Cyber Attacks. *University of Illinois Law Review*, *No. 1,* pp. 45-110.
31. Sherman, J. (2020). *Beyond CSR: The Story of the UN Guiding Principles on Business and Human Rights.*
32. Smaili, N., Radu, C., Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*, *Vol. 27, Iss. 4,* pp. 1049-1071, doi:10.1007/s10997-022-09637-6
33. Strupczewski, G. (2021). Definicja ryzyka cybernetycznego. *Nauka o bezpieczeństwie*, *Vol. 135,* pp. 105-143.
34. Szadziewska, A., Majchrzak, I., Remlein, M., Szychta, A. (2021). *Rachunkowość zarządcza a zrównoważony rozwój przedsiębiorstwa.* Warszawa: Instytut Prawa Gospodarczego Sp. z o.o.
35. World Economic Forum - WEF (2023). *The Global Risks Report 2023 – 18th Edition – Insight Report.* Geneva: World Economic Forum.
36. Yang, L., Lau, L., Gan, H. (2020). Investors perceptions of the cybersecurity risk management reporting framework. *International Journal of Accounting & Information Management*, *Vol. 28, Iss. 1,* pp. 1-23, doi:10.1108/IJAIM-05-2019-0022