Winter 12-10-2023

Cyber Security and Risk Disclosure: A Literature Review for Theory and Practice

Laura Georg Schaffner
Université de Strasbourg, laura.g.schaffner@em-strasbourg.eu

Patrizia Tettamanzi
LIUC Cattaneo University

Michael Murgolo
LIUC Cattaneo University

Cyber Security and Risk Disclosure: A Literature Review for Theory and Practice

Laura Georg Schaffner[1]
Université de Strasbourg,
Strasbourg, FR

Patrizia Tettamanzi
LIUC – Cattaneo University,
Varese, IT

Michael Murgolo
LIUC – Cattaneo University,
Varese, IT

ABSTRACT

Corporations and SMEs are facing 'new' external and internal pressures, which frequently result in modifications to their corporate governance structures and accounting/reporting systems. Because of the digital transformation, the environment – be it real or virtual – in which these companies operate has experienced significant changes. Business operations are a key and important component of human development all over the world – not only financially – and their influence on societal and environmental conditions as well as their necessary preservation are essentially undeniable. However, these operations increasingly undergo cyber-attacks that dramatically represent true causes of disruptions and breakdowns, eluding international governments' inspection and sophisticated corporate control systems. The concepts of governance, internal control and accountability are critical for the protection of sustainable business activities from cyber-attacks, and their effectiveness is arguably dependent on corporations' ability to govern themselves well and demonstrate accountability to their many stakeholders (across their entire value chain) also in relation to cyber dynamics. This should be accomplished by implementing well-accepted governance system standards that are globally harmonized with 'Environment, Social and Governance' (ESG) reporting and performance measurement tools capable of strategically assessing and evaluating risk exposure and providing

[1] Corresponding author. laura.g.schaffner@em-strasbourg.eu

forward-looking information on a multiple level. Few studies have adequately explored these issues in this defining setting, and due to the contrasting evidence arising from the extant literature, there is still no undisputed identification of effective measurement, reporting and disclosure systems for cyber risk and crime anticipation and/or neutralization.

Keywords: Cybersecurity; ESG; Risk Disclosure; SLNA; Digitalization; Internal Control; Literature Review

1. INTRODUCTION

The digital transformation has revolutionized the way organizations do business in terms of evolving relationship with their customers, which is increasingly shifting towards a digital environment, with the consequent extension in the range of services provided through digital platforms and apps. Moreover, it has affected how the 'internal' management of various business processes has been currently conceived and implemented in a context strictly automated. In this, cybersecurity, accounting and corporate governance are evidently interconnected since the strategic role of the boards in managing cyber risks is, by now, undisputed (Florackis et al., 2023). The issue in analysis is not only relevant in private and corporate settings, but also in the public arena. For instance, several administrations worldwide have considered proposals for strategic policies so to implement and control the national cloud, realizing national strategic poles to migrate data and strategic services of the public administration (Bansal and Axelton, 2023).

A direct consequence of this ongoing transition is the inevitable creation, storage and sharing of a large amount of data. While this data is extremely valuable to companies, it is so also to those who intend to steal, manipulate and exploit it for malicious purposes, with

potentially disruptive consequences for the entire organization (Frank et al., 2021). Hence, cyber risk management and insurance has been placed at the top of the agendas across the globe, accompanied by a growing awareness that this is a problem involving the overall business operations through the value chain, no longer just the information technology (IT) department (Wang et al., 2021; Van der Kleij et al., 2023). In fact, technology will exacerbate inequalities while risks from cybersecurity will remain a constant concern (World Economic Forum – WEF, 2023). Historically, severe fines for data loss are also helping change the cost-benefit assessment around investment in cybersecurity measures, but questions remain around the individual rights to action, damage and compensation in cases of breach. It is, therefore, incumbent on organization to consider the ethics of data collection and usage to minimize reputational considerations beyond regulatory compliance (Arena et al., 2022). Moreover, spurred by both increased cyberattacks and tighter data laws, the voluntary disposal and destruction of personal data may become a stronger priority – with potential environmental co-benefits of minimizing data storage needs. Finally, governments should also develop more appropriate and sophisticated emergency plan to respond to data breaches and violation of privacy to minimize follow-on repercussions. In short, widespread cybercrime and cyber insecurity are ranked among the ten most severe global risks over the short and long term (World Economic Forum – WEF, 2023).

From a regulatory perspective, to support the implementation of appropriate cyber governance systems, there is a multitude of norms and legal frameworks to risk management whose efficacy, however, is yet to be determined (Jiang et al., 2022; Arena et al., 2022). For instance, several national norms and the EU Directive 1148/2016, i.e. Network and Information Security (NIS) Directive, provide a well-defined catalogue of indications to companies about the adoption of technical/organizational measures aimed at preventing and minimizing the impact of

cyber incidents. The application of the NIS Directive is not mandatory for all enterprises (but only for those that perform essential functions in our country); yet, it does play the role of key reference point to look at in order to take care of and assess the adequacy of the organizational set-up in this respect. In addition to this, some relevant international best practices are worth mentioning, which are all converging to identify who, what and how cyber risks should be managed (cf. ISO/IEC 27001, NIST, ENISA, National Cyber Security Framework, ISO 22301, etc.), as well as the necessary compliance with EU Regulation 679/2016 (GDPR), which are increasingly leading to an 'integrated' compliance (Wang et al., 2021; Lam and Seifert, 2023). More internationally, CSA Multilateral Staff Notice 51-347 and the SEC's Commission Statement and Guidance on Public Company Cybersecurity Disclosures (2023) are also worth mentioning since they provided lists of items of interest that might allow for a more effective cybersecurity disclosure assessment (Smith et al., 2018; Fortin and Héroux, 2020; Frank et al., 2023; Lam and Seifert, 2023).

Having said that, the main objective of a corporate risk governance model – and, in particular, of a cyber risk management one – is to provide the board and the supporting C-level executives with a complete, clear and real-time understanding of the state of risk and the measures put in place to protect the organization as well as all the useful information for making strategic decisions to minimize risk and improve the company financial and sustainable performance overall. Hence, the starting point for building this model is represented by the business organization as a whole: through process mapping, all internal processes are identified and analyzed, identifying the strategic ones, the supporting ones and focusing especially on the 'core' or critical ones, i.e., those that drive the operational survival of the organization. In short, the choice and decisions taken by a board of directors to devote the maximum effort to build

appropriate governance systems for cybersecurity to protect the company is not only necessary from a compliance perspective, but it can also be considered an actual strategic and sustainable competitive advantage toward their stakeholders, customers, and the market in response to the challenges today arising from technological change. Yet, several studies reported that cybersecurity information as it is currently produced remains of limited usefulness. Regulators are, therefore, challenged to revisit their disclosure requirements (Fortin and Héroux, 2022). In short, results show that cybersecurity disclosure levels are low (Fortin and Héroux, 2020; Hashemi and Ray, 2023), claiming that, in general, information provided is often not company-specific. Moreover, not all firms provide informative or quality disclosures following a cybersecurity breach event. Yet, in an international context where firms are subject to rising cybersecurity risks, the only way these firms can communicate cybersecurity uncertainty and reduce information asymmetry with external stakeholders is still through cybersecurity risk disclosure (Jiang et al., 2022). That said, ineffective disclosure guidance, as it has been deemed SEC one (Lam and Seifert, 2023), may unintentionally encourage firms to disclose cybersecurity risks regardless of the level of risks. Moreover, from a financial standpoint, disclosing companies generally experience significant negative stock market price effects on account of making new disclosures; hence, rather than viewing disclosure as a positive signal of management attentiveness, investors appear to view it as a cautionary sign (Knechel, 2021).

This systematic literature network analysis (SLNA) is focused on this thorny and timely issue with the objective of viewing at the phenomenon in analysis from an 'ESG'-oriented perspective. To the best of our knowledge, no literature reviews have focused on the role of accounting, risk measurement and disclosure activities relating to cyber threats and security, and their effect on, and interrelationships with, the going concern of companies undergoing the

digital transition. As a result, the purpose of this paper is to assess the state of the art of previous literature on the ability of existing accounting, measurement and disclosure systems to prevent, anticipate, or at least control for future cyber risk disruptions, with the underlying rationale of providing 'forward-looking' information and effectively managing cyber risks as a whole. Furthermore, it intends to recommend future study directions. Indeed, it is now time for businesses to step up their efforts to include and hold responsible for digitally-oriented practices in their strategy, management style, and governance supervision.

This research is organized as follows. First, the material and research technique utilized to perform the suggested literature review are presented, including evidence from the SLNA, CSA, and keyword analysis. The subsequent subsections describe additional methodological procedures and outcomes from the research strategy's first, second and third stages. Following that, the key findings are synthesized, and recommendations for further studies are shown. The study concludes with closing observations for the ongoing debate on cyber governance

2. METHODOLOGY

The SLNA is based on the collection of data deriving from chosen citation databases such as Web of Science, Google Scholar, Scopus and so forth. For the purpose of this study, Scopus was chosen as, due to its comparative largeness, scholarly reliability and document consistency, it represents the most commonly preferred database for these analyses (Strozzi et al., 2017). Moreover, the adoption of the SLNA is also justified by the growing interest of accounting and public policy studies on this specific protocol (Comoli et al., 2023). In **Fig. 1**, the SLNA methodology has been visualized so to give a depiction of the entire research strategy as per the

three steps involved. Specifically, **Fig. 1** presents each specific analysis conducted and provides a summarized reference of the study so to make the overall discussion more accessible.

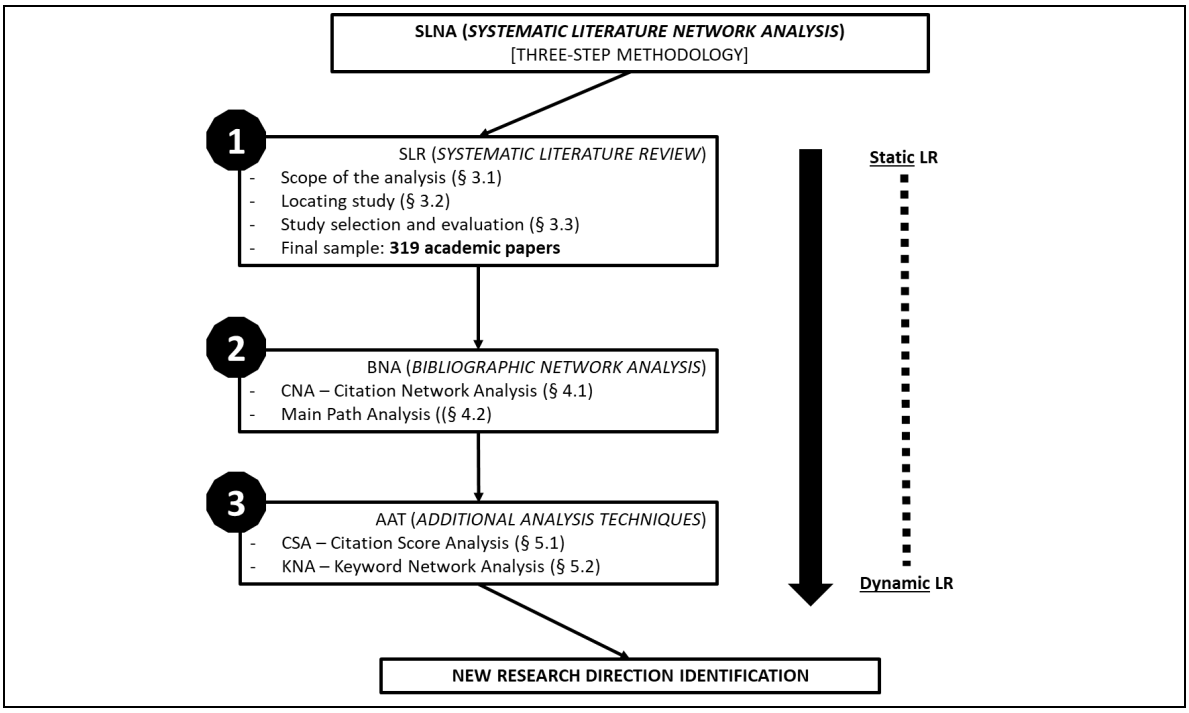

Figure 1. SLNA three-step methodology protocol.

The combined use of the presented methodological tools allows us to avoid the limitations and subjectivity that reside in each of them taken singularly. For instance, a consideration of findings generated solely by citations of papers might be biased since studies that are not cited could be indeed relevant. Conversely, the most cited papers may not necessarily represent those of the highest quality and/or relevance (Strozzi et al., 2017). To conclude this first section, references to the several software applications are deemed crucial. In fact, in order to perform this SLNA – concerning the role of accounting for cyber risks and related disclosure from a governance perspective – the following five AI tools were applied, i.e. VOSviewer, Pajek, Sci2 Tool, GIMP and Scopus analytics.

In the following sections, we will go through the proposed steps again by means of the various AI tools applied and the described protocol as well.

3. FIRST STEP OF SLNA APPLICATION: SLR

3.1. LOCATING STUDY

The concurrent (i.e. 'AND' function) components of the Scopus search string chosen to run the SLNA are (a) ['cyber risk' OR 'cyberrisk' OR 'cybersecurity' OR 'cyber security' OR 'cybercrime' OR 'cyber crime' OR 'cyber incident' OR 'cyberincident'] and (b) ['disclosure']. Each of them was found using the function 'article title, abstract, and keywords' (also known as the 'TITLE-ABS-KEY'). The proposed search string is regarded as optimum since fewer things would have resulted in an extremely big database, but the addition of just one element would have resulted in a significant decrease in the number of articles picked. This option also includes a suitable SLNA based on a sufficient number of publications (Strozzi et al., 2017), highlighting major issues and trends in the research field under examination.

3.2. STUDY SELECTION AND EVALUATION

The article search was carried out in March 2023, spanning almost twenty years. Other Scopus features, such as include or omitting scientific articles from the final dataset, were used to include just the research items deemed relevant and suitable for the scholarship evaluation. As a consequence, 319 scholarly papers were included in the final sample. This collection of papers acts as the SLNA's basis. The most noteworthy research will be identified and then evaluated in the sections and processes that follow.

4. SECOND STEP OF SLNA APPLICATION: BNA

4.1. SAMPLE DESCRIPTION AND STATIC ANALYSIS

In this section, the extracted sample shall be presented as well as the methodological features of the citation network analysis (CNA). At the end of this section, the main results stemming from this specific analysis are offered, leading to the identification of the 'main path'. That said, two perspectives can be mentioned when it comes to analyzing a citation network:

1. Static perspective: analyzing the network as it simply is – some results of which are presented below;

2. Dynamic perspective: conducting, over the identified network, to the main path analysis – this perspective will be investigated in depth in the following paragraph (**Par. 4.2**).

As far as the static analysis is concerned, **Fig. 2** shows that, based on the publishing year, the number of published studies on the topic under investigation increased over the period 2003–2022.

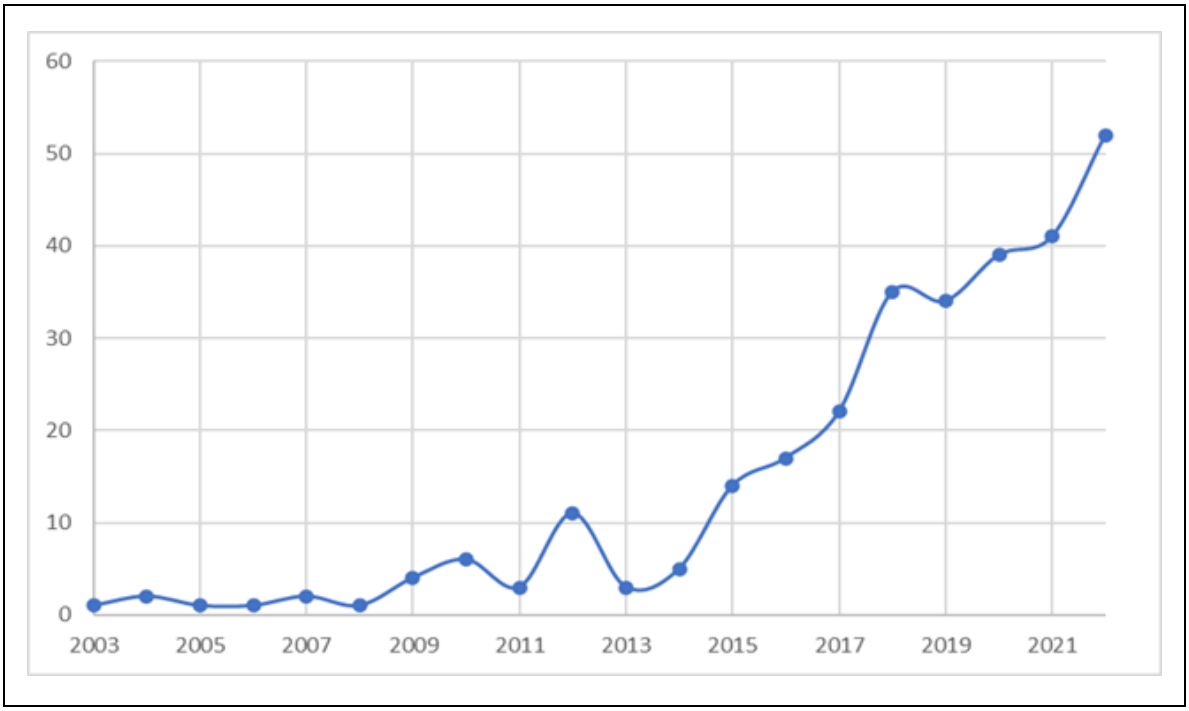

Figure 2. Distribution of 319 scientific studies published in the 2003-2022 time span.

Hence, it may be maintained that this specific research area is in expansion. Though the sample and the analyses carried out include data concerning 2023, this latter year was excluded (i.e. 25 publications) from the depiction since it has not ended yet. Nevertheless, studies published in 2023 will be presented in following sections. In short, the depiction in analysis shows an increasing consideration that the topic under investigation is receiving from researchers, hence justifying this study and its aim of organizing and synthesizing what has been achieved so far in academia, so as to determine possible research avenues and to legitimize deeper investigation in the future.

4.2. DYNAMIC ANALYSIS, MAIN PATH IDENTIFICATION AND STUDY DISCUSSION

The main path, in details, is selected using the Pajek software (Strozzi et al., 2017; Comoli et al., 2023). The main path of the largest identified connected nodes is composed of 23 papers.

The extrapolated papers date from 2018 to 2022, and the most researched topic, pertaining originally to data threat, breach notification, severity assessment and firm response behavior, remains the most researched topic today. Overall, 87% of the linked publications are empirical, relying on both qualitative (e.g., semi-structured interviews, case studies, and content analyses) and quantitative (e.g., longitudinal assessments and bivariate/multivariate non-parametric statistics) research approaches. Only two of these are literature reviews (the most recent was published in 2021), and none of them used bibliometric tools. One study is just a dataset that provides information related to data breaches.

In more detail, the topics – based on the content analysis conducted over it – within the research domain concerning accounting and disclosure for cyber risks and security activities and that constitute the main path are:

a. Cyber risk disclosure and accounting practices: private vs public and voluntary vs mandatory;

b. Data threat, breach notification, severity assessment and firms' response behavior;

c. 10-K disclosure analysis, regulators and market/investment assessment;

d. Audit and assurance role in cyber security, monitoring costs and risk management models;

e. Board of directors' disclosure determinants, IT governance and CIO characteristics;

f. Information sharing and internal auditing/control systems.

5. THIRD STEP OF SLNA APPLICATION: AAT

5.1. CITATION SCORE ANALYSIS (CSA)

One limitation of the main path analysis is that, despite their relevance, certain publications may be left out of the citation network due to a lack of citation links with other research. In other words, the 'main' path ignores publications that are not related to its nodes. As a result, critical material information in the field of cybersecurity disclosure and data governance may be lost. The CNA and GCS's opposite limits are decreased when they are combined.

Due to the multidisciplinary nature of this study, the titles and journals in the tables may appear not to exactly suit accounting research themes (e.g. reporting, disclosure, assurance, etc.). Yet, they all provide evidence pertaining to cyber risks and security from an information sharing and economic/business perspective. Moreover, as per the aforementioned 'pulverization' of

literature on the issue under investigation, only four publications have already been evaluated inside the 'main path' analysis, while the rest of the papers have not.

Overall, a few more topical issues emerge crossing the other extrapolated papers via the computations of GCS, 2019-2023 GLCS, and INCEX, starting from the topics listed before, where the research areas within the domain of data and cyber governance and disclosure pertaining to the main path were indicated. In fact, in addition to, and partially compensating for the previously mentioned study subjects (see **Par. 4.2**), cyber governance researchers have also investigated the following issues (from 2005 to 2022):

a. Cyber and adversarial attacks, ransomware spread detection and authentication protocol in the medical sector;

b. Vulnerability disclosure and reports: timing and signaling information asymmetry;

c. Cybersecurity information sharing, disclosure alliances and politicization in global Internet governance;

d. Cybersecurity economic challenges, financial damage and network data;

e. Internet of Things (IoT) development and security schemes/systems;

f. Human factors, lifestyle routine activities and cyberbullying on social networking sites (SNS);

g. Cyber-insurance policies and risk measurement modelling.

5.2. KEYWORD NETWORK ANALYSIS (KNA)

5.2.1. Co-Occurrence Analysis Of Authors' Keywords

The previous section's GCS analysis findings can be improved by using the authors' keywords network of the collection of articles extracted using SLR approaches, which contains not only the biggest and most linked components, but also the isolated nodes.

The fundamental assumption underlying co-occurrence analysis is that the authors' keywords should serve as a proxy for the substance of the selected articles (Lee and Zhou, 2022).

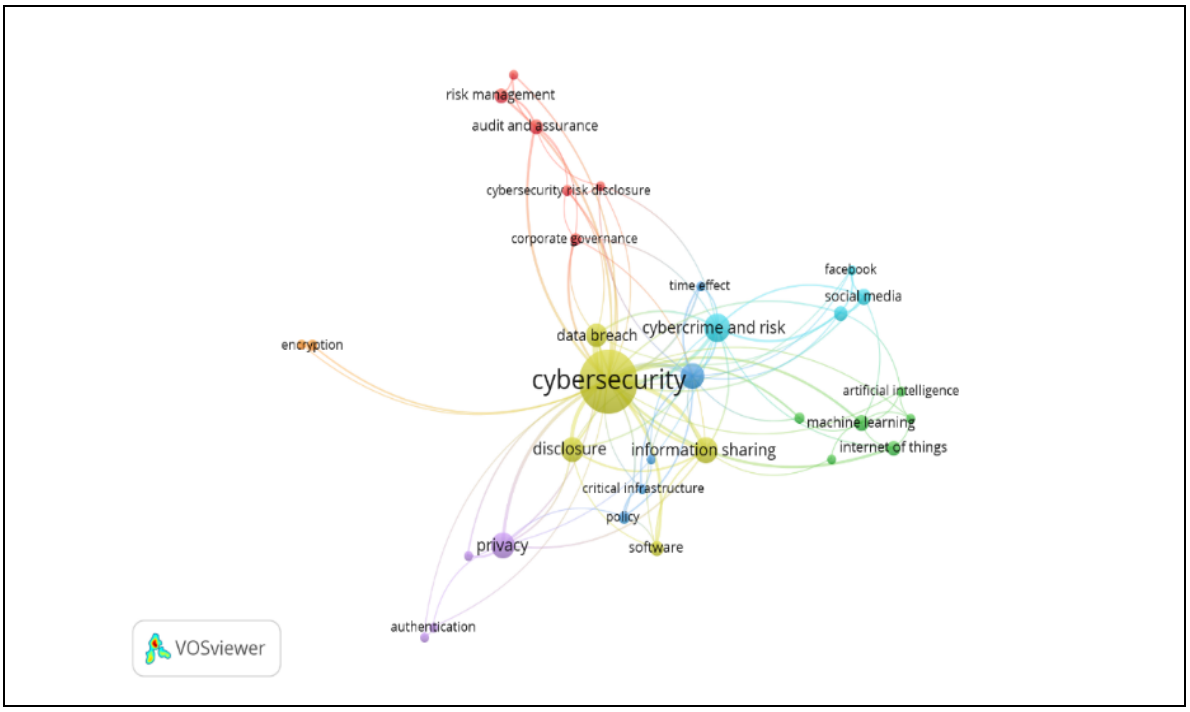

Figure 3. Co-occurrence author keyword network analysis in thematic clusters.

Fig. 3 depicts the results of the test on the keywords used by the Scopus researchers. The VOSviewer software identified 32 keywords and classified them into four major groups. The network nodes correspond to the most commonly used keywords, and the weights of their connections show how many times they appear in the articles. The larger the circle (or node), the more common (and, hence, relevant) the term should be among the research being considered. Furthermore, the different colors visually identify keywords pertaining to one sub-cluster from those related to others, and the size of each node shows the overall connection strength.

5.2.2. Kleinberg's Burst Detection Algorithm

Our final analysis uses the burst detection technique implementation. We found a variety of bursts which signals that something is going on within the research area and that the research

field in analysis is not static. Furthermore, the exact themes investigated by scholars within the research field are changing and evolving in a more structured way. According to the findings of this investigation, early bursts are associated with externalities, anonymity, instant messaging and response when dealing with cybersecurity: this reflects a predominance of the economic, individual or atomic aspects while discussing cyber issues.

For quite a long time (almost 10 years), this tendency characterized research. Bearing this in mind, researchers' focus, then, shifted to more sophisticated topics and problems (such as the social impacts of cyberattacks, vulnerabilities in systems and accessibility) and their related implication at the corporate level beginning in 2015, with a particular emphasis on online spreading, cybercrimes and privacy concerns, emphasizing the importance of developing and implementing appropriate managerial theories to practice as well as appropriate and effective integrated systems and classification. Furthermore, in the context of cyber risks disclosure, the focus has more recently shifted from the atomic idea of cyber issues relegated to the AI department to a more strategic and comprehensive view of the topic under investigation which is now starting to be taken into consideration at corporate governance level due to the critical role of information asymmetry in decision making and the emergence of relevant data breach along the entire value chain. The most recent topical research studies, hence, now attempt to highlight the strategic role at governance level of cyber risks disclosure and security systems implemented.

6. IDENTIFYING NEW RESEARCH DIRECTIONS

Previous tests (such as the 'main path' network, citation scores, and keyword analysis) enabled us to examine the study domain's dynamic evolution, indicating new research trends.

A growing number of studies on cyber security disclosure and data governance have been published, and it is worth noting that academics' emphasis has shifted from general concepts

primarily pertaining to externalities, accessibility issues and response behavior in a broader sense, to more specific, strategic and diverse issues ranging from data breaches and cybercrimes, integrated systems and information sharing, insurance and assurance aspects, ESG implications to corporate governance at large.

All of these are instances of contemporary issues pertaining to the cyber and AI vulnerability world that we must all deal with both at the individual and at the corporate level. More efforts are required to improve cyber risks and security disclosure and eradicate (or, at least, contain) bad practices, unawareness and lack of expertise, and misconduct on multiple levels, as well as to transform cyber risk reporting practices into a forward-looking and anticipatory tool for strategic management and decision making (Walton et al., 2021; Arena et al., 2022; Chen et al., 2022; Comoli et al., 2023; Bansal and Axelton, 2023; Frank et al., 2023). Academic research could, indeed, help reporting and disclosure activities discover the best solutions to the difficulties stated above, determining a definitive paradigm to a distinctive phenomenon characterizing cyber security reporting: on the one hand, data sharing and disclosure reduce information asymmetry; yet, it generally leads to higher chances of corporate data breach and other failures. Hence, more investigation is required. As a result of our tests, the authors believe it is especially important to investigate the following topics:

a. **Data management**: data value, data threat, breach notification, severity assessment, supply-chain attacks, ransomware, business email compromise and funds transfer fraud (FTF) and firm's response behavior;

b. **Role of external parties**: audit and assurance role in cyber security disclosure, monitoring costs and risk management model determination; insurance premium determination;

c. **Recommendations to board of directors**: These look for disclosure determinants, IT governance and important CIO/CISO characteristics;

d. **Managing challenges of distributed systems**: Internet of Things (IoT) development and vulnerability disclosure, big data and blockchain security systems;

e. **Meeting financial authorities' requirements**: E.g., SEC and ESMA requirements for cyber disclosure require the monetary quantification of financial damage, remediation and protection costs, stakeholder compensation, reputation and competitiveness damage; and

f. **Developing methods for ESG implications**: these shall lead to good cyber and data governance practices and social aspects in cyber security.

Beyond our own analysis, these topics have received multiple calls for more research, and their impact is relevant on a worldwide scale (Lam and Seifert, 2023; Aguerri et al., 2023; Comoli et al., 2023; Frank et al., 2023; Bansal and Axelton, 2023). Furthermore, from a methodological standpoint, many academics advocate qualitative and quantitative investigations, highlighting the importance of results that are more accurate as a consequence of interviews, case studies, action research, and experimental designs. However, there is also a shortage of quantitative and empirical investigations in this field of study, analyzing cross-national, longitudinal studies using regression techniques, or even more robust and complex methodology which allow for more sophisticated analysis. To the best of our knowledge, very few studies within the field of cyber security disclosure and data governance have used methodologies such as 'Partial Least Squares – Structural Equation Modelling' (PLS-SEM), Gap and Gephi analysis, 'Causal Mediation' analysis (CMA), scoring grid methodology applications and propensity score matching analysis, and cross-field research among business, management and IT departments, which might result in intriguing theoretical conclusions to adopt in practice as well as in the

actual construction of a solid theoretical framework, beneficial both for theory and real-world processes and activities.

7. DISCUSSION AND CONCLUSIONS

Corporate governance is, once again, increasingly becoming indispensable since the twin (green and digital) transition requires corporations to fundamentally change their mindset, strategies, and objectives (Lankton et al., 2021; Jiang et al., 2022). Society has indeed become increasingly dependent on IT infrastructure and services. Under this new paradigm, businesses should transition from shareholder primacy to stakeholder capitalism, emphasizing less on short-term economic gains and prioritizing shared value. In so doing, they must be able, on the one hand, to produce big data so to effectively confront financial, climate, energy and societal concerns and, on the other hand, to protect their data from cyber-attacks of any kind. This requires aligning corporate initiatives with sustainable development objectives and the most advanced AI tools, deliverable via a transformative corporate governance model. While there is a general agreement on the necessity of an update of corporate governance systems, there is little to no understanding of how such effective corporate governance frameworks could be developed. This systematic literature network analysis (SLNA) tried to address this gap in scholarship by conducting in-depth analyses on extant literature so to further explore, in particular, the state of the art in relation to cyber security disclosure so to, more broadly, provide insights on how businesses can integrate appropriate values of Industry 5.0 pillars (such as big data, cybersecurity, cloud systems and augmented reality) into their corporate strategies and develop measurable indices to assess their progress toward those values as well as protocols to prevent information leakage threats (Smith et al., 2021; Bansal and Axelton, 2023; Frank et al., 2023).

Twin transition is, in fact, the main concern of the European (and, tendentially, international) authorities, and the new watchword that reshapes the activity of companies, but also of other categories of stakeholders considering both the need to protect the environment and promote the low carbon economy, and to take advantage of the opportunities offered by digitalization. The European Union (EU) countries have set well-marked targets for these transitions, driven by the need to manage the challenges posed by climate change and cyber-attacks. Through its efforts to regulate the transition process, the EU is an international leader in a world where the connections generated by globalization are increasingly intense and the need for sustainable restoration is pressing in the new geopolitical context.

In short, the overarching purpose of this literature review is to give a comprehensive assessment of the most recent state of knowledge on cyber risks and security disclosure with an emphasis on practical and policy implications. Furthermore, several prospective future research areas have been indicated. The overall findings show that, despite an increase in the number of research papers published over time, the specific issues pertaining to the cyber disclosure study domain remain important and leave room for future investigation, albeit with a shift in focus to other criticalities (in comparison to the initial related studies). Future research should provide empirically comparable studies across time, settings, and sectors, as well as take into account the realities of small and medium-sized businesses along the entire value chain, with a focus on a qualitative methodological approach (via top management interviews and action research) and a quantitative approach -primarily involving regression techniques and, potentially, SEM-PLS designs. These studies should also consider new data sources, such as annual and online reports, which would allow for triangulation of results, as well as other forms of analysis, particularly qualitative forms, such as case studies, interviews, and surveys, because these methodologies

may provide more robust evidence for practice (Comoli et al., 2023). Furthermore, the impact of the COVID-19 pandemic, climate change, and the energy industry crisis caused by the ongoing Russo-Ukrainian War on the overall prospects of implementing sustainable development practices throughout the value chain, the implementation of the so-called 'twin transition' and, hence, the digital transformation should be examined. The increased dependency of modern society in digital services has, in fact, led organizations in significant investments for administrative and technical countermeasures to prevent accidental or malicious cyber security incidents. That said, the realization of modern cyberattacks and cyber security incidents that result in severe impacts have made evident that organizational cyber security management cannot rely solely on risk mitigation measures. Based on these assumptions, additional research should focus on data governance dynamics, risk disclosure assessment and provision of forward-looking information, effective auditing and assurance protocols – all topics that should make the quality of cyber disclosure more robust and reliable, enhancing the likelihood of success of cyber insurance mechanisms (Frank et al., 2021; Frank et al., 2023; Bansal and Axelton, 2023).

Finally, significant contributions are made by this work. First, it broadens understanding of cyber risks disclosure and governance in the accounting research domain, with a focus on the most recent research trends (such as first COVID-19 pandemic impacts, ESG implications, Internet of Things (IoT) and breach notification). Second, by providing a clear approach and set of criteria, the implementation of a novel strategy (i.e. SLNA techniques) to complete the literature analysis lowers subjectivity (Comoli et al., 2023). To the best of our knowledge, no previous full-scale deployments of SLNA techniques in the domain of cyber security disclosure have been completed, with the presentation of the topical scoping keyword review (TSKR) protocol, ideal for making emerge to what extent some specific issues have (and have not) been

considered by the academic community in a wider research domain. Third, our article suggests how the field of study could evolve in the future. Fourth, it displays the SLNA's ability to perform dynamic studies on a study issue, particularly in a changing environment like cyber security.

To conclude, information and cyber security management is widely accepted as a risk-based process. Following a risk assessment, companies can decide how to manage risks by choosing amongst four strategies: risk modification, risk retention, risk avoidance and risk sharing. In this strategic and governance decision making process, reliability, robustness and quality of disclosure is the necessary (but not sufficient) condition so to take more informed and educated choices at corporate level; yet, organizations are increasingly called upon to compromise, in a continuous asymmetry information pendulum, between the provision of appropriate and effective data for this purposes and the general increase in cyber threat and crimes likelihood. The optimal solution is for future research to be substantiated.

REFERENCES

Aguerri, J., Molnar, L. and Miró-Llinares, F. (2023). "Old Crimes Reported in New Bottles: The Disclosure of Child Sexual Abuse on Twitter through the Case #MeTooInceste". *Social Network Analysis and Mining*, 13.

Arena, C., Catuogno, S., Lamboglia, R., Silvestri, A. and Veltri, S. (2022). "The Disclosure of Non-Financial Risk. The Emerging of Cyber-Risk". Non-Financial Disclosure and Integrated Reporting – Theoretical Framework and Empirical Evidence, *SIDREA Series in Accounting and Business Administration*.

Bansal, G. and Axelton, Z. (2023). "Impact of Cybersecurity Disclosures on Stakeholder Intentions". *Journal of Computer Information Systems*.

Bem, D. (1995). "Writing a Review Article for Psychological Bulletin". *Psychological Bulletin*, 172-177.

Chen, J., Henry, E. and Jiang, X. (2022). "Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach". *Journal of Business Ethics*.

Comoli, M., Tettamanzi, P. and Murgolo, M. (2023). "Accounting for 'ESG' under Disruptions: A Systematic Literature Network Analysis". *Sustainability*, 15.

Cram, W., D'Arcy, J. and Proudfoot, J. (2019). "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance". MIS Quarterly, 525-554.

Florackis, C., Louca, C., Michaely, R. and Weber, M. (2023). "Cybersecurity Risk". *The Review of Financial Studies*. 36, 351-407.

Fortin, A. and Héroux, S. (2023). "Limited Usefulness of Firm-Provided Cybersecurity Information in Institutional Investors' Investment Analysis". *Information and Computer Security*, 31.

Frank, M., Grenier, J. and 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*, 40.

Frank, M., Grenier, J., Pyzoha, J. and Zielinski, N. (2023). "Implications of Enhanced Cybersecurity Risk Management Reporting and Independent Assurance". *Current Issues in Auditing*. 17, 11-18.

Georg-Schaffner, L., Behnam, E. and Pallud, J. (2021). "Cyber Risk Disclosure: How Transparent are CAC40 Companies in their Annual Reports?" *AIM Nice 2021*, 30 Ans.

Jiang, W., Legoria, J., Reichelt, K. and Walton, S. (2022). "Firm Use of Cybersecurity Risk Disclosures". *Journal of Information Systems*, 36.

Lam, W. and Seifert, J. (2023). "Regulating Data Privacy and Cybersecurity". *The Journal of Industrial Economics*.

Lankton, N., Price, J. and Karim, M. (2021). "Cybersecurity Breaches and the Role of Information Technology Governance in Audit Committee Charters". *American Accounting Association*, 35.

Lee, S. and Zhou, Y. (2022). "The Outlook for Sustainable Development Goals in Business and Management: A Systematic Literature Review and Keyword Cluster Analysis". *Sustainability*, 14, 11976.

Romanow, D., Cho, S. and Straub, D. (2012). "Riding the Wave: Past Trends and Future Directions for Health IT Research". *MIS Quarterly*.

Smith, T., Higgs, J. and Pinsker, R. (2018). "Do Auditors Price Breach Risk in Their Audit Fees? ". *Journal of Information Systems*.

Smith, T., Tadesse, A. and Vincent, N. (2021). "The Impact of CIO Characteristics on Data Breaches". *International Journal of Accounting Information Systems*.

Strozzi, F., Colicchia, C., Creazza, A. and Noè, C. (2017). "Literature Review on the 'Smart Factory' Concept Using Bibliometric Tools". *International Journal of Production Research*, 55, 6572-6591.

Van der Kleij, R., Van't Hof-De Goede, S., Van de Weijer, S. and Leukfeldt, R. (2023). "Social Engineering and the Disclosure of Personal Identifiable Information: Examining the Relationship and Moderating Factors using a Population-based Survey Experiment". *Journal of Criminology*.

Walton, S., Wheeler, P., Zhang, Y. and Zhao, X. (2021). "An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions". *Journal of Information Systems*, 35.

Wang, D., Zhou, T. and Wang, M., (2021). "Information and Communication Technology (ICT), Digital Divide and Urbanisation: Evidence from Chinese Cities". *Technology in Society*, 64, 101516.

World Economic Forum – WEF (2023). "The Global Risks Report 2023 – 18th Edition – Insight Report". *World Economic Forum*.