European Research Studies Journal
Volume XXVII, Issue 4, 2024

pp. 1513-1535

Disclosures on Cybersecurity, Cyber Risks, and Information Security in Non-Financial Reports of Polish Companies

Submitted 10/11/24, 1st revision 25/11/24, 2nd revision 01/12/24, accepted 28/12/24

Bogusława Bek-Gaik[1], Anna Surowiec[2]

Abstract:

Purpose*: The aim of the article is to identify and assess the scope of disclosures on cybersecurity, cyber risks, and cyber threats in the non-financial reports of selected companies listed on the Warsaw Stock Exchange. The subject of the study included the non-financial reports of five selected companies operating in sectors designated as operators of essential services under the Act on the National Cybersecurity System (2018), prepared for the year 2023.*
Design/methodology/approach*: The study employed a method of literature review, and the content analysis of selected non-financial reports in terms of disclosures related to cybersecurity, cyber risks, and cyber threats of companies.*
Findings: *The findings of the study revealed that disclosures related to cyber risks and cybersecurity in the examined companies are relatively limited.*
Practical Implications*: The results of the study complement the research gap of current literature on the non-financial reporting by presenting the examples of Polish non-financial reports.*
Originality/Value*: The research presented in the article contributes to the current literature on non-financial reporting by identifying gaps related to reporting on measures taken to mitigate the risks associated with cyber threats, and is aimed at presenting a critical interpretative perspective.*

Keywords: *Non-financial reporting, disclosure, cybersecurity.*

JEL codes: *M40.*

Paper type: *Research article.*

[1]*AGH University of Krakow, Faculty of Management, Poland,*
ORCID ID: 0000-0003-4982-5356, bekgaik@agh.edu.pl;
[2]*AGH University of Krakow, Faculty of Management, Poland,*
ORCID ID: 0000-0001-6407-7136, surowiec@agh.edu.pl;

1. Introduction

In recent years, significant advancements have been observed in the field of digital technologies. Progressive digitalization presents considerable opportunities but also generates new threats – cyber threats. The annual increase in the number of cyberattacks introduces new risks for organizations. In light of these threats, ensuring the protection of resources has become a fundamental priority for organizations, as any breach of security can have a substantial impact on their reputation, financial stability, and the privacy of affected individuals.

As a result, organizations implement various security policies to counter potential threats. At the same time, a transformation in risk management is occurring, and organizations are forced to adopt new risk management solutions that include modern tools and techniques aimed at effectively countering cyber threats.

The implementation of an effective security system, which should be integrated into the organization's business model, enabling an understanding of the business logic and infrastructure necessary to operationalize this concept constitutes a challenge for many organizations.

The National Cyber Security Alliance, a non-profit organization on a mission to create a more secure, interconnected world, recommends a top-down approach to cybersecurity, in which corporate leadership prioritizes cybersecurity management across all business practices. Undoubtedly, stakeholders are interested in these issues, and this information can primarily be obtained from the rapidly evolving non-financial reports of organizations.

The aim of the article is to identify and assess the scope of disclosures on cybersecurity, cyber risks, and cyber threats in the non-financial reports of selected companies listed on the Warsaw Stock Exchange. The subject of the study included the non-financial reports of five selected companies operating in sectors designated as operators of essential services under the Act on the National Cybersecurity System (2018), prepared for the year 2023.

The authors also sought answers to the questions of whether companies are effectively addressing the issue of cybersecurity and how they are doing so, which seems to be a highly significant topic and of great importance to stakeholders. Integrated reports and the Management Commentary were selected for the case study analysis, as this types of reports are the most appropriate documents disclosing organizations' activities in this area, accessible to a broad range of stakeholders.

The authors are aware that the article has limitations related to generalizing the conclusions to all companies recognized by the legislator as operators of essential services.

2. Literature Review

2.1 Cybersecurity – Theoretical Framework

In the era of advancing digitalization and increasing reliance on information technologies, ensuring security in cyberspace has become one of the key challenges of the modern world. Organizations, regardless of industry or scale, must contend with an increasingly complex and dynamic threat landscape, which includes cyberattacks, data breaches, online fraud, and industrial espionage (Kowalewski and Kowalewski, 2017; Thalassinos *et al.,* 2023; Grima *et al.,* 2023).

Effective management of cybersecurity and information protection therefore requires not only the implementation of appropriate technological solutions but also an understanding of the theoretical foundations of these issues. Central to this is the awareness of cyber risk and the ability to assess the potential consequences of security breach incidents for the organization's operations, reputation, and financial situation (Mikiewicz, 2018).

The topic of cyberspace and the threats associated with it has been known since the advent of the internet, as evidenced by numerous studies by both foreign and Polish authors, such as: K.J. Knapp *et al.* (2009), R. Ottis, P. Lorents (2010), K.T. Smith *et al.* (2011), D.S. Reveron (2012), L.B.A. Rabai *et al.* (2013), D. Schatz, R. Bashroush, J. Wall (2017), L. Gao, T.G. Calderon, F. Tang (2020), L. Yang, L. Lau, H. Gan (2020), K. Lieder (2012), J. Wasilewski (2013), J. Kowalewski, M. Kowalewski (2014), T.R. Dębowski, U. Wrocławski (2018), A. Ferens (2021), A. E. Sawicka, (2022), A. Ferens (2023).

The concept of cybersecurity is defined in many ways, both in academic literature, legal acts, and by organizations dealing with this topic. For instance, according to a dictionary definition, cybersecurity is described as the resilience of networks and information systems to accidental events or malicious actions that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted data, or related services (Hydzik, 2019).

The statutory definition, provided in Article 2, point 4 of the Act on the National Cybersecurity System, states that cybersecurity is "the resilience of information systems to actions that compromise the confidentiality, integrity, availability, and authenticity of processed data or related services offered by these systems" (Babś, 2019).

In the literature on the subject, various perspectives on cybersecurity can be found. M. Matacz and W. Vodickova (2023) defined it as "all actions – methods, procedures, legal solutions – undertaken by the relevant entities in this regard, aimed at ensuring the integrity of collected, stored, and processed information resources, with the goal of protecting them from unwanted, unauthorized disclosure, alteration,

or destruction". According to the definition provided by the U.S. Cybersecurity and Infrastructure Security Agency[3], "cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information".

In turn, W. Filipkowski (2022) highlights that cybersecurity is a challenge for modern states and societies because key sectors of human activity, such as politics, economy, finance, transportation, infrastructure, medicine, and science, are closely dependent on information technologies.

There is no doubt that ensuring cybersecurity is of fundamental importance for the effective functioning of modern states, economies, and societies. As J. Wasilewski (2013) emphasized, cyberspace has become a domain where behaviors and solutions from the physical world are transferred, bringing both opportunities and risks.

Therefore, cybersecurity is essential for protecting critical services, ensuring citizens' privacy, and countering cybercrime. It serves as the foundation of trust in digital technologies and a prerequisite for the continued development of the information society. Ensuring cybersecurity requires a comprehensive approach that encompasses legal, organizational, technical, and educational measures. Close cooperation at both national and international levels is also essential, involving the active participation of both public and private entities.

The concept of cyber risk is closely related to cybersecurity. According to the Financial Stability Board's Cyber Lexicon, cyber risk is defined, for financial risk management purposes, as the "combination of the probability of cyber incidents occurring and their impact". F. Curti *et al.* (2023) described cyber incident as "an observable occurrence in an information system that a) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or b) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not".

This definition aligns closely with private sector initiatives aimed at defining cyber risk, such as ORX's Cyber and Information Security Risk Initiative, which describes it as a subset of operational risk associated with losses arising from digital incidents. These incidents may be caused by internal, external, or third-party actors and include threats such as data theft, breaches of information integrity, damage to technological resources, internal and external fraud, and disruptions to operations. Cyber risk management involves coordinated activities to guide and oversee an organization regarding cyber risk (Mąkosa, 2019).

According to Biener et al. (2015), cyber risk means "operational risks to information and technology assets that have consequences affecting the confidentiality,

[3]*https://www.cisa.gov/news-events/news/what-cybersecurity.*

availability or integrity of information or information systems". The authors categorize cyber risk into four classes: (1) actions of people (e.g., inadvertent loss of data by employee), (2) systems and technology failures (e.g., malfunction of hardware), (3) failed internal processes (e.g., insufficiently defined responsibilities), and (4) external events (e.g., fire).

An integral part of the cyber risk management process is ongoing communication with stakeholders (informing and consulting) and the continuous monitoring and review of risk types and their factors. This aims to identify changes and maintain an up-to-date understanding of the risk landscape (Mąkosa, 2019).

Non-financial reports provide an avenue for organizations to disclose information on cyber risks, cybersecurity, and related concerns. This topic, as emphasized by the authors, is of critical importance since the potential consequences of cyber risks for organizations remain constant. According to Allianz studies (2015), the three most common causes of economic losses due to cyber incidents are reputational damage, business interruption, and liability from personal data breaches.

Additionally, cyber incidents can result in theft of funds, trade secrets, intellectual property, and, in extreme cases, drive companies to the brink of bankruptcy. According to a study by PwC (2018), in the previous year, 44% of Polish companies suffered financial losses as a result of cyberattacks, and 62% experienced disruptions and downtimes in their operations. Additionally, PwC's experts noted that only 8% of Polish companies are considered mature in terms of cybersecurity preparedness (Urban, 2018). Furthermore, statistics from 2020 indicate that nearly 55,000 cybercrime-related incidents were reported.

Information security in contemporary organizations is intrinsically linked to adherence to legal frameworks and the implementation of globally recognized standards and best practices. Among these, the ISO/IEC 27000 series, which focuses on information security management systems (ISMS), holds significant prominence.

The ISO/IEC 27001 standard within this series is central, as it outlines the requirements for the establishment, implementation, maintenance, and continuous improvement of an ISMS tailored to the organizational context while addressing the needs of relevant stakeholders. This standard is essential for organizations striving to protect their informational assets, ensure compliance with regulatory obligations, and uphold trust with stakeholders through structured risk management and robust security measures.

It should be noted that ISO/IEC 27001 requires organizations to implement a series of interconnected processes, starting with the establishment of the context, information security policies, and objectives, through planning and implementing controls, risk assessment, incident management, and concluding with monitoring, reviewing, and continuous improvement of the entire system.

A key aspect of this standard is the risk-based approach – selection and implementation of controls must be preceded by a risk assessment that takes into account the specific context of the organization, legal requirements, and business needs. A certified information security management system can be a significant asset in building a competitive advantage and fostering trust among clients, business partners, and investors (Gałaj-Emiliańczyk, 2022).

Another widely recognized standard is the NIST Cybersecurity Framework[4] (Framework for Improving Critical Infrastructure Cybersecurity), developed by the U.S. National Institute of Standards and Technology (NIST). This framework provides organizations with a flexible and risk-based approach to managing cybersecurity risks, especially for critical infrastructure sectors. It is designed to help organizations improve their ability to prevent, detect, and respond to cyber threats while fostering resilience in their operations.

An important legal act in the European Union is the General Data Protection Regulation (GDPR), which sets strict guidelines on the collection, storage, and processing of personal data to protect the privacy of individuals. GDPR applies to all organizations that handle the data of EU citizens, regardless of their location. The NIS 2 Directive (EU Directive 2022/2555) is a critical part of EU legislation designed to enhance cybersecurity across Europe.

It updates and expands the scope of the original NIS Directive, aiming to ensure a higher and more uniform level of cybersecurity across member states. It applies to essential sectors like energy, transport, health, and digital infrastructure, requiring organizations to take stronger measures to manage and protect their networks and information systems.

In the Polish legal framework, an important legislation regarding cybersecurity is the Act on the National Cybersecurity System of 2018. This law aims to ensure a high level of network and information system security across Poland. In addition to this act, sector-specific regulations also play a critical role in ensuring information security, particularly in areas like finance, energy, and telecommunications, where additional measures are applied to protect sensitive data and infrastructure. These legal frameworks establish clear requirements for cybersecurity practices and incident response procedures in order to reduce risks and enhance resilience against cyber threats in key sectors.

In this context, both international standards such as ISO/IEC 27001 and legal regulations like the General Data Protection Regulation (GDPR), the NIS 2 Directive, and sector-specific laws play a pivotal role. ISO/IEC 27001, for instance, is based on a rigorous risk management approach, ensuring that organizations assess and mitigate cybersecurity risks systematically. Meanwhile, regulations like the

[4] *https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf*.

GDPR, NIS 2 Directive, and sector-specific legislation impose strict requirements on organizations to protect sensitive data, ensure compliance with privacy standards, and guarantee the resilience of critical infrastructure. These laws create a regulatory environment where organizations must adhere to stringent data protection measures, implement robust cybersecurity protocols, and be prepared to respond to incidents effectively.

2.2 Cybersecurity and Cyber Risk in Non-Financial Reports

Disclosure of information on cybersecurity and cyber risk in the context of the above considerations seems essential. The question arises: what and how should be reported, and where (in which report)? Considering the growing regulatory pressure and stakeholder expectations, cybersecurity and data protection issues are becoming an integral part of non-financial reporting.

Information about the approach to cybersecurity management, risk assessment results, descriptions of implemented policies and security measures, data on incidents and breaches, as well as educational and developmental initiatives in this area, should have their rightful place within the structure of non-financial reports.

The concept of integrated reporting is particularly significant in this context, as it emphasizes a holistic representation of an organization's business model, strategy, opportunities, risks, performance, and future prospects, situated within its operational environment and its reliance on various forms of capital (IIRC, 2021). Risk management information within such reports should be articulated in terms of its implications for future value creation, encompassing economic, social, and environmental dimensions (Stubbs and Higgins, 2014).

Furthermore, the Management Commentary serves as another vital reporting framework where organizations can disclose information about risks, including cyber risks, and the corresponding policies for their mitigation. In this framework, details about the organization's approach to cybersecurity management, the results of risk assessments, descriptions of implemented policies and controls, incident and breach data, as well as initiatives for education and development in this domain, should be effectively integrated into the structure of non-financial reports.

In accordance with Directive 2022/2464/EU on Corporate Sustainability Reporting (CSRD), companies are now obligated to prepare ESG (Environmental, Social, and Governance) reports. ESG reporting has emerged as a critical component of corporate sustainability strategies, its importance amplified by increasing regulatory requirements and growing investor expectations.

These guidelines aim to assist organizations in identifying, managing, and disclosing risks and opportunities associated with environmental, social, and governance aspects. Furthermore, the European Sustainability Reporting Standards (ESRS),

developed by the European Financial Reporting Advisory Group (EFRAG), provide a comprehensive framework for sustainability reporting. The ESRS serves as a detailed guide, ensuring organizations adhere to consistent and comparable disclosure practices that address the requirements of the CSRD. These standards are designed to enhance transparency, enable stakeholders to evaluate corporate sustainability efforts effectively, and support informed decision-making processes.

The European Sustainability Reporting Standards (ESRS) are structured into three main categories:

- cross-cutting standards: these standards encompass general requirements and disclosures, defining the principles for data collection and presentation. They serve as a foundation for consistent and comprehensive sustainability reporting across various industries and sectors;
- topical standards (Environmental, Social and Governance standards);
- Sector-specific standards applicable to all undertakings within a sector. They address impacts, risks and opportunities that are likely to be material for all undertakings in a specific sector and that are not covered, or not sufficiently covered, by topical standards. Sector-specific standards are multi-topical and cover the topics that are most relevant to the sector in question.

This dual categorization ensures that organizations address both overarching sustainability principles and the particularities of diverse environmental, social, and governance issues, promoting transparency and comparability in corporate sustainability practices. Additionally, the GRI Standards[5] support the process of preparing an ESG report.

In the context of ESG reporting, understanding the relationship between the Global Reporting Initiative (GRI) guidelines and regulatory frameworks such as the Non-Financial Reporting Directive and the Corporate Sustainability Reporting Directive is critical. The GRI Standards provide a globally recognized framework for voluntary non-financial reporting, enabling companies to disclose material information about their sustainability practices. These standards cover environmental, social, and governance dimensions, offering guidance on transparency and accountability.

On the other hand, NFRD and CSRD are binding EU directives requiring companies to report on sustainability topics. The NFRD introduced mandatory non-financial disclosures for large companies, while the CSRD, which is being implemented progressively, significantly expands the scope and detail of these requirements. CSRD also incorporates alignment with international frameworks, such as the GRI, and introduces the ESRS to ensure consistent and comparable disclosures. The GRI standards are widely regarded as complementary to these directives, offering a

[5] *https://www.globalreporting.org/.*

robust methodology that companies can adopt to meet the disclosure demands of NFRD and CSRD. For organizations subject to these regulations, leveraging GRI guidelines provides a practical tool to align with both regulatory requirements and broader stakeholder expectations in ESG reporting. This alignment helps firms effectively manage and communicate their sustainability strategies. However, the ESG reporting guidelines do not specify requirements regarding the reporting of information related to cyber risk and cybersecurity.

It is undeniable that organizations capable of demonstrating adherence to recognized standards and best practices in cybersecurity – an opportunity facilitated by non-financial reports – gain a significant advantage in stakeholder relations. In the era of widespread digitization and an increasing number of incidents, the ability to adequately protect entrusted informational assets has become a critical criterion for evaluating a company's credibility and responsibility.

Implementing and certifying an information security management system in compliance with the ISO/IEC 27001 standard, or demonstrating full compliance with GDPR requirements, can serve as a strong argument in building trust-based relationships with stakeholders.

The current practice of reporting on cybersecurity and personal data protection among companies listed on the Warsaw Stock Exchange remains highly diverse (Ferens, 2021). While most entities include basic information on these topics in their integrated reports and Management Commentary, the disclosures are often fragmented, general, and difficult to compare.

A common trend is that many companies provide details about various types of risks and the measures they take to mitigate them. The primary reports used to communicate an organization's approach to risk management are the integrated report and the Management Commentary, which serve as platforms to address enterprise risk management comprehensively.

The lack of standardized indicators and metrics to demonstrate the scale and effectiveness of cybersecurity measures significantly hinders stakeholders' ability to assess organizational maturity and performance in this critical area. Key factors contributing to this state include (Ferens, 2021):

- absence of uniform reporting guidelines: companies lack consistent frameworks or guidelines for the scope and format of cybersecurity reporting;
- concerns over disclosing sensitive data: many organizations fear that sharing detailed information about their cybersecurity efforts may expose vulnerabilities;
- challenges in quantifying impact: measuring the outcomes of cybersecurity initiatives is inherently complex and lacks universally accepted

methodologies;
- limited awareness among decision-makers: management teams should understand the importance of comprehensive cybersecurity reporting and its implications for trust and risk management.

These challenges underscore the need for a globally recognized framework or set of best practices to ensure transparency and comparability in cybersecurity reporting across industries. Therefore, developing consistent reporting standards that address both stakeholders' informational needs and the unique sensitivity of the cybersecurity domain appears essential for enhancing the quality and utility of disclosures in this area.

However, a key challenge arises in balancing transparency with confidentiality of information (Kobis, 2015), aiming to both build trust with stakeholders and avoid exposing the organization to additional risks. Excessive transparency when disclosing weaknesses in systems or security incidents may be exploited by cybercriminals, while also negatively impacting the organization's reputation with stakeholders. Therefore, it is essential to develop an optimal reporting model that takes into account these complex and sometimes contradictory expectations and conditions.

3. Methodology

The aim of the study was to identify and assess the scope of disclosures on cybersecurity, cyber risks, and cyber threats in the non-financial reports of selected companies listed on the Warsaw Stock Exchange. The case study method was used.

According to Hartley (2004), case study research “consists of a detailed investigation, often with data collected over a period of time, of phenomena, within their context," with the aim being "to provide an analysis of the context and processes which illuminate the theoretical issues being studied". In this respect, it is important to note that case studies have an important function in generating hypotheses and building theory.

The subject of the study included the non-financial reports of four selected companies operating in sectors designated as operators of essential services under the Act on the National Cybersecurity System (2018), prepared for the year 2023.

The theoretical concepts and existing guidelines regarding reporting information on cybersecurity and cyber risk presented earlier have been confronted with reporting practice in order to answer the question: how the information on cybersecurity and cyber risk is presented in the practice of listed companies. The study analyzed disclosures about the information on cybersecurity and cyber risk in non-financial reports prepared by four capital groups: mBank; Orange Polska Capital Group; PZU Group; ORLEN Group.

Key elements of the disclosure were analyzed, namely:

- Identified cyber risks: the various cybersecurity risks the company faces. These risks could include cyberattacks (e.g., phishing, ransomware), data breaches, vulnerabilities in software and infrastructure, and threats related to employee actions or third-party vendors. The identification of these risks helps stakeholders understand the company's cybersecurity landscape and its preparedness.
- Disclosures on cybersecurity: qualitative and quantitative information about their cybersecurity policies, measures, and strategies, for example: the steps taken to mitigate identified risks, such as investments in new technologies, employee training, or partnerships with cybersecurity providers, information on governance structures, compliance with standards, the role of the board in overseeing cybersecurity.
- Quantitative data on incidents: metrics on cybersecurity incidents, such as the number of attacks, breaches, or downtime caused by cyber incidents, the financial impacts of these incidents, including costs related to recovery efforts, legal fees, and regulatory fines. Providing such quantitative data helps stakeholders assess the scale and impact of the company's cybersecurity challenges.

It should be emphasized that the study is illustrative, the content analysis was used.

4. Research Results and Discussion

The analysis aimed to assess how examined companies address the challenges associated with cybersecurity and risk management, and how comprehensively they communicate their strategies and practices in non-financial reporting. This includes examining whether the companies provide sufficient details on their risk management processes, the security measures they use, and any incidents or breaches that have occurred (Table 1).

Based on the identified material topics from the non-financial reports of the analyzed companies, it is evident which cybersecurity related issues are considered significant from the stakeholders' perspective.

In mBank's Integrated Report, both cybersecurity and the protection of customer personal data hold a prominent position. This is likely related to the increasing importance of electronic services and, consequently, the organization's exposure to internet fraud. Cybersecurity and the protection of customer data are crucial for mBank, as they directly impact customer trust and the bank's reputation. Violations in this area can lead to a loss of trust and significant financial penalties related to legal regulations, such as GDPR. Protection against internet fraud is essential to safeguard both customers and the bank, making cyber risk management increasingly important in today's world.

The process of defining material topics for the Integrated Report of the Orange Polska Capital Group was multidimensional. It involved public opinion research, surveys from individual customers, business clients, and employees. Internal stakeholders identified privacy and data security as critical issues, while external stakeholders highlighted the impact of digital technology on democracy and freedom of expression. This approach reflects a comprehensive understanding of the various concerns surrounding cybersecurity, data protection, and the broader social implications of technology.

The process of identifying material topics for the 2023 Integrated Report of the PZU Group consisted of several stages: updating material topics, internal evaluation of material topics, stakeholder evaluation of topics, materiality matrix, and expert verification.

After expert verification, the significant topics were selected. It is worth noting that, topics related to information security and cybersecurity were identified as material issues within the governance area. This reflects the growing importance of these issues in the context of corporate responsibility and risk management, particularly as cyber threats and data protection regulations continue to evolve.

The process of selecting material aspects to be reported by the ORLEN Group in its 2023 Integrated Report involved both external and internal stakeholders. In the process of selecting material aspects to report in the 2023 Integrated Report, ORLEN Group did not listed issues related to cybersecurity and information security as the material aspect. For the specific 2023 report, ORLEN has focused on topics such as climate responsibility, sustainable development, and governance, which includes elements of digital security and risk management within their sustainability strategy.

The reporting approach to cybersecurity, cyber risk, and information security in non-financial reports is difficult to evaluate due to the lack of established standards for such disclosures. In the integrated report of the mBank Group, cybersecurity and information security are addressed, though spread across various sections. Notably, there is an extensive sub-chapter titled "Security and Privacy," which covers a broad range of cybersecurity aspects and personal data protection. Topics discussed include security policies, data protection (including personal data), cyberattacks, and security education for clients, bank employees, and society at large.

The report details the bank's information security policy, emphasizing that managing information security is a key part of its operations. It also describes personal data protection measures and mentions the relevant regulations governing these activities. The bank's cybersecurity policy is outlined, with specific goals set to ensure high digital security standards. These include goals related to cybersecurity, such as conducting mandatory employee training and public awareness campaigns. Additionally, cybersecurity is one of the five pillars of mBank Group’s strategy,

aimed at ensuring the highest possible security for both clients and employees. However, the report does not provide quantitative data on cyber incidents or abuses in cyberspace, focusing instead on complaints submitted to the Data Protection Office regarding GDPR-related issues.

The integrated report of Orange Polska includes information related to network security, information security (including personal data protection), and cybersecurity. The report highlights the company's CSR pillars, with one of them focusing on a secure network. The organization's strategic plan for 2021-2024 emphasizes cybersecurity as a key area. Orange Polska aims to ensure that the use of new technologies remains free from threats. The company uses AI solutions to detect cyber threats and continuously adapts to evolving cybersecurity trends. Secure usage of new technologies is identified as a societal challenge by Orange Polska.

Additionally, the company defines core competencies that are crucial for achieving business goals, with cybersecurity being one of them. Orange Polska runs educational programs for employees on cybersecurity and places special emphasis on protecting younger users in the digital environment, providing tools and knowledge to ensure safety for children, parents, and guardians. Monitoring by CERT and SOC teams significantly reduces the risk of cyberattacks, which could disrupt both internal and external services and lead to data loss.

Cybersecurity, cyber risk, information security, and personal data security are addressed in various sections of the report. The " ESG Management" (subchapter "Customers and users") chapter includes information on personal data security and network safety. The report also provides data on the number of phishing attempts blocked by CyberShield.

The PZU Group Annual Report contains detailed information on various aspects of security, including information security, personal data protection, and cybersecurity. These details are spread across chapters like "Risks and Opportunities", "Strategy and Perspectives", and "Corporate Governance". A specific subchapter, "Security System" in the "Corporate Governance" section describes the company's security policies in detail. PZU conducts educational programs for its employees focused on information security and cybersecurity. The report also includes many quantitative data on security incidents.

This data covers complaints about PZU's operations filed by external entities to the President of the Personal Data Protection Office (PUODO), as well as data protection violations reported to PUODO by PZU Group entities. The effectiveness of the security management system in PZU and PZU Życie is discussed with numbers such as the number of potential infections blocked, number of blocked connection attempts to send malicious emails, number of high-risk attacks blocked, number of blocked redirects to unsafe resources, number of malicious emails blocked.

Additionally, the report provides the number of security analyses, tests, and system vulnerabilities detected. These quantitative figures are provided for both 2022 and 2023 for comparison.

The 2023 non-financial report of ORLEN emphasizes significant efforts in network security and cybersecurity to ensure business resilience and protect sensitive data. Cybersecurity is integrated into ORLEN's digital transformation strategy, focusing on protecting assets while enhancing operational efficiency. However, the report does not provide detailed information on the identified material topics related to cybersecurity, specific identified cyber risks, disclosures about cybersecurity initiatives, or quantitative data on incidents. This gap in disclosure limits the ability to assess ORLEN's cybersecurity performance and risk management comprehensively.

The review of cybersecurity, information security, and cyber risk reporting in corporate non-financial and integrated reports reveals several general trends:

- *Increasing emphasis on cybersecurity:* All analyzed reports highlight the growing importance of cybersecurity as part of corporate strategies, often linking it to broader goals such as digital transformation, operational resilience, or CSR (Corporate Social Responsibility);
- *Varied levels of detail:* While some companies, like PZU and Orange Polska, provide detailed accounts of their cybersecurity policies, risk management efforts, and quantitative data on incidents, others, such as mBank and ORLEN, offer less granularity, particularly in terms of specific risk disclosures or incident metrics.
- *Dispersed information:* cybersecurity and information security topics are often addressed across multiple sections of reports, making it challenging to gain a comprehensive understanding of their practices without thorough examination.
- *Focus on education and prevention:* Many organizations report efforts to educate employees, clients, and the public about cybersecurity risks, indicating a proactive approach to risk mitigation.
- *Gaps in quantitative data:* Despite growing attention to cybersecurity, reports often lack detailed quantitative data on cyber incidents, vulnerabilities, or the effectiveness of implemented measures, limiting the ability to assess performance or make comparisons.
- *Lack of standardization:* The absence of standardized reporting frameworks for cybersecurity and related risks leads to inconsistent disclosures, making it difficult to compare practices across companies and industries.

In summary, while companies recognize the significance of cybersecurity and related issues, reporting practices vary widely, and the field would benefit from greater standardization and transparency to enhance accountability and comparability.

5. Conclusions

In conclusion, it can be stated that cybersecurity is a complex, multifaceted concept, defined in various ways depending on the perspective taken. In the most general sense, it refers to the resilience of information systems against actions that violate the core attributes of information security, such as confidentiality, integrity, availability, and authenticity. It is crucial to note that cybersecurity encompasses the protection of informational resources, infrastructure, processes, and users in cyberspace from a wide range of threats.

It is of paramount importance for the effective functioning of states, economies, and societies in the era of advancing digitization. It forms the foundation of trust in digital technologies and is a prerequisite for continued development. Therefore, ensuring cybersecurity is a horizontal challenge, requiring a comprehensive approach and collaboration among numerous entities at both the national and international levels.

The role of information regarding cybersecurity initiatives is crucial in promoting and supporting these efforts within business organizations. It should be presented in corporate reports to demonstrate commitment to securing information and managing cyber risks.

These disclosures not only inform stakeholders of the organization's cybersecurity posture but also reinforce its transparency, accountability, and readiness to address emerging digital threats. Including such information in business reports helps build trust with investors, partners, and regulators, while also enhancing the organization's credibility in an increasingly digital environment.

It is essential to supplement and structure of reported non-financial information with details on risk management, as well as to include cybersecurity issues within the business model of the organization, ensuring it addresses the management of cyber risks. This integration will provide several benefits, including increased transparency in the value creation concept, for both the customer and the company's owners. It will also help achieve a competitive advantage, strengthen existing relationships, and build new, long-term relationships with stakeholders.

References:

Act of 5 July 2018 on the National Cybersecurity System (Journal of Laws 2024, item 1077) (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2024 r., poz. 1077).

Allianz. 2015. A guide to cyber risk. Managing the impact of increasing interconnectivity. Cyber Security In An Interconnected World, Allianz Group Economic Research. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Cyber-Risk-Guide.pdf.

Babś, A. 2019. Bezpieczeństwo informatyczne inteligentnych systemów pomiarowych w

świetle ustawy o krajowym systemie cyberbezpieczeństwa. Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej, 62, 59-62.

Biener, C., Eling, M., Wirfs, J.H. 2015. Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 131-158.

Chałubińska-Jentkiewicz, K. 2019. Cyberbezpieczeństwo - zagadnienia definicyjne. Cybersecurity and Law, 2(2), 7-23.

Curti, F., Gerlach, J., Kazinnik, S., Lee, M.J., Mihov, A. 2023. Cyber risk definition and classification for financial risk management. The Journal of Operational Risk, 20.

Dębowski, T.R., Wrocławski, U. 2018. Cyberbezpieczeństwo wyzwaniem XXI wieku. Łódź: Wydawnictwo Naukowe ArchaeGraph Diana Łukomiak.

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, PE/35/2022/REV/1, The Official Journal of the European Union, L 322, 16.12.2022.

Ferens, A. 2021. Cyberbezpieczeństwo i cyberryzyko w raportach zintegrowanych i sprawozdaniach zarządu operatorów usług kluczowych. Zeszyty Teoretyczne Rachunkowości, 45(2), 31-50.

Ferens, A. 2023. Ujawnienie szczególnych obszarów ryzyka w wybranych sprawozdaniach w dobie kryzysu. Zeszyty Naukowe Wydziału Zarządzania GWSH, 20, 23-32.

Filipkowski, W. 2022. Technika i taktyka kontrwykrywcza cyberprzestępstw. In: P. Chlebowicz, P. Łabuz, T. Sajański (Eds.), Antykryminalistyka: taktyka i technika działań kontrwykrywczych, Wydawnictwo Difin.

Gałaj-Emiliańczyk, K. 2022. Wdrożenie systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001:2019. Wydawnictwo ODDK, Gdańsk.

Gao, L., Calderon, T.G., Tang, F. 2020. Public companies' cybersecurity risk disclosures. International Journal of Accounting Information Systems, 38(C), 100468.

GDPR. 2016. General Data Protection Regulation - Regulation (EU) 2016/679, European Parliament and Council of the European Union, Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive), The Official Journal of the European Union L119, 4 May 2016, 1-88.

Grima, S., Thalassinos, E., Cristea, M., Kadłubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital transformation, strategic resilience, cyber security and risk management. Emerald Publishing Limited.

Hydzik, W. 2019. Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych. Przegląd Ustawodawstwa Gospodarczego, 3, 84-87.

IIRC. 2021. The International <IR> Framework. Retrieved from: https://integratedreporting.org/wp-content/uploads/2021/01/InternationalIntegratedReportingFramework.pdf.

Janvrin, D.J., Wang, T. 2019. Implications of Cybersecurity on Accounting Information. Journal of Information Systems, 33(3), A1-A2.

Knapp, K.J., Morris, R.F., Marshall, T.E., Byrd, T.A. 2009. Information security policy: An organizational-level process model. Computers & Security, 28(7), 493-508.

Kobis, P. 2015. Zarządzanie bezpieczeństwem informacji w przedsiębiorstwie - podejście holistyczne. Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług, 117, 113-123.

Kowalewski, J., Kowalewski, M. 2014. Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa. Telekomunikacja i Techniki Informacyjne, 1-2, 24-32.

Kowalewski, J., Kowalewski, M. 2017. Zagrożenia informacji w cyberprzestrzeni.

Cyberterroryzm. Oficyna Wydawnicza PWN, Warszawa.
Lambert, S. 2008. A conceptual framework for business model research. 21st Bled eConference eCollaboration: Overcoming Boundaries through Multi-Channel Interaction, Bled, Slovenia.
Marczyk, M. 2018. Cyberprzestrzeń jako nowy wymiar aktywności człowieka: analiza pojęciowa obszaru. Przegląd Teleinformatyczny, 6, 59-72.
Matacz, M., Vodickova, W. 2023. Rola organów ścigania w zwalczaniu cyberprzestępczości. In J. Kufel-Orłowska (Ed.), Polityka kryminalna a zapewnianie bezpieczeństwa. Cz. 1. Wydawnictwo Naukowe Uniwersytetu Przyrodniczo-Humanistycznego.
Mąkosa, G. 2019. Zarządzanie ryzykiem jako determinanta cyberbezpieczeństwa. Nowoczesne Systemy Zarządzania, 3, 67-80.
Mikiewicz, P. 2018. Cyberbezpieczeństwo jako konstrukt w polskiej przestrzeni publicznej. In: T. Dębowski (Ed.), Cyberbezpieczeństwo wyzwaniem XXI wieku. Wydawnictwo Naukowe ArchaEgRaph, Łódź - Wrocław.
Ottis, R., Lorents, P. 2010. Cyberspace: Definition and implications. 5th International Conference on Cyber Warfare and Security, Dayton, OH: Academic Publishing Limited, 267-270.
PWC. 2018. Cyber-ruletka po polsku. 5. edycja Badania Stanu Bezpieczeństwa Informacji. pwc.pl/badaniebezpieczenstwa.
Rabai, L.B.A., Jouini, M., Aissa, A.B., Mil, A. 2013. A cybersecurity model in cloud computing environments. Journal of King Saud University-Computer and Information Sciences, 25(1), 63-75.
Regulation of the Council of Ministers of 31 October 2018 on the thresholds for recognizing an incident as serious (Journal of Laws 2018, item 2180). (Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny, Dz.U. z 2018 r., poz. 2180).
Sawicka, A.E. 2022. Cyberbezpieczeństwo jako współczesne wyzwanie w zarządzaniu małym i średnim przedsiębiorstwem. Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie, (47), 43-59.
Schatz, D., Bashroush, R., Wall, J. 2017. Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 53-74.
Smith, K.T., Smith, L.M., Smith, J.L. 2011. Case Studies of Cybercrime and the Impact on Marketing Activity and Shareholder Value. Academy of Marketing Studies Journal, 15(2), 67-86.
Stubbs, W., Higgins, C. 2014. Integrated reporting and internal mechanisms of change. Accounting, Auditing & Accountability Journal, 27(7), 1068-1089.
Thalassinos, E., Kadłubek, M., Norena-Chavez, D. 2023. Theoretical Essence of Organisational Resilience in Management. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 133-145). Emerald Publishing Limited.
Von Solms, R., Van Niekerk, J. 2013. From information security to cyber security. Computers and Security, 38, 97-102.
Wasilewski, J. 2013. Zarys definicyjny cyberprzestrzeni. Przegląd Bezpieczeństwa Wewnętrznego, 5(9), 225-234.
Yang, L., Lau, L., Gan, H. 2020. Investors' perceptions of the cybersecurity risk management reporting framework. International Journal of Accounting & Information Management, 28(1), 167-183.

Table 1. *Analysis of the scope of disclosures on cybersecurity, cyber risk and information security*

Company/ Type or report	**Identified material topics related to cybersecurity**	**Identified cyber risks**	**Disclosures on cybersecurity**	**Quantitative data on incidents**
mBank / Integrated Report	cybersecurity; protection of customer data	Listed cyber threats include: • hacking attacks, such as those targeting customers (phishing, vishing, smishing) • attacks directed at the bank's systems, for example, DDoS attacks causing service unavailability • other IT system and application failures	Internal Security Policies: • Information Security Policy • Personal Data Security Policy and Time-Based Personal Data Management Policy • Cybersecurity Policy • Business Continuity Management Policy • Clean Desk and Screen Policy • Social Media Usage Policy • Online Payment Security Policy • Outsourcing Policy Personal Data Protection: • GDPR Package for individual and business clients • GDPR Package for Private Banking and Brokerage Office clients • GDPR Package for corporate clients • GDPR Package for mBank Mortgage clients • GDPR Package for contractors and their employees Security Education: • Cybersecurity courses • Security Academy for bank employees • Educational campaign on cybersecurity Cyber Threat Risk Management: Information Security Management System, managed by the Security	Information on complaints submitted to the Data Protection Office regarding GDPR-related issues

		• consequences of unauthorized access to personal or other protected data	Department, includes: • Security Operations Center (SOC). • mBank CERT team. Security Level Verification: • Security audits; Compliance audits; Advanced security tests; Penetration tests; Comprehensive Red Team tests; Analysis.	

Orange Polska Capital Group / Integrated Report	privacy and data security; impact of digital technology on democracy and freedom of expression	Telecommunication services: • Orange Polska's exposure to cyberattacks Information security: • Breaches of information security, including personal data • Cyberattacks, especially those aimed at stealing personal data War in Ukraine: • Cyberattacks on Poland's critical infrastructure as a NATO member. Revenues and profits: • Identification of new types of fraud accompanying the development	Internal Security Policies: • Information Security Policy in the Management Area • Certified Information Security Management System • Certificate of Compliance with ISO 27018 Requirements • FIRST and Trusted Introducer Certificates for the CERT Orange Polska Personal Data Protection: • Certificate confirming compliance with ISO/IEC 27018: pertains to the Code of Practice for protecting personal data in cloud computing, implemented in the ICS (Integrated Computing Standard) and ICM (Integrated Computing Managed) models • Assessment and mitigation process for impacts on rights and freedoms of data subjects: focused on individuals whose data is processed by Orange Polska, in line with GDPR regulations, ISO 29134:2017 standards, and guidelines from the Article 29 Working Party Security Education: • Education for children on safe Internet usage • Collaboration with the Empowering Children Foundation: Aimed at educating on avoiding digital threats • Educational materials: courses, educational games, lesson plans, and publications • Workshops for children and teenagers: focused on internet safety. • Dedicated website: online safety for children, accessible at www.orange.pl/razemwsieci • MegaMission: a social project for schools, offering a 10-month course for primary school grades 1–3, teaching balance and safety in the online world • Courses for seniors: "My First Smartphone" • Employee training: focused on information security and personal data protection.	Number of phishing attempts blocked by CyberShield

		of new technologies.	Cyber Threat Risk Management: Telecommunications Services • Planning: Development of network and IT systems • Implementation: Business continuity and crisis management plans • Monitoring: Conducted by the CERT and SOC teams • Certification: Compliance with ISO 22301 for the Business Continuity Management System. Information Security • ISO/IEC 27001 Certification: For the Information Security Management System • ISO/IEC 27018 Certification: Code of Conduct for personal data protection in cloud computing • FIRST and Trusted Introducer Certificates: For Orange's CERT team War in Ukraine • Incident Response Teams: Addressing cybersecurity breaches in Orange Polska Revenues and Profits • Comprehensive Cybersecurity Solutions: Enhancing profitability and operational safety Security Level Verification: • based on an internal audit	

PZU Group / Annual Report	information security; cybersecurity	• Risk assessment and personal data protection impact assessment procedure in PZU SA and PZU Życie SA; • Management of anti-malware safeguards • Instruction manual (methodology) for identification and risk assessment of personal data processing; • Cyberattacks are identified as one of the risks affecting the continuity of the organization'	Internal Security Policies: • Information and IT system security protection • Information security procedure • Service provider monitoring procedure (for providers to whom PZU Group has entrusted personal data processing) • IT security risk management procedure • Malware protection management • IT security rules – IT Security Management System • Vulnerability and security testing management principles for IT infrastructure • DLP (Data Loss Prevention) monitoring system • • Classification of information and security levels at PZU and PZU Życie; • • Periodic reporting to the Management Boards of PZU and PZU Życie as regards data concerning DPIA analyses performed • • Rules for managing the IT infrastructure vulnerabilities and security tests; Personal Data Protection: • Data protection officer: who fulfills the responsibilities of both the personal data administrator and the data protection officer (DPO). • Personal data protection procedure: Specifies the principles for processing personal data, regulations regarding access to this data, procedures for handling requests from data subjects, and guidelines for handling incidents. • Principles for secure processing of personal data • Principles for managing the risk of personal data processing • Risk assessment and impact evaluation procedure (for personal data processing) Security Education: • Training for newly hired employees focusing on the processing	• Number of complaints about PZU's operations filed by external entities with PUODO • Data protection violations reported to PUODO by PZU Group entities • Effectiveness of the security management systemin PZU and PZU Życie

		s operations • Among ESG risks, the risk of disclosing personal data and insurance secrets to unauthorized individuals is highlighted	of customer personal data • Educational campaigns addressing topics related to information security and cyber threats, including disinformation • Online meetings with external and internal experts focusing on issues related to social engineering and disinformation. • Information materials on cybersecurity Security Level Verification: • IT infrastructure security tests • Vendor audits in the area of data protection • Process audits	
ORLEN Group / Non-Financial Report	No identified material topics related to cybersecurity	• cyber incidents, particularly in the form of ransomware and data theft, were acknowledged as significant challenges	Internal Security Policies: • Cybersecurity is covered within the governance pillar of Sustainable Development Strategy for 2024–2030 Security Education: • In partnership with the Provincial Police Headquarters, the ORLEN Foundation launched the 'Safe Teenager in the Digital World' project aimed to heighten students' awareness of cyber threats, including cyberbullying	No specific quantitative data on cyber incidents

Source: *Author's elaborations.*