IS and Cybersecurity Practice: avoiding self-sabotage

Peter Bednar[1,2], Christine Welch[3] and Moufida Sadok[4]

[1] *University of Portsmouth, School of Computing, Portsmouth, United Kingdom*
[2] *Lund University, Department of Informatics, Lund, Sweden*
[3] *University of Portsmouth, Portsmouth Business School, Portsmouth, United Kingdom*
[4] *University of Portsmouth, School of Criminology and Criminal Justice, Portsmouth, United Kingdom*

Abstract

In this paper, we explore cybersecurity from a sociotechnical work-system perspective and focus on the visibility and effectiveness of security practices as part of the everyday work practices of typical employees. The empirical inquiry involved 471 employees from 259 different organizations, drawn from both private and public sectors using semi-structured interviews and conducted from an interpretive stance. Employees interviewed were all expected to follow cybersecurity practices but were not involved in the development of such. The key findings reveal that actual work practices and routines of most employees were either ignored or insufficiently intertwined with security management efforts. Consequently, engagement and participation by professionals are needed to promote the design of work systems that are not only user-friendly but also genuinely supportive of meaningful use in context.

Keywords

Cybersecurity Practice, Sociotechnical, Information Systems, Work-system, Sustainable Cybersecurity

1. Introduction

It is widely recognized that cybersecurity is not only a technical issue and that a socio-technical perspective is necessary to both illuminate the causes and facilitators of compliance with security policies and regulations. However, research in information security suggests that information security is often viewed as an overlay on top of other tasks and responsibilities. A plethora of examples in the literature shows that when security processes are designed outside of the real-world organisational context are prone to undermine effective organisational practices and create unintended consequences in the operation of work systems.

This paper emphasizes the importance of a better understanding of the role and application of security functions in situated practices. It aims to explore the applicability and the relevance in practice of available security measures and to present empirical results exemplifying challenges related to cybersecurity from employees' perspective.

The remainder of this paper is organised as follows: the next section presents the background research. Section three focuses on past research related to cybersecurity. Section four summarises the research method and design and provides details about data collection process and data analysis method. Section five presents the key findings of the empirical study which illustrate significant areas of concern in security practices. The final section discusses the results and draws some conclusions.

2. Background

Proceedings STPIS2023: Proceedings of The 9th International Conference on Socio-Technical Perspectives in IS, October 27-28, Portsmouth, UK

peter.bednar@port.ac.uk (P.Bednar); christine.welch@port.ac.uk (C. Welch); moufida.sadok@port.ac.uk (M. Sadok)

0000-0002-3631-2626 (P. Bednar); 0000-0002-7149-3354 (C. Welch); 0000-0003-2981-6516 (M. Sadok)

At one time, organizational management was viewed by researchers as a challenge of bringing together optimal resources in order to achieve some predefined objectives [38, 36]. However, in more recent times, it has been recognized rather as an exercise in maintaining or enhancing the organization's position amid the various forces operating upon it from its environment [39, 11, 12, 7]. An organization can be viewed as an open system in which many human and non-human elements interact [6, 11, 14, 20]. At every level, organizational actors will be making sense of their situations while interacting and co-creating their contextually- dependent roles. Many and varied norms and objectives will emerge in different parts/levels of the organization [6, 11]. While it would be possible to conceive of professional, business activities as constituting a system to be served by another system of technical resources, such a mental model is inadequate in practice as a reflection of organizational life as it is lived. Clearly, design of any serving system would depend upon the conception of a system to be served [6, 7, 10]. When such a system is itself perceived as continually (re-) creating itself in response to evolving contextual dependencies, it follows that coevolution of these two perceived systems would be imperative [3, 4, 7]. Once this is accepted, the shift to a sociotechnical mental model is essential, i.e. one in which organizational systems are viewed as emerging through interactions among actors in their professional roles, and using relevant technologies, within an organization's social and organizational context [15, 24, 34].

It has long been recognized that the apparent epistemological divide between business organization and an associated information system represents a false dichotomy [20]. In the age of M-commerce, and as we move from Industry 4.0 into the realms of Industry 5.0, in which products are routinely customised to individual client requirements, and sales must address a target market of one, most managers would recognize that digital resources are fundamental to the business [8]. Yet even today, when the overwhelming majority of organizations depend upon both connectivity and instant availability of data, the perception persists that developing and managing these resources is best left to technical experts.

For many years, researchers have been pointing out that IT services are only useful in conjunction with embedded competences of staff throughout the organization [27] and that attention needs to be paid to whole work systems in which communication and information technologies will be situated [31]. Recognition does emerge among researchers in technical spheres that challenges extend beyond their domain. For instance, research relating to digital innovation may acknowledge that attention must also be paid to process innovation [26]. However, this continues to ignore the indivisible relationship between design of any technological system and its system for use [25]. The pervasive nature of digital resources in the current age has led to a change in focus from innovation projects to 'digital transformation', which goes some way to signposting a more holistic perspective. Jiang [19], for example, suggests moving from a project-based to a programme-based approach to transformation, and points out the pitfalls when moving from strategic to operational levels of attention that management may become fragmented between different areas of an organization. When dealing with external threats to business prosperity, resilience may depend upon a whole system view. For instance, in a study of resilience following the recent pandemic, Saleh Al-Omoush, Simón-Moya, & Sendra-García [33] suggest that: "*Achieving e-business proactiveness requires investment in social capital and collaborative knowledge creation to respond to … crises*" (2020, p.286).

3. Cybersecurity

ISO/IEC 27032:2023 defines cybersecurity as the protection of privacy, integrity, and accessibility of data information in Cyberspace, a complex environment, resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it. Efforts to ensure the security of an information system in use may be seen as an instance of intentional organizational change, where that change is both endemic and continuous. The system must be designed so that the variety in its behaviour can match the variety in its environment [5], and this will itself be in a state of continuous change. The multiple dimensions of connectivity, which transcend traditional organizational boundaries, will mean that the system for use of any information technology must be designed to be flexible and responsive to evolving threats. There is no opportunity to stand back and consider how best to tackle particular issues, as situations move on quickly and delay may be disastrous. It must, instead, be possible for human and technological aspects of the system to coevolve to meet new challenges, as both work patterns and environmental threats change. In this way, the need for proactive, as well as reactive security measures can be anticipated [30].

There are many forces outside the boundary of an organizational system that challenge its ongoing stability and prosperity. In recent decades, these challenges have included a rise in cybercrime and other types of cyber loss. This could mean security or data breaches, attacks by hackers, employee errors, industrial espionage, and ransomware. Such cyber incidents are becoming increasingly prevalent and costly, and are the inverse image of the increasing dependence upon connectivity and digital transformations of organizations. Business continuity and sustainability may be threatened by these threats, and reputation damage may be very costly. The Allianz Risk Barometer for 2023 [1], which consults risk managers in some 94 countries, highlights business interruption and supply chain disruption, together with cyber incidents as the top areas of concern in business, with 34% of votes each, reflecting the importance of the digital economy. Moreover, the consequences of cyber incidents may not be limited to financial loss, as the recent data breach relating to the Police Service for Northern Ireland has illustrated [18].

However, as Perozzo, Zaghloul and Ravarini [28] point out in relation to SMEs, organizations can struggle to achieve a satisfactory level of readiness to address cyber issues. While many recognize that everyone involved has a role to play in cybersecurity, and experts providing advice may suggest a sociotechnical approach, attention still seems to focus on technologies and technical expertise. McEvoy and Kowalski [22] suggest that problems arise because of '*degradation in working practices over time'* (p.48) and offer an ethnographic approach that maps cybersecurity threats against '*poor working practices'*. However, there may be a danger here that actors struggle to identify which are the '*poor'* practices involved, and by the time an ethnographic analysis has been completed to produce a relevant map, both the internal and external environments of the organization have changed again.

Cybersecurity policies will need to be derived which are clear to all and adaptable in use to meet on-going challenges. While any organization will, of course, require appropriate technological tools to protect its vital systems, these will be unlikely to be efficacious unless they are embedded in sound organizational routines and practices, and understood by all. Just as organizational systems must coevolve, so too must policies be derived in consideration of the many, varied, and contextually dependent professional roles in which actors are engaged, and with their active involvement [31]. Ghelani [16] conducted a qualitative study among Korean businesses to determine how businesses approached information security policy. The results showed an overwhelming focus on preventive measures. He goes on to suggest that a management perspective, rather than an exclusively IT viewpoint, could aid businesses in adopting new organizational practices and change management activities. Lee [21] suggests that investment in cyber risk management could take a four-layered approach:

- a cyber ecosystem layer to build an understanding of the external environment;
- a cyberinfrastructure layer to evaluate organization, internal actors, and existing cyber technologies;
- a cyber risk assessment layer to focus on assessment of risks; and
- a cyber performance layer to conduct specific cyber security activities.

However, crucially, he suggests that: "*All the four layers are strongly intertwined and referenced to the cyber risk management framework, so that a holistic cyber risk management is achieved*" (2021, p.28).

Organizations need to embrace good system design and effective management practices in order to address cybersecurity challenges successfully. We suggest that this is best achieved by adopting a sociotechnical perspective to design of work systems, using appropriate tools and techniques [8, 40]. It is the interactions among engaged actors on an ongoing basis, forming a complex, open system, that co-creates and re-creates what is recognizable as 'organization' [6, 7, 8].

By considering business professionals' own understandings of their contextually dependent work roles, security measures can be related to actual, everyday professional practice. By involving all relevant stakeholders in developing sound practices, cyber security risks may be identified, assessed and mitigated and a culture of security awareness can be promoted [32]. Security practice will therefore be meaningful to stakeholders, who will see it as part of their own zones of responsibility and not as something to be left to remote IT 'experts' [31]. Engagement and participation by professionals at all levels is needed to promote design of systems that are not only user-friendly, but genuinely supportive of meaningful use in context. Principles for good sociotechnical design should be considered at all stages and levels, whenever desirable change is contemplated. Where change is endemic and continuous, these principles become imperative. Flexible systems that are adaptable in use can deal with security contingencies without generating unintended consequences, or requiring professionals to engage with ad hoc "work-arounds" to enable them to complete their work.

Reflecting upon the issues set out above, a study was conducted, which was designed to illuminate actual experiences of actors in real-world organizations in relation to cyber security.

4. Research Methodology

The study undertaken is an exploratory study, conducted from an interpretive stance. This means that it was not intended to test any particular hypothesis, or to uncover any statistically significant or generalizable conclusions, but rather to shed light on actual, experienced practices within a sample of real-world organizations. The reported results may, of course, be used to generate further investigations into any patterns that appear to emerge. Spratley (1980), cited in Robson [29], illustrates the distinction between exploratory and positivist forms of inquiry by analogy with the roles of petroleum engineers and pioneers. The former begin their inquiries with careful study of geological maps to identify areas likely to have gas or oil below ground. They then go on to carry out detailed surveys to 'find' these resources they suspected to be there. This is a positivist stance. Pioneers, in contrast, go out to discover the terrain. They take a path, retrace their steps, take another, and so on until they come upon interesting features, such as a wood or a lake. They take frequent compass readings, note prominent landmarks, and record observations. The result is a better conception of the nature of the area than they had before.

In taking a critical, interpretive stance, the team recognize that respondents' accounts of their experiences are not simple reflections of an objective reality. They, and the inquirers, are part of the arena of inquiry and co-creators of the inquiry process, and the conversation that emerges. The inquiry intrudes into participants' private worlds of experience and takes place within their individual work contexts. It is necessary to bear these points in mind and also to consider the double hermeneutic involved in any inquiry into human experience – the subject is interpreting the inquirer, and vice versa (Hammersley and Atkinson, 1983, cited in [37]). A critical stance means that the team needs to question assumptions made, about process and about results obtained [25].

The study made use of instruments from the Sociotechnical Toolbox [40], which were used as the basis for a semi-structured interview protocol. (NB the instruments in the toolbox cover a range of areas and issues besides cybersecurity, but these are beyond the scope of the current paper). The interviews were intended to take the form of guided conversations. The initial questions, some open-ended and some closed, were intended to elicit a response that could then be followed up in a conversational manner to draw out participants' own views of their experiences and practice. Participants were, in many cases, interviewed more than once following reflection upon their responses. The semi-structured nature of the protocol was advantageous in helping to promote consistency among the approach of different interviewers, but was not to be regarded as a survey.

Sampling was undertaken on a convenience model. The team of investigators was diverse in background and employment, and therefore interview participants were drawn from a range of companies in which the team members had contacts from their own professional and social networks. The companies therefore varied in size, from large multinational corporations to small local businesses, in sphere of business – including both public and private sector organizations, and in all geographic location, though almost all were UK based. The interviewees were all employees from non-IT professions, who, according to their own description, handle sensitive data and therefore, should take security considerations into account while doing their job.

Since the study presented here is qualitative and interpretative in character, the numbers set out are intended only to display transparency and to support a discussion related to patterns disclosed.

Interviews were conducted with 471 employees from 259 different organizations, drawn from both private and public sectors. Each one of the individual employees were interviewed more than once, over a period of five to six months, each interview lasted between 30 minutes to 1 hour. The discussion in this paper is based on two subject areas, Sociotechnical and Cybersecurity (including Systemic Sustainability).

5. Findings

In this paper, we explore findings related to a subset of a few emerging areas of concern.

5.1. Cybersecurity Issues

According to their employees, every company has suffered some kind of serious cybersecurity incident. Most (447) employees said that their organizations had experienced serious issues and disruption due to ransomware. In each case, this had been blamed on users falling for email-based phishing scams. The majority of employees (428) explained that their companies had not offered to pay the ransom, but instead had reverted to backups. This however had caused major disruptions in the corporate network and business activities. It was not unusual that the disruption had lasted for more than three weeks. Only a relatively few employees (18) said that their company had managed to get their (all of their) system up and running within a scope of less than one week. The explanation for the disruption was always the same; an employee had clicked on a link in an email.

5.2. Corporate Security Policy:

Respondents in most companies reported that the security policy was difficult to find in practice. The majority (468) of employees we talked to could not find the security policy themselves, and many (431) did not even locate it after explicitly asking their own IT department for help finding it. When IT security documents were available, the majority were found to be out of date (37 out of 40 found), not recently updated, and sometimes not even updated according to the very deadlines described in these same documents.

In every available security policy document, reference was made to training and practices in an abstract way, without relating these to any organizational or professional context. In every document the focus and the responsibility for IS and Cybersecurity were put explicitly on the employee, and not the Security or IT professionals within the company.

5.3. Emerging Areas of Concern:

- Lack of access to security policy documents. Their locations were not known or easily available to most employees. On many occasions, access to these documents was not even forthcoming when specifically requested from IT/support departments.

- Security policies had the appearance of being created as a perfunctory 'tick box' exercise. The content was clearly a collection of standard phrases, which had limited or no contextual bearing on the actual business activities in which they were situated. The lack of contextuality of content resulted in employees being unable to identify the real-world relevance of the policy documents. Instead, the content was experienced as abstract and contained no explicit contextual examples relevant to the employees' own work situation.
- The majority of documents were out of date and had not been updated according to their own schedule. Often, there was a clear date within the document stating when it was supposed to be updated, but this had not happened. Employees who actually obtained these security documents still had no access to a policy that was valid as described.
- The lack of contextualisation of the content of the policy and security documents meant that there was also often no actionable advice or support available for employees who needed to know how to apply security policy or understand how to address exceptions. There was no guidance as to what kind of workarounds were acceptable, for instance, and what to do when these were needed. This also meant that there was no feedback on further development of contextually relevant policies. Employees were able to show a few emails, in which they sought help from their managers and/or IT support, and responses tended to avoid addressing the actual questions put to them, instead referring the employee back to the (out-of-date and not always available) corporate security policy document.

6. Discussion and Conclusion

The challenges this paper seeks to highlight are concerned with engagement by all interested participants with the context and impetus of change. Implementation of cybersecurity practices is an example of an IS and organizational change which is intended to directly impact on, influence, and change, the real-world work system that the employee is engaged with. As such it is also a prime example of a sociotechnical IS and IT project. The literature of IS has been littered with case instances of failure in information technology projects and the difficulties of bringing projects to a '*successful'* conclusion [4, 6, 25]. Many solutions have also been presented in the past, but the problem persists. The very concept of a '*project'* and the expectation of a '*conclusion'* may lie at the heart of these failures. Technological solutions cannot be developed in isolation from people who will use them, in contexts that are real, ongoing, complex and '*messy'*. Amarilli, van den Hooff and van Vliet [3] highlight the complex coevolution dynamics involved in successful use of IT resources, and call for a sociotechnical approach. Organizational transformation involves changing every aspect of the system. It is not possible to change one aspect alone without this impacting on the whole [10,12]. Attempts to make unilateral changes to technological elements in a work system are likely to result in unintended consequences [17].

A sociotechnical perspective does not, of itself, lead either to successful change or systems experienced as useful. Savageta, Geissdoerfera, Kharrazib and Evans [35] discuss their extensive literature review on sociotechnical systems change and sustainability, saying that "*The analysis of sociotechnical systems often implies the ultimate idea that there are mutually reinforcing and highly institutionalised processes in sociotechnical regimes. This makes it difficult for sustainable innovations to succeed against the existing unsustainable alternatives, consequently constraining radical structural changes*."

It is suggested that when business is conceived as organized activity among people, a transformation process can best be seen as an emergent learning process, whereby exploration and (co)understanding of contextual dependencies are supported by appropriate socio-technical tools and techniques [8]. As March [23] pointed out, technological change involves trading off exploration of new possibilities with exploration of old certainties in organizational learning. In relation to sociotechnical systems design, relevance of contextual analysis is emphasised, i.e.

exploring human and technical dependencies together in the context of an evolving organizational environment.

As Ciborra and Willcocks [13] highlighted, a situated perspective is needed, calling for methods of inquiry which capture the inner lives of actors: minds and hearts. Without such an approach it is difficult to see any significant evidence of any increase in cybersecurity in practice.

References

[1] Allianz Risk Barometer Report | January 2023. The top business risks for 2023, https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

[2] Alvesson, M. & Jansson, A. (2021). Organizational Dischronization: On Meaning and Meaninglessness, Sensemaking and Nonsensemaking. *Journal of Management Studies*. https://doi.org/10.1111/joms.12790

[3] Amarilli, F., van den Hooff, B., and van Vliet, M. (2023). Business-IT alignment as a coevolution process: An empirical study. *J Strat Info Sys*, 32(2), Art.101776, DOI: 10.1016/j.jsis.2023.101776.

[4] Amelsvoort, P. & Mohr, B. (editors) (2016). Co-creating Humane and Innovative Organizations: Evolution in the Practice of Socio-technical Systems Design. Global STS-D Network Press.

[5] Ashby, W.R. (1956) An introduction to cybernetics. London: Chapman & Hall.

[6] Bednar, P. (2000). A Contextual Integration of Individual and Organizational Learning Perspectives as Part of IS Analysis. *Informing Science: journal of an emerging transdiscipline*, 3(3):145-156. DOI: 10.28945/590.

[7] Bednar P. (2016). *Complex methods of inquiry: structuring uncertainty*. Lund University Press. https://lup.lub.lu.se/record/b8f3f911-7f63-4455-bd7a-e91937440711

[8] Bednar, P.., Sadok, M. & Shiderova, V. (2014). Socio-Technical Toolbox for Business Analysis in Practice, in L. Caporarello, B. Di Martino, & M. Martinez (editors), Smart Organizations and Smart Artifacts, *Lecture Notes in Information Systems and Organisation*. Springer International.

[9] Bednar, P.M. and Welch, C. (2020) Socio-Technical Perspectives on Smart Working: Creating Meaningful and Sustainable Systems. *Information Systems Frontiers* 22(2). p.281-298. https://doi.org/10.1007/s10796-019-09921-1

[10] Checkland, P. (1981). *Systems Thinking, Systems Practice*. Chichester: J. Wiley & Sons.

[11] Checkland, P. (1994). Systems Theory and Management Thinking. *American Behavioral Scientist*, 38(1), 75-91. https://doi.org/10.1177/0002764294038001007.

[12] Checkland, P. & Holwell, S. (1998), *Information, Systems and Information Systems*, Wiley.

[13] Ciborra, C. and Willcocks, L. P. (2006) The mind or the heart?: it depends on the (definition of) situation. *Journal of Information Technology*, 21 (3). pp. 129-139. DOI: 10.1057/palgrave.jit.2000.

[14] Emery, M. (2000). The Current Version of Emery's Open Systems Theory. *Sys Pract & Action Res*, 13(5), 623-643. DOI: 10.1023/A:1009577509972.

[15] Geels, F.W. (2004). From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory. *Research Policy*, 33(6–7), 897-920. DOI: 10.1016/j.respol.2004.01.015.

[16] Ghelani, D. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *Authorea Preprints*. September 22, 2022. DOI: 10.22541/au.166385207.73483369/v1.

[17] Harrison, M.I. & Koppel, R. (2010). Interactive Sociotechnical Analysis: Identifying and Coping with Unintended Consequences of IT Implementation, in K. Khoumbati, Y.K. Dwivedi, A. Srivastava & B. Lal, editors, *Handbook of Research on Advances in Health Informatics and Electronic Healthcare Applications: Global Adoption and Impact of Information Communication Technologies*. IGI Global. pp. 33-51. DOI: 10.4018/978-1-60566-030-1.

[18] Hill, M. (2023). Police Service of Northern Ireland discloses second data breach in as many days. *CSO On-line*, available at https://www.csoonline.com/article/649200/police-service-of-northern-ireland-discloses-second-data-breach-in-as-many-days.html.

[19] Jiang, J.J. (2023). From Information Technology Projects to Digital Transformation Programs: Research Pathways. *Proj Man J*, 54(4), 327-333. DOI: 10.1177/875697282311702.

[20] Langefors, B (1966), Theoretical Analysis of Information Systems, Studentlitteratur.

[21] Lee, I. (2022). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons,* 64(5), 659-671. DOI: https://doi.org/10.1016/j.bushor.2021.02.022.

[22] McEvoy, T.R. & Kowalski, S.J. (2019). Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach. *Complex Systems Informatics & Modeling Quarterly*, 18: 47-64 (2019). DOI: 10.7250/csimq.2019-18.03.

[23] March, J.G. (1991). Exploration and Exploitation in Organizational Learning. *Organization Science*, 2 (1), 71-87. DOI:10.1287/ORSC.2.1.71.

[24] Mumford, E. (2006). The study of socio-technical design: reflections on its successes, failures and potential. *Information Systems Journal*, 16, 317–342.

[25] Nissen, H-E., Bednar, P.M. & Welch, C.E., editors (2007). *Use and Redesign in IS: Double Helix Relationships?* Informing Science Press. DOI: 10.13140/2.1.3525.0561.

[26] Nylén, D. & Holmström, J., (2015). Digital innovation strategy: A framework for diagnosing and improving digital product and service innovation. *Business Horizons*, 58(1), 57-67. DOI: 10.1016/j.bushor.2014.09.001

[27] Peppard, J. and Ward, J. (2004). Beyond strategic information systems: towards an IS capability. *J Strat Info Sys*, 13(2), 167-194. DOI:10.1016/j.jsis.2004.02.002.

[28] Perozzo, H., Zaghloul, F. & Ravarini, A. (2022). CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective. *Complex Syst. Informatics Model. Q.*, 33, 53-66. DOI:10.7250/csimq.2022-33.04.

[29] Robson, C. (2011). Real World Research. 3rd edition, Oxford: Wiley-Blackwell.

[30] Sadok, M., Katos, V., & Bednar, P.M. (2014). Developing Contextual Understanding of Information Security Risks. *Proceedings of Conference: Human Aspects of Information Security & Assurance (HAISA 2014)*, Plymouth, UK.

[31] Sadok, M., Alter, S. & Bednar, P.M. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. Information and Computer Security, 28(3), 467-483. DOI: 10.1108/ICS-01-2019-0010.

[32] Sadok, M., Welch, C., & Bednar, P.M. (2020). A socio-technical perspective to counter cyber-enabled industrial espionage. *Security Journal*, 33(1), 27–42. DOI: 10.1057/s41284-019-00198-2.

[33] Saleh Al-Omoush, K., Simón-Moya, V. & Sendra-García, J. (2020). The impact of social capital and collaborative knowledge creation on e-business proactiveness and organizational agility in responding to the COVID-19 crisis. *J. Innov & Knowl*, 5(4), 279-288. DOI: 10.1016/j.jik.2020.10.002.

[34] Savaget, P., & Acero, L. (2018). Plurality in understandings of innovation, sociotechnical progress and sustainable development: An analysis of OECD expert narratives. *Public Understanding of Science*, 27(5), 611–628. https://doi.org/10.1177/0963662517695056.

[35] Savageta, P., Geissdoerfera, M., Kharrazib, A and Evans, S. (2019). The theoretical foundations of sociotechnical systems change for sustainability: A systematic literature review. *J. Cleaner Prod*, 20(6), 878-892. DOI: 10.1016/j.jclepro.2018.09.208.

[36] Silverman, D. (1970). *The theory of organizations*. London: Heinemann.

[37] Silverman, D. (2019). Interpreting Qualitative Data. 6th edition, London: Sage Publications.

[38] Simon, H. A. (1960). *The new science of management decision*. New York: Harper & Row.

[39] Vickers, G. (1968). *Value systems and social process*. Abingdon: Tavistock Press.

[40] Bednar P. (2022). *Sociotechnical Toolbox*. Portsmouth: Craneswater Press.