Beyond Regulatory Compliance: Towards a multi-layered responsible cybersecurity perspective

Boineelo R Nthubu
Lancaster University, b.nthubu1@lancaster.ac.uk

Niki Panteli
Lancaster University, n.panteli1@lancaster.ac.uk

Konstantinos Mersinas
Lancaster University, Konstantinos.Mersinas@rhul.ac.uk

Research In progress

Abstract

The paper develops a "multi-layered responsible cybersecurity" perspective as a holistic and collective approach to protecting people, organisations, supply chains and societies. This perspective posits that responsible cybersecurity extends beyond regulatory compliance, to the extent that it encompasses different layers of responsibilities that span across techno-centric, human-centric, organisational (intra and inter) and societal perspectives. Our theoretical development emerges from raw data through an exploratory study that involved qualitative interviews with senior cybersecurity professionals and consultants. The "responsible cybersecurity" perspective generates significant implications. First, it has implications for cybersecurity research in that it provides an integrative and balanced approach to viewing the multiple and diverse stakeholders who might be impacted by potential attacks that expand beyond regulations and the organisation. Second, it has implications for digital responsibility research in that responsible cybersecurity can be viewed from different layers each exposing different stakeholders who may be affected as well as different responsibilities.

Keywords: Cybersecurity, Compliance, Regulation, Responsible, Exploratory Study

1.0 Introduction

With growing digitalisation and the acceleration of digital transformation, cybersecurity attacks are becoming increasingly prominent and are a constant threat to individuals, organisations and societies at large. Such incidents do not just cause unnecessary disruptions to organisations and their business operations, but they also contribute to huge financial and reputational costs to the organisations involved (Safa et al., 2016) and society more widely (Agrafiotis, Nurse et al. 2018). Moreover, cybersecurity is not limited to organisations' employees and end-users, but relates to essentially every individual in digitally advanced societies. A privacy violation of a single individual's personal data can have devastating effects for the wellbeing of that

person; a leak of confidential information or a denial of service due to a ransomware attack can have catastrophic consequences for a company and its employees; consequently, the exploitation of a vulnerability in any of the healthcare, transportation, energy, financial etc. sectors can have catastrophic societal impacts.

Although regulations are needed in order to compel organisations to protect their data and systems from cyber attacks, some cyberattacks are not covered by regulations. Srinivas et al., (2019) reviewed cybersecurity regulations adapted by several federal governments and highlights that there is a tendency to focus on specific industries such as healthcare, homeland security, finance etc. Further, regulations may not be enough to protect an organisation and its business partners in the same supply chain.

Accordingly, in this paper, we posit for the need for developing an understanding of cybersecurity from a responsible perspective, one that goes beyond being compliant. The need for responsible cybersecurity derives from an increased realisation that cyber threats and attacks have implications beyond the individuals and organisations that may be directly affected and impact societies at large. Following from these, the driving question of the study is '*How can organisations move beyond regulatory compliance to a responsible and more holistic cybersecurity perspective?*

In what follows we review relevant literature on the role of compliance in cybersecurity and present literature on responsible digital and the responsible perspective more generally. Following this, we present the research design and methodology of the empirical study and the analytical approach adopted. We then show the findings to-date and broadly discuss the implications of the study.

2.0 Literature Review

2.1 Cybersecurity - Beyond Compliance

Due to the interconnectedness and dependencies on other organisations' services, cybersecurity is no longer a concern limited to isolated organisations or specific sectors. Instead, it impacts every layer of society, from individuals and organisations to supply chains and the society at large. Despite the interconnectedness and spread impact, regulations tend to focus on organisations' internal responsibilities within their sector even though e,g. third party risks come from beyond the sector (Didenko,

2020). Further, Srinivas et al (2019)'s review of federal government regulations in cyber security has shown that regulations leave out some sectors. These regulation challenges means that compliance can leave gaps in security and organisations cannot rely on compliance alone to protect themselves and their supply chains. A compliant organisation may still have vulnerabilities that aren't covered by regulatory standards (Marotta and Madnick, 2020). Although essential, compliance can be incomplete when it comes to providing comprehensive protection (Harris and Martin 2021). Additional proactive measures are needed beyond what regulations mandate (Harris and Martin, 2021). In light of this, Didenko, (2020) highlight the necessity for what they call a "*cross-sectoral"* cybersecurity framework to address risks that extend beyond industry sectors. Similarly, Tropina and Callanan, (2015) emphasise the importance of self-regulation to augment the limitations of regulations in cybersecurity. Together, these studies emphasise the importance of moving beyond compliance which has an "organisation" focus, towards a holistic framework that encompasses different layers and scope of responsibilities.

2.2 The Responsible Perspective

Researchers interested in the promoting a responsible perspective in the digital era often highlight ethical concerns such as the reinforcement of existing bias, lack of transparency whilst proposing an urgent need for regulation (Trocin et al, 2023). Within this body of literature, digital responsibility is viewed as the ethical and accountable use of digital technologies, including, ethical decision making, online behaviour, and protecting one's privacy and security (Zhang and Hon, 2020) with other researchers referring to a perspective that is ethical, sustainable, and respectful of human values and society (Pappas et al., 2023). Reasons for adopting a responsible perspective includes a need to promote fairness and equality in the design, implementation and use of digital technologies (Trocin et al, 2023), as well as a need to minimize any potential negative impacts on users' wellbeing and the society in general (Dignum, 2019), and benefit multiple-stakeholders (Pappas et al. 2023). Pappas et al (2023) argue that digital initiatives need to be designed and implemented in a way that benefits multiple-stakeholders. They posit that the value of such digital initiatives should be both co-created and shared. The expectation is that when digital (and other) initiatives are built on responsible principles negative outcomes are

avoided whilst individuals, organisations and societies experience great positive impacts (Dignum, 2019).

3.0 Research Methodology

We carried out a series of semi-structured interviews with cyber leaders and other members of the senior management team to explore understandings and attributes of responsible cybersecurity and the role of the organisation and cyber leaders in promoting this cybersecurity perspective. Interviewees were encouraged to share their understanding of responsible cybersecurity and contribute towards the co-design of a framework for fostering a responsible cybersecurity mindset. Sample interview questions included: *In your view, what are the fundamental principles (dimensions) that responsible cybersecurity should encompass? What challenges does your organisation face in adhering to the fundamental principles of responsible cybersecurity? Are there specific opportunities or best practices that contribute to fostering a responsible cybersecurity approach?*

In total, 20 interviews were conducted and included 15 male and 5 female participants who held leadership positions in cybersecurity e.g Directors, Chief Information Security Officer (CISO) etc. The participants were chosen because of their responsibility in managing and directing cybersecurity operations. Our participants represented a range of sectors including finance, IT, transport, consultancy and government. Their experience in the cybersecurity sector varied from 5 to 30 years. The duration of the interviews which took place online (via Teams) was between 25 to 70 minutes and they were all audio recorded and transcribed. NVivo was used for data analysis as it enabled systematic coding, organisation and retrieval of data. We followed the approach outlined by Gioia, Corley, & Hamilton (2013) to discover the dimensions of responsible cybersecurity, which we later named "layers", and how to foster responsibility in each layer.

4.0 Findings

The findings reveal that responsible cybersecurity requires a collective commitment where all stakeholders act as stewards, not only of their data but also of their supply chain and the broader wellbeing of individuals and society. The interviews highlighted five core layers of responsibility: **techno-centric**, focusing on

technological defenses; **human-centric**, emphasising security solutions designed with users in mind and safeguarding the wellbeing of security professionals; **intra-organisational**, stressing the role of team collaboration and leadership buy in, in promoting a strong security culture; **inter-organisational**, concerning the security of supply chains and third-party partners; and **societal**, recognising the ethical implications of security solutions on a broader societal scale. This multi-layered approach emphasises the scope of responsibilities beyond the organisation and compliance.

5.0 Implications and Potential Contributions

We are currently at the stage of further analysing the data. At the time of writing, we expect at least two theoretical contributions to derive from the study: First, it provides an integrative and balanced approach of not only different views that can be represented in the responsibility domain but also the multiple and diverse stakeholders who have an interest in cybersecurity and who may be affected by potential attacks. This approach confirms that compliance is not enough for ensuring robust cybersecurity in organisations. Second, it expands literature on responsible digital and digital responsibility by showing that responsible cybersecurity can be viewed from different layers each exposing different stakeholders who may be affected as well as different responsibilities. Further, the study provides opportunities for practical implications and in particular for decision-makers and organisational leaders who can be encouraged to identify security practices for not just their own organisation but for peer organisations, entities in the supply chain, and the broader security ecosystem.

6.0 Future Research Directions

While the current study has made significant progress in exploring responsible cybersecurity, several key research activities remain to be undertaken to enhance the understanding of responsible cybersecurity. First, we plan to conduct a co-participatory workshop with senior cybersecurity professionals to further develop a responsible cybersecurity framework. Following this, additional qualitative coding and validation of emerging themes will be necessary to refine the resulting framework.

References

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1-15.

Dignum, V. (2019). Responsible Artificial Intelligence*: How to Develop and Use AI in a Responsible Way*. Springer International Publishing. https://doi.org/10.1007/978-3-030-30371-6.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational research methods*, *16*(1), 15-31.

Harris, M. A., & Martin, R. (2019). Promoting cybersecurity compliance. In *Cybersecurity education for awareness and compliance* (pp. 54-71). IGI Global.

Pappas, I. O., Mikalef, P., Dwivedi, Y. K., Jaccheri, L., & Krogstie, J. (2023). Responsible Digital Transformation for a Sustainable Society. Information Systems Frontiers, 1-9.

Marotta, A., & Madnick, S. (2020). Analysing the interplay between regulatory compliance and cybersecurity (Revised).

Trocin, C., Mikalef, P., Papamitsiou, Z. *et al.* Responsible AI for Digital Health: a Synthesis and a Research Agenda. *Inf Syst Front* 25, 2139–2157 (2023). https://doi.org/10.1007/s10796-021-10146-4

Tropina, T., & Callanan, C. (2015). *Self-and co-regulation in cybercrime, cybersecurity and national security* (p. 25). Heidelberg: Springer.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442-451.

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, *2016*(2), 15-18.

Srinivas, J., Das, *A.* K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, *92*, pp.178-188.

Zhang, J., & Hon, H. W. (2020). Towards responsible digital transformation. *California Management Review Insights*.