ISBN- 978-978-57388-7-2

Trinity University, Nigeria
Society for Multidisciplinary & Advanced Research Techniques (SMART) Africa
IEEE Computer Society, Nigeria
The ICT University Foundations, USA.

LASUSTECH Multidisciplinary Innovations Conference (LASUSTECH-MIC)

16th – 18th April, 2022

Towards An Exploration of Developing Issues and the Relationship Between Information Technology Governance and Multi-stakeholder Security Governance Scaling for Cyber Security Decision-Makers within the UK Small and Medium-Sized Enterprises Aviation

Ademola, Emmanuel Ojo (PhD)
British Computer Society's Information Security Specialist Group (ISSG)
Executive Committee Member
Full Professor & Governing Council Member
American International University West Africa Gambia
College of Management & Information Technology
The Gambia

E-mails: ojo_ademola@hotmail.co.uk

Phone No: +447958139157

Proceedings Citation Format

Ademola, E.O. (2022): Towards An Exploration of Developing Issues and the Relationship Between Information Technology Governance and Multi-stakeholder Security Governance Scaling for Cyber Security Decision-Makers within the UK Small and Medium-Sized Enterprises Aviation. Proceedings of the LASUSTECH 30th iSTEAMS Multidisciplinary Innovations Conference. Lagos State University of Science & Technology, Ikorodu, Lagos State, Nigeria May 2022. Pp 83-100
www.isteams.net/lasustech2022Pp
DOI: https://doi.org/10.22624/AIMS/iSTEAMS/LASUSTECH2022V30P8

ISBN- 978-978-57388-7-2

Towards An Exploration of Developing Issues and the Relationship Between Information Technology Governance and Multi-stakeholder Security Governance Scaling for Cyber Security Decision-Makers within the UK Small and Medium-Sized Enterprises Aviation

Ademola, E.O.
British Computer Society's Information Security Specialist Group (ISSG)
Executive Committee Member
Full Professor & Governing Council Member
American International University West Africa Gambia
College of Management & Information Technology
The Gambia
Email: ojo_ademola@hotmail.co.uk
Phone No: +447958139157

ABSTRACT

The trajectory of our present efforts is to feature the developing issues and explore the relationship between Information Technology Governance (ITG) and Multi- stakeholder Security Governance Scaling (MSGS) for decision-makers within the UK's SME Aviation, which should benefit academia and practitioners. By conducting an extensive literature review, covering expert and scholarly writing, lean implementation thinking, SMEs cyber policymaking industrial and grand synergy, a profound knowledge level and concise synthesis can be presented, which informsthe exploratory secondary qualitative research. In creating the framework, a process theory approach is pursued by transcribing primary data into secondary data to develop models and identify themes with a purposive survey sample from SMEs decision-makers. This submission sets the stage afor our discourses and outlines our research agenda

Keywords: Cyber Security, Cyber Policy, Information Technology Governance, Culture, Agile, Multi-stakeholder Security Governance Scaling, Information Technology, Scaling Techniques, SME Aviation, Security

1. INTRODUCTION

1.1 Background to the Study

Mainly, Information technology (IT) plays a vital role in organisational innovation adoption (Vejseli *et al*., 2019). As such, ITG is dominant in add-on IT to permit innovation. However, the conventional idea of ITG to control the plan and execution of IT methodology is not entirely outfitted to manage the present changes happening in the digital age. For instance, Saeidi *et al*., (2019) argue that due to the impact of enterprise risk management on competitive advantage, there should be a paradigm shift in the approach to the implementation of ITG. Notably, ITG implementation in SMEs remains centralised for decades in a diverse industrialsector. Zarvić *et al*. (2012) argued that the application of ITG in SMEs should tie with strategic frameworks and its esteem conveyance to the business. Nonetheless,it is a view that could have direct impacts on decision-making (Devos, Van Landeghem and Deschoolmeester, 2012; Nfuka and Rusu, 2011; Wilkin, 2012).

ISBN- 978-978-57388-7-2

Furthermore, such an approach could play a paramount role in analysing and identifying constraints in an active uptake in SMEs (McCarthy, 2009). The need to successfully implement ITG to improve some business outcomes in the SMEs estimation of innovation could make its application a significant issue (Sambamurthy and Zmud, 1999; Weill and Ross, 2004). In the digital age, the most significant inclining difficulties confronting SMEs are less identifiable with technology than to governance (McCarthy, 2009; Nfuka and Rusu, 2011). However, SMEs could leverage limited resources to support the adoption of the MSGS.

In the SME context of ITG, Banham and He (2010) argues that the application of the converging definitions and expanding expectations could result in some specific challenges. ITG implementation could suffice the need for a change of approach to help decision-makers in the communication of their strategic plan. It could mean that procedures and strategies to align business techniques and objectives in meeting outcomes must change to sustain an existing organisation culture. For example, decision-makers need to know where personal information of clients reside in following the prevailing regulations.

It might be a new challenge that centres on the platform that holds personal information; and whether the cybersecurity standards are implemented securely. It was noted that the GDPR (2016) reinforces the Article 8 (1) of the Charter ofFundamental Rights of the European Union and the Article 16(1) of the Treaty on theFunctioning of the European Union that the protection of natural persons in relationto the processing of personal data is a fundamental right. Bergeron *et al*. (2015) accentuate the need to dedicate both scholars and practitioners' skills, understanding to support the development and implementation of ITG frameworks suitable for the use of SMEs. Undoubtedly, most industrial policy related to ITG particularly mobilises and proposes theories and frameworks to explain and implement governance. However, most ITG functionalities andprocedures are often criticised as not implementable in SMEs (Banham and He, 2010; Bergeron *et al*., 2015).

For instance, to achieve the six objectives in the UK Aviation Strategy 2017,ITG must be suitably inclusive. The strategy has six targets, which are to help the aviation industry work for its customers; guarantee a protected and secured approach to travel; build a global and connected Britain; encourage competitive markets; support growth while tackling environmental impacts; develop innovation, technology and skills. For the assertion of suitability, practitioners and scholars couldrecall the impact of theories and frameworks, and possibly propose alternatives that are cost effective and specifically implementable in SMEs (Banham and He, 2010; Bergeron *et al*., 2015; Silva *et al*., 2018). SME Aviation not only need the appropriate strategy – for emailing, printing documents, consumer access to secure information platform on pricing; it must also boost stakeholder's confidence in the security aswell as encourage a collaborative approach to governance.

Nonetheless, how could the implementation of the right industrial cyberpolicy contribute to the robustness of multi-stakeholder governance approach? GreenPope *et al*. (2010) argued that such an approach "requires tightly choreographed activities across organisations in diverse locations." The strategy accentuates the responsibilities of Airport Commissions, Department of Transport, Ministry of Defense (MOD) and other Aviation security organisations; under which the synergy works. Aggarwal and Reddie (2018) evaluate the role of businesses, governments, other critical stakeholders in the emergence of industrial policy. Aggarwal and Reddie corroborated Sender's (2016) view that there is the emerging escalation of the geopolitical context in cyber policy content of both UK, US, and other world power to strategic competition.

ISBN- 978-978-57388-7-2

This competition could anchor the widespread use of the internet as a global venue for international cybercrime. Timmers (2018) underscores that due to the diverse content of economic cooperation of its member states, EU levelled cybersecurity as security-strategy within various industry and that of policymaking. In the development of effectivecyber policy, there could be some challenges (Ademola, 2019); for example, if there is evidence of constrained command, EU nations could perceive the economic implication regarding cybersecurity as a matter of national security concern. Despite the challenges, Timmer concluded that with multi-stakeholder governance approach,decision-makers could provide EU member states with a joint cyber industrial policy.

The latest Aviation Strategy reiterates the centrality and efficacy of the UK as the most significant internet economy in the G20 (Carr and Tanczer, 2018). It's an envisioned synergy for been the 'safest place in the world to live and work online'. Carr and Tanczer accentuate the opportunities due to the November 2011's launchof the UK's first National Cyber Security Strategy (NCSS). The strategy underpinsthe emergency from an initial heavy reliance on market forces towards more collaborative governance as a state-driven public-private partnership (De Haes and

Van Grembergen, 2009). Remarkably, it is a call for an urgent and more proactive role in policy debates concerning how to address and maintain an 'edge' in global competition surrounding high ITG. Additionally, with the notion of multi-stakeholder governance security scaling, the practice of industrial policy in the marketplaceremains an emerging force.

With the robust implementation of ITG, De Haes and Grembergen (2008) noted that a cyber policy can always be at an efficiency to align business outcomes and IT appropriately. For instance, with effective adoption of appropriate ITG, theuse of process theory could imply a limited synergy regarding business/IT alignment's maturity. De Haes and Grembergen (2009) suggest that at such point of business/IT alignment, such could be an effective synergy to implement a policy. Apparently, in practice, a process might exhibit a likely outcome for robust competitiveness. Huang *et al*. (2010) agreed with De Haes and Grembergen's conclusion that applying a mix of mature ITG implementations in SMEs promote the efficiency of cyber policymaking. Conversely, a state-driven policy with linkages to internet governance could suffice a dramatic outcome considering Porter's (1979)five forces (Gary and Heiko, 2015; Porter, 2008).

The exploration will premise on developing a cyber policy framework. It is a proposition that intends to enhance the governance approach. Objectively, it will deliver an exploratory notion of engaging with ITG and MSGS. Notwithstanding, the extensive work about ITG since the late nineties up-till-date (Ademola, 2019; Callahan *et al*., 2004; De Haes and Grembergen, 2006; Grembergen and De Haes, 2018; Peterson, 2001, 2004). The researchers are notably concurring with the notionof exploring the linkages between ITG and MSGS and considering such as anintriguing in meeting future research needs.

ISBN- 978-978-57388-7-2

2. RESEARCH FOCUS

There is some perplexity to the implementable cyber policy in SMEs. Serious issues remain as concerning possible impediments to the successful implementation of cyber policy. For instance, there have been concerns over uniting different points of view from a different arrangement of security contribution of scholasticcommitments in research philosophy and approach (Babbie, 2017; Parn and Edwards, 2019). It is essential to evaluate how the exploration of ideas from a multidisciplinary preceptive helps to examine mechanical strategies to address cybersecurity vulnerabilities (Emmersen *et al*., 2019; Fields, 2018). With the developing number of SMEs in the UK excluding Northern Ireland, 5.5 million as of November 2016 (Gov.uk 2016), the UK has the most extensive internet economy of the G20 countries with percentage contribution to GDP since 2010 (Department for Culture, Media and Sport 2017). Cyber policy researchers advocate for governance cooperation in general industrial policy making (Carr and Tanczer, 2018; Timmers, 2018).

Cyber policy analysts and decision-makers are also warning that researchers and practitioners in businesses require to understand the challenges associated withthe theoretical framework for the analysis of cyber industrial policy (Editorial Office, 2018). Such structure of knowledge underpins a geographically diverse set of country and regional case studies in the examination of cyber industrial systems and further the drivers with global implications of cyber industrial policy across the industrial sector and nation. The digital industry represents 16% of the UK household; yielding 10% of its employment and 24% of the UK's exports (Chakravortiand Chturvedi, 2017); while the SMEs, BAE Systems and QinetiQ combined working in offensive cyber programmes, the UK emerged as a core player in the global cyber industrial equation.

The sector is enormous to the UK economy. It contributes to more than 120,000 jobs, most of which are outside London and the South-East with a yearly turnover of £35bn (data.parliament.uk, 2018). Scholars' and practitioners' supportare crucial for the success of developing cyber policy implementable in SME Aviation. Governments are responding to market failures in cybersecurity with different approaches. Japan relies on market incentives and partnerships (Bartlett, 2018); China and Taiwan depended principally on their legislatures to drive change (Cheung, 2018; Huang and Li, 2018).

In Europe and North America, governments proactively present cybersecurity measures, making a shift from previous market-driven approaches to promote competitive advantages (Jensen, 2018; Aggarwal and Reddie, 2018). While every nation and industrial sectors show qualities to some degree with various methods for getting things done, there are likenesses of methodology among a considerable lotof the intra-segment, nations and districts to underscore (Bartlett, 2018; Carr and Tanczer, 2018; Cheung, 2018; Huang and Li, 2018; Griffith, 2018; Timmers, 2018).

Nonetheless, suffices are aptitudes deficiencies and endemic digital instability. Its exceptionally associated divisions and social orders underlined inside the extentof the examination. A primary focus of this research will concentrate on the issues developing in cyber policy, including the exploration of the relationship that exists between ITG and the problems that arise with MSGS for decision-makers. Also, to underscore the barriers to enhance decision making by reducing the risk of technical cyber policy failure in the SME Aviation in the UK.

ISBN- 978-978-57388-7-2

There are trainings for decision makers to prepare them to implement robust cyber policy with identifying the linkages that exist ITG and MSGS and advice available for practical implementation in the promotion of healthy competitive advantages and secure SME Aviation working environment. Furthermore, to gain a meaningful picture of the correlation between ITG and MSGS, researchers in the future could build theoretical models and generate potential hypotheses for testing and validation.

The cyber policy provides possible exploration on genuine multi-stakeholder's commitment irrespective of challenges arising from IT/Business alignment (Banham and He, 2010). Mysore *et al*. (2019) presented an argument for the synchronisationof ideas to implement ITG in SMEs in contrast to Flyvbjerg's (2016) proposition ofthe fragility scaling versus scalability is a preferred concept to apply MSGS. Nonetheless, the pedagogical attempt to theorise scaling could be a notion of interest to cybersecurity as a body of knowledge (BoK). Supposedly, such understanding could strengthen the linkages that could exist between cyber strategy and the grand strategy for structures, processes and relational mechanisms (Weber 2018). For instance, the conclusion of Savage and McConnell's (2015) investigation strengthens the justification for the simplification and refinement of internet governance. In addition to this, the study provides for pedagogic attention to underscore motivation and relevance to similar BoK.

Further, Rashid *et al*. (2018) assert that the body of knowledge within the cybersecurity curriculum is an indication that cyber policy is turning into a critical academic component at instructional levels. Such a view underpins the similar conclusion of Banham and He (2010), Flyvbjerg's (2016), and Mysore *et al*. (2019). However, it could be a subtle point, but mostly, the challenge for scholars and practitioners is to delineate ways of moving through the subject. As practitioners move to agile policymaking, it could be a paradigm shift to a constructivist approach to further research on collaboration between scholars and practitioners in cyberpolicy development. According to Rashid and colleagues, such scoping of the bodyof knowledge could pave the way for the centrality of learning cybersecurity. Such adoption, according to Hallett *et al*. (2018), could make the study of cyber policymaking a route for a constructive paradigm shift, which is an area of study worthy of further research.

3. RESEARCH AIMS AND OBJECTIVES

The study aims to highlight developing issues and explore the relationship between ITG and MSGS for decision-makers within the UK SME Aviation digital world. The exploration is to advance an understanding of the connection with issues developing in cyber policy. However, to understand the emerging multi-stakeholder approach, it is felt necessary to gain an insight to the relationship that exists betweenITG and the problems that arise with MSGS for decision-makers and to explore support for decision makers by reducing the risk of technical cyber policy failure inthe SME Aviation in the UK.
Given the confusion between those who predict statistical driven ITG models and those who raise some concerns about the implementable cyber policy in SMEs, it is more important to try and clarify MSGS.

Further, this research will explore existing governance guidelines supporting decision makers involved in the development and deployment of implementablecyber policy in SME Aviation. In turn, two primary research vehicles will be exploited to facilitate this understudy: an analytical exploration of secondary data as well as an in-depth review of relevant literature for descriptiveness.

ISBN- 978-978-57388-7-2

Specifically, within the context of governance, the objectives of this research are to:

1) Study Objective 1: Analyse the linkages between ITG and MSGS to theimplementation of a cyber policy
2) Study Objective 2: Explore scaling and scalability mechanisms related todecision making strategy tools
3) Study Objective 3: Investigate how the vulnerability of ITG models and MSGScorrelate to supporting decision makers
4) Study Objective 4: Theorise scaling as a security strategy in coping with ITG implementation.
5) Study Objective 5: Discuss the decision-making scalability mechanism to the successful implementation of ITG within SME Aviation.
6) Study Objective 6: Formulate recommendations on cyber policyimplementation

At the risk of misrepresentation of the reason and estimation of every one of the above goals, objectives 1, 2 and 4 focus on the analytical accentuation of theemerging relationship that exists between ITG and MSGS with the primary discourseon strategic tools for theorising scaling as an ITG security pathway for cyber policy decision makers. Objectives 3, 5 and 6 focus on the governance correlative element of ITG and MSGS, where this understudy will make critical contributions to the fieldof governance. It would be an error for the reader to see every one of the expressed research objectives as independent, unrelated academic exercises.

The listed objectives are necessarily interlinked and add values. The first objective – linkages between ITG and MSGS - will cover the definitive strategic stakeholders' elements that make ITG implementable as well as the scaling relevant to the existing ITG support; each of which will be relevance to SME Aviation preparing for governance. For example, it will attempt to answer the question 'are there linkages within the elements of ITG pushing SME Aviation towards management and if so, what are they?' An example of such a coupling could be perceived as being cost-effective and timesaving in implementation, which, if the case, may catalyse ITG alignment with other business elements for governance furtherance. Objective 2 – on structured approaches will explore scholar and practitioner discourse on scaling versus scalability; in alignment with the answer fromobjectives 1 and 4, will support decision makers in developing the cyber policy and make recommendation towards an efficient implementation.

Objective 3 will investigate how existing vulnerabilities of ITG model and MSGS relate — for example, comparing ITG frameworks, which may yield the top performing standardin pricing? Such an answer will provide an opportunity for decision-makers to gain meaningful insight into the views of why some ITG elements remain undoable in SMEs regarding pricing strategy. Objective 5 will concentrate on a new approachthat could emerge due to the multi-stakeholder's synergy in formulating implementable cyber policy to impact existing governance for SME Aviation consideration. Objective 6 will focus on an attempt to formulate recommendations asa result of the review of the literature and the exploration of secondary data in use. The objectives are not to be autonomous of one another, instead, as all connected toissues encompassing ITG and MSGS in SME Aviation.

ISBN- 978-978-57388-7-2

4. RESEARCH APPROACH

The approach to this study primarily consists of literature research, a matter of UK's SME Aviation and benchmarking in research. The researcher will consistently follow the project plan outlined below:

1. A survey of the expert and scholarly writing spread over 20 to 50 sources
2. An investigation of how the vulnerability of ITG models and MSGS correlate to support decision-makers
3. An attempt to theorise scaling with the input of the existing ITG frameworks
4. With the use of secondary qualitative data, the researcher investigated the relationship between ITG and the MSGS to support Cyber policymaking
5. Recommendations made for further research

The study plan is to conduct research that entails the correct and most ethical means to achieve the research objectives promptly. The researcher primarily used extensive sources ranging upwards of fifty, including academic journals, articles and reports. Notwithstanding, the approach, the study focused on secondary data. Sucha method allows the researcher to concentrate on theorising while connecting with the developing issues in cyber policies implemented within the UK's SME Aviation. Consequentially, the analysis of previous professional and academic sources soughtto contribute to the ITG deliveries. The researcher attempted to find firm relationships between ITG and MSGS that could be helpful in a presentation and standardising of the process in cyber policymaking.

5. VALUE OF THIS RESEARCH

The understudy will contribute to the development of the discipline of governance in several essential ways. Firstly, by providing an investigation to the linkages that may exist between ITG and MSGS; in a way, accentuating the existing vulnerabilities of ITG models. Secondly, by theorising scaling and scalability to aid further development in cyber policymaking. Thirdly, by exploring scholar and practitioner discourse analytically to support decision-makers in furthering the enrichment of the implementation of cyber policy in SMEs. Finally, by understanding the existing practices in a multi-stakeholder paradigm, a rich picture of ITG and MSGS can emerge, allowing a better understanding of theory and practice of governance; and possibly raise issues for further research.

ISBN- 978-978-57388-7-2

Bibliography

1. Aasi, P., Rusu, L. and Leidner, D. (2017). IT organizational structure relationship with IT governance performance: case of a public organization. In Information Technology Governance in Public Organizations (pp. 229-252). Springer, Cham.
2. Ademola, E.O. (2021). Towards an Effective Information Assurance and Risk Management (IA&RM) Guide: A Case Study. Journal of Behavioural Informatics, Digital Humanities and Development Research. 7(1), 45-56.
3. Ademola, E. O. (2020). An Investigation of The Vulnerability of Information Technology Governance (ITG) Models And Multi-Stakeholder Security Governance Scaling (MSGS) Correlates that Supports Decision-Makers Scalability Mechanism for the Successful Implementation of ITG Within UK's SME Aviation. Social Informatics, 6(1), 1-12.
4. Ademola, E. O. (2019). Insights into Cyber Policies, Information Technology Governance (ITG) and, Multi-stakeholder Security Governance Scaling (MSGS) for Decision Makers within UK SME Aviation. Journal of Behavioral Informatics, 5(4), 1- 14.
5. Aggarwal, V.K. and Reddie, A.W. (2018). Comparative industrial policy and cybersecurity: a framework for analysis. Journal of Cyber Policy, 3(3), pp.291-305.
6. Aggarwal, V.K. and Reddie, A.W. (2018). Comparative industrial policy and cybersecurity: the US case. Journal of Cyber Policy, 3(3), pp.445-466.
7. Aldrich, H.E. and Wiedenmayer, G. (2019). From traits to rates: An ecological perspective on organizational foundings. In Seminal Ideas for the Next Twenty-Five Years of Advances(pp. 61-97). Emerald Publishing Limited.
8. Alhaj, S.T.S. (2006). Barriers of implementing ISO 9001: 2000 in the government departments and authorities in the Emirate of Sharjah, United Arab Emirates [sic] (Doctoral dissertation, University of Salford).
9. Alkhoraif, A. (2018). Lean implementation in small and medium enterprises: Literature review. Operations Research Perspectives, p.100089.
10. Alreemy, Z., Chang, V., Walters, R. and Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). International Journal of Information Management, 36(6), pp.907-916.
11. Asgarkhani, M., Cater-Steel, A., Toleman, M. and Ally, M. (2018), May. A Conceptual Model to Evaluate the Effectiveness of Information Technology Governance. In ICMLG 2018 6th International Conference on Management Leadership and Governance (p. 41). Academic Conferences and publishing limited.
12. Azmi, R., Tibben, W. and Win, K.T. (2018). Review of cybersecurity frameworks: context and shared concepts. Journal of Cyber Policy, 3(2), pp.258-283.
13. Babbie, E. (2017). Basics of social research (7th ed.). Boston: Cengage Learning. Badr, Y., Biennier, F. and Tata, S. (2010). The integration of corporate security strategies in collaborative business processes. IEEE transactions on services computing, 4(3), pp.243-254.

ISBN- 978-978-57388-7-2

14. Banham, H. and He, Y. (2010). SME governance: converging definitions and expanding expectations. International Business & Economics Research Journal, 9(2), pp.77-82.
15. Bartlett, B. (2018). Government as facilitator: how Japan is building its cybersecurity market. Journal of Cyber Policy, 3(3), pp.327-343.
16. Bell, J. (2005). Doing your research project: A guide for first-time researchers in education. Health and Social Science, 4.
17. Benbasat, I. and Zmud, R.W. (1999). Empirical research in information systems: The practice or relevance. MIS quarterly, 23(1), pp.3-16
18. Bergeron, F., Croteau, A.M., Uwizeyemungu, S. and Raymond, L. (2017). A framework for research on information technology governance in SMEs. In Strategic IT Governance and alignment in business settings (pp. 53-81). Pennsylvania: IGI Global.
19. Bergeron, F., Croteau, A.M., Uwizeyemungu, S. and Raymond, L. (2015), January. IT governance theories and the reality of SMEs: Bridging the gap. In 2015 48th Hawaii International Conference on System Sciences (pp. 4544-4553). IEEE.
20. Bernauer, J.A. (2015). Opening the ears that science closed: Transforming qualitative data using oral coding. The Qualitative Report, 20(4), pp.406-415.
21. Bernik, I. (2014). Cybercrime: The Cost of Investments into Protection. Varstvoslovje: Journal of Criminal Justice & Security, 16(2).
22. Biggam, J. (2015). Succeeding with your master's dissertation: a step-by-step handbook. UK: McGraw-Hill Education.
23. Bishop, L. and Kuula-Luumi, A. (2017). Revisiting qualitative data reuse: A decade on. Sage Open, 7(1), p.2158244016685136.
24. Bloomberg, L.D. and Volpe, M. (2018). Completing your qualitative dissertation: A road map from beginning to end. London: Sage Publications.
25. Brantly, A.F. (2019). Conceptualizing cyber policy through complexity theory. Journal of Cyber Policy, pp.1-15.
26. Bryman, A., Teevan, J.J. and Bell, E. (2009). Social Research Methods. 2nd Canadian Edition. Don Mills: Oxford University.
27. Callahan, J., Bastos, C. and Keyes, D. (2004). The evolution of IT Governance at NB
28. Power. In Strategies for information technology governance (pp. 343-356). Pennsylvania: IGI Global.
29. Carr, M. and Tanczer, L.M. (2018). UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions. Journal of Cyber Policy, 3(3), pp.430-444.
30. Cater-Steel, A. and Toleman, M. (2010). IT service management standards: education challenges. In New applications in IT standards: developments and progress (pp. 225-241). Pennsylvania: IGI Global.
31. Chakravorti, B. and Chaturvedi, R.S. (2017). Digital planet 2017: how competitiveness and trust in digital economies vary across the world. The Fletcher School, Tufts University, 70, p.70.
32. Cheung, T.M. (2018). The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities. Journal of Cyber Policy, 3(3), pp.306-326.

ISBN- 978-978-57388-7-2

33. Clarke, S.P. and Cossette, S. (2016). Secondary analysis: Theoretical, methodological, and practical considerations. Canadian Journal of Nursing Research Archive, 32(3).
34. Coltman, T., Tallon, P., Sharma, R. and Queiroz, M. (2015). Strategic IT alignment: twenty-five years on. Available at https://link.springer.com/content/pdf/10.1057/jit.2014.35.pdf (Accessed: 19 April 2021).
35. Cunha, L.O. and Alves, J.M. (2014). Application of Lean manufacturing and quality management in aeronautical industry. International Review of Mechanical Engineering, 8(3), pp.592-598.
36. Dahlberg, T. and Kivijarvi, H. (2006), January. An integrated framework for IT governance and the development and validation of an assessment instrument. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) (Vol. 8, pp. 194b-194b). IEEE.
37. De Haes, S. and Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. Information Systems Management, 26(2), pp.123-137.
38. De Haes, S. and Van Grembergen, W. (2008), January. Analysing the relationship between IT governance and business/IT alignment maturity. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) (pp. 428-428). IEEE.
39. De Haes, S. and Van Grembergen, W. (2006), January. Information technology governance best practices in Belgian organisations. In Proceedings of the 39th
40. Annual Hawaii International Conference on System Sciences (HICSS'06) (Vol. 8, pp. 195b-195b). IEEE.
41. Delgado, A.P. and Velthuis, M.P. (2015). Proposal for a continuous improvement IT governance framework at financial institutions/Propuesta de marco de mejora continua de gobierno TI en entidades financieras. RISTI (Revista Iberica de Sistemas e Tecnologias de Informacao), (15), pp.51-68.
42. D'Elia, D. (2018). Industrial policy: the holy grail of French cybersecurity strategy? Journal of Cyber Policy, 3 (3), pp.385-406.
43. de Mingo, A.C. and Cerrillo-i-Martínez, A. (2018). Improving records management to promote transparency and prevent corruption. International Journal of Information Management, 38(1), pp.256-261.
44. Denzin, N.K. and Lincoln, Y.S. eds. (2011). The Sage handbook of qualitative research. London: Sage.
45. Devos, J., Van Landeghem, H. and Deschoolmeester, D. (2012). Rethinking IT governance for SMEs. Industrial Management & Data Systems, 112(2), pp.206-223.
46. Doyle, P. (1989). Markets and innovation. European Management Journal, 7(4), pp.413-421.
47. Dwivedi, Y.K., Wastell, D., Laumer, S., Henriksen, H.Z., Myers, M.D., Bunker, D., Elbanna, A., Ravishankar, M.N. and Srivastava, S.C. (2015). Research on information systems failures and successes: Status update and future directions. Information Systems Frontiers, 17(1), pp.143-157.

ISBN- 978-978-57388-7-2

48. Eastin, M.S., Brinson, N.H., Doorey, A. and Wilcox, G. (2016). Living in a big dat world: Predicting mobile commerce activity through privacy concerns. Computers in Human Behavior, 58, pp.214-220.
49. Edelman, S. (2016). The minority report: some common assumptions to reconsider in the modelling of the brain and behaviour. Journal of Experimental & Theoretical Artificial Intelligence, 28(4), pp.751-776.
50. Emmersen, T., Hatfield, J.M., Kosseff, J. and Orr IV, S.R. (2019). The USNA's Interdisciplinary Approach to Cybersecurity Education. Computer, 52(3), pp.48-57.
51. Flyvbjerg, B. (2016). Big is Fragile: An attempt at theorizing scale. by B. Flyvbjerg. Oxford: Oxford University Press.(2016b).“The fallacy of beneficial ignorance: A test of hirschman’s hiding hand”. In: World Development, 84, pp.176-189.
52. Fields, Z. ed. (2018). Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution. Pennsylvania: IGI Global.
53. Gary, J.E. and Heiko, A. (2015). The future of foresight professionals: Results from a global Delphi study. Futures, 71, pp.132-145.
54. GreenPope, R.A., Beaton, E.K., Boiney, L.G., Drury, J.L., Henriques, R.D., Howland, M. and Klein, G.L. (2010), May. Aviation security collaboration stakeholder governance review. In 2010 Integrated Communications, Navigation, and Surveillance Conference Proceedings (pp. N4-1). IEEE.
55. Gregory, R.W., Kaganer, E., Henfridsson, O. and Ruch, T.J. (2018). IT Consumerization and the Transformation of IT Governance. MIS Quarterly, 42(4), pp.1225-1253.
56. Griffith, M.K. (2018). A comprehensive security approach: bolstering Finnish cybersecurity capacity. Journal of Cyber Policy, 3(3), pp.407-429.
57. Hallett, J., Larson, R. and Rashid, A. (2018). Mirror, Mirror, On the Wall: What are we Teaching Them All? Characterising the Focus of Cybersecurity Curricular
58. Frameworks. In 2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18).
59. Harding, J. (2018). Qualitative data analysis: From start to finish. London: SAGE Publications Limited.
60. Hassan, N.R., Mingers, J. and Stahl, B. (2018). Philosophy and information systems: where are we and where should we go?. Available at: http://www.jtaer.com/statistics/download/download.php?co_id=JTA20190200 (Accessed: 20 April 2021).
61. Hayes, J. and Bodhani, A. (2013). Cyber security: small firms under fire [InformatIon Technology Professionalism]. Engineering & Technology, 8(6), pp.80-83.
62. Henderson, J.C. and Venkatraman, N. (1994). Strategic alignment: a model fororganizational transformation via information technology (pp. 202-220). New York: Oxford University Press.
63. Howlett, M. (2018). Matching policy tools and their targets: beyond nudges and utility maximisation in policy design. Policy & Politics, 46(1), pp.101-124.
64. Hox, J.J. and Boeije, H.R. (2005). Data collection, primary versus secondary. Available at: https:// https://dspace.library.uu.nl/handle/1874/23634.pdf (Accessed: 23 September 2020)

ISBN- 978-978-57388-7-2

65. Huang, H. and Li, T.S. (2018). A centralised cybersecurity strategy for Taiwan. Journal of Cyber Policy, 3(3), pp.344-362.
66. Huang, R., Zmud, R.W. and Price, R.L. (2010). Influencing the effectiveness of IT governance practices through steering committees and communication policies. European Journal of Information Systems, 19(3), pp.288-302.
67. Hubbard, D.W. and Seiersen, R. (2016). How to measure anything in cybersecurity risk. New Jersey: John Wiley & Sons.
68. Hyman, P. (2013). Cybercrime: it's serious, but exactly how serious?. Communications of the ACM, 56(3), pp.18-20.
69. Iden, J. (2009). Implementing IT service management: Lessons learned from University IT department. In Information technology governance and service management: Frameworks and adaptations (pp. 333-349). IGI Global.
70. Jensen, M.S. (2018). Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle. Scandinavian Journal of Military Studies, 1(1).
71. Johnston, M.P. (2017). Secondary data analysis: A method of which the time has come. Qualitative and quantitative methods in libraries, 3(3), pp.619-626.
72. Khallaf, A., Omran, M.A. and Zakaria, T. (2017). Explaining the inconsistent results of the impact of information technology investments on firm performance: A longitudinal analysis. Journal of Accounting & Organizational Change, 13(3), pp.359- 380.
73. Khan, S.N., Nicho, M., Takruri, H., Maamar, Z. and Kamoun, F. (2019). Role assigning and taking in cloud computing. Human Systems Management, 38(1), pp.1- 27.
74. Laurenza, E., Quintano, M., Schiavone, F. and Vrontis, D. (2018). The effect of digital technologies adoption in healthcare industry: a case based analysis. Business Process Management Journal, 24(5), pp.1124-1144.
75. Lelarge, M. and Bolot, J. (2009), April. Economic incentives to increase security in the internet: The case for insurance. In IEEE INFOCOM 2009 (pp. 1494-1502). IEEE.
76. Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. Computers & Security, 77, pp.262-276.
77. Lowry, P.B., D'Arcy, J., Hammer, B. and Moody, G.D. (2016). "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. The Journal of Strategic Information Systems, 25(3), pp.232-240.
78. Lynch, R.L. and Smith, J.R. (2006). Corporate strategy. Harlow, England: FT/Prentice Hall.
79. Mahmood, M.A. and Mann, G.J. (1993). Measuring the organizational impact of information technology investment: an exploratory study. Journal of management information systems, 10(1), pp.97-122.
80. Makridis, C.A. and Smeets, M. (2019). Determinants of cyber readiness. Journal of Cyber Policy, 4(1), pp.72-89.
81. Manville, G., Papadopoulos, T. and Garengo, P. (2019). Twenty-first century supply chain management: a multiple case study analysis within the UK aerospace industry. Total Quality Management & Business Excellence, pp.1-17.

ISBN- 978-978-57388-7-2

82. Manyika, J. (2017). A future that works: AI automation employment and productivity. McKinsey Global Institute Research, Tech. Rep. Available at https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/1 70622-slides-manyika.pdf (Accessed: 22 March 2021)
83. Matthews, R. ed. (2019). The Political Economy of Defence. England: Cambridge University Press.
84. Matten, D. and Moon, J. (2008). "Implicit" and "explicit" CSR: A conceptual framework for a comparative understanding of corporate social responsibility. Academy of management Review, 33(2), pp.404-424.
85. McCarthy, J. (2009). An examination of the impact of e-business evolution within small and micro businesses (Doctoral dissertation, Buckinghamshire New University).
86. McKinsey Global Institute (2019). Automation at scale: The benefits for payers. Available at: https://www. mckinsey.com/industries/healthcare-systems-and- services/our-insights/automation-at-scale-the-benefits-for-payers (Accessed: 12 April 2021).
87. Mora, M., Rory, V.O., Rainsinghani, M. and Gelman, O. (2016). Impacts of electronic process guides by types of user: An experimental study. International Journal of Information Management, 36(1), pp.73-88.
88. Mosteller, J. and Poddar, A. (2017). To share and protect: Using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors. Journal of Interactive Marketing, 39, pp.27-38.
89. Myers, M.D. (1997). Critical ethnography in information systems. In Information systems and qualitative research (pp. 276-300). Boston: Springer.
90. Mysore, K., Elmualim, A. and Kirytopoulos, K. (2019). The Influence of Themes of Interplay on Multistakeholders Engagement Amidst Adversities in Globally Distributed ICT Projects–A Case Study Approach. Journal of Global Information Technology Management, pp.1-23.
91. Nfuka, E.N. and Rusu, L. (2011). The effect of critical success factors on IT governance performance. Industrial Management & Data Systems, 111(9), pp.1418- 1448.
92. Nicho, M., Khan, S. and Rahman, M.S.M.K. (2017), September. Managing information security risk using integrated governance risk and compliance. In 2017 International Conference on Computer and Applications (ICCA) (pp. 56-66). IEEE.
93. Nicho, M. and Khan, S. (2017). IT governance measurement tools and its application in IT-business alignment. Journal of International Technology and Information Management, 26(1), pp.81-111.
94. Olawumi, T.O. and Chan, D.W. (2019). Development of a benchmarking model for BIM implementation in developing countries. Benchmarking: An International Journal, 26(4), pp.1210-1232.
95. Organisation for Economic Co-operation and Development (2012). Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National
96. Cybersecurity Strategies for the Internet Economy. Paris: OECD Publishing.
97. O'Sullivan, E., Berner, M., Taliaferro, J.D. and Rassel, G.R. (2017). Research methods for public administrators. Oxon: Routledge.

ISBN- 978-978-57388-7-2

98. O'Sullivan, E. (2016). Practical Research Methods for Nonprofit and Public Administrators, Instructor's Manual (Download only). Oxon: Routledge.
99. Pal, R., Golubchik, L., Psounis, K. and Hui, P. (2014), April. Will cyber-insurance improve network security? A market analysis. In IEEE INFOCOM 2014-IEEE Conference on Computer Communications (pp. 235-243). IEEE.
100. Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N. and Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and policy in mental health and mental health services research, 42(5), pp.533-544.
101. Parn, E.A. and Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. Engineering, Construction and Architectural Management.
102. Pascal, A., Aldebert, B. and Rouzies, A. (2018). Mixed methods in information systems research: epistemological and methodological challenges. Systèmes d'Information et Management (French Journal of Management Information Systems), 23(3).
103. Pawlak, P. and Barmpaliou, P.N. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. Journal of Cyber Policy, 2(1), pp.123-144
104. Pearce, A., Pons, D. and Neitzert, T. (2018). Implementing lean—Outcomes from SME case studies. Operations Research Perspectives, 5, pp.94-104.
105. Peterson, R. (2004). Crafting information technology governance. Information systems management, 21(4), pp.7-22.
106. Peterson, R.R. (2001), January. Configurations and coordination for global information technology governance: complex designs in a transnational European context. In Proceedings of the 34th Annual Hawaii International Conference on System Sciences (pp. 10-pp). IEEE.
107. Porter, M.E. and Kramer, M.R. (2019). Creating shared value. In Managing sustainable business (pp. 323-346). Dordrecht: Springer.
108. Porter, M.E. (2008). Competitive strategy: Techniques for analyzing industries and competitors. New Jersey: Simon and Schuster.
109. Puklavec, B., Oliveira, T. and Popovič, A. (2018). Understanding the determinants of business intelligence system adoption stages: An empirical study of SMEs. Industrial Management & Data Systems, 118(1), pp.236-261.
110. Rahimi, F., Møller, C. and Hvam, L. (2016). Business process management and IT management: The missing integration. International Journal of Information Management, 36(1), pp.142-154.
111. Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M. and Peersman, C. (2018). Scoping the Cyber Security Body of Knowledge. IEEE Security & Privacy, 16(3), pp.96-102.
112. Ribbers, P.M., Peterson, R.R. and Parker, M.M. (2002), January. Designing information technology governance processes: diagnosing contemporary practices and competing theories. In Proceedings of the 35th annual Hawaii international conference on system sciences (pp. 3143-3154). IEEE.

113. Robinson, N. (2005). IT excellence starts with governance. Journal of investment compliance, 6(3), pp.45-49.
114. Saeidi, P., Saeidi, S.P., Sofian, S., Saeidi, S.P., Nilashi, M. and Mardani, A. (2019) The impact of enterprise risk management on competitive advantage by moderating role of information technology. Computer Standards & Interfaces, 63, pp.67-82.
115. Safa, N.S., Von Solms, R. and Furnell, S. (2016). Information security policy compliance model in organizations. computers & security, 56, pp.70-82.
116. Saini, H., Rao, Y.S. and Panda, T.C. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), pp.202-209.
117. Sallé, M. (2004). IT Service Management and IT Governance: review, comparative analysis and their impact on utility computing. Hewlett-Packard Company, pp.8-17.
118. Sambamurthy, V. and Zmud, R.W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. MIS quarterly, pp.261-290.
119. Sandberg, A. (2019). There is plenty of time at the bottom: the economics, risk and ethics of time compression. foresight, 21(1), pp.84-99.
120. Saunders, M., Lewis, P. and Thornhill, A. (2007). Research methods. Business Students. London: Pearson.
121. Savage, J.E. and McConnell, B.W. (2015). Exploring Multi-Stakeholder Internet Governance. Brown University Bruce W. McConnell, EastWest Institute. https://www. eastwest. ngo/sites/default/files/Exploring% 20Multi-Stakeholder% 20Internet% 20Governance_0. Pdf (Accessed: 17 November 2020).
122. Scheepers, R.A., Lombarts, K.M., Van Aken, M.A., Heineman, M.J. and Arah, O.A. (2014). Personality traits affect teaching performance of attending physicians: results of a multi-center observational study. PLoS One, 9(5), p.e98107.
123. Scoones, I., Edelman, M., Borras Jr, S.M., Hall, R., Wolford, W. and White, B. (2018). Emancipatory rural politics: confronting authoritarian populism. The Journal of Peasant Studies, 45(1), pp.1-20.
124. Sender, H. (2016). US Defence: Losing its edge in technology?. Financial Times. Available at: https://www.ft.com/content/a7203ec2-6ea4-11e6-9ac1-1055824ca907 (Accessed: 18 November 2020).
125. Shackelford, S.J. (2012). Should your firm invest in cyber risk insurance?. Business Horizons, 55 (4), pp.349-356.
126. Shirazi, S.N., Gouglidis, A., Farshad, A. and Hutchison, D. (2017). The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective. IEEE Journal on Selected Areas in Communications, 35(11), pp.2586-2595.
127. Siebert, S. ed. (2017). Management Research: European Perspectives. Oxon: Routledge.
128. Silva, D., da Silva, M.M. and Pereira, R. (2018), July. Baseline Mechanisms for Enterprise Governance of IT in SMEs. In 2018 IEEE 20th Conference on Business Informatics (CBI)(Vol. 2, pp. 32-41). IEEE.
129. Silverman, D. ed. (2016). Qualitative research. London: Sage.
130. Singh, H. and Montgomery, C.A. (1987). Corporate acquisition strategies and economic performance. Strategic Management Journal, 8(4), pp.377-386.

131. Song, M., Pan, X., Pan, X. and Jiao, Z. (2018). Influence of basic research investment on corporate performance: Exploring the moderating effect of human capital structure. Management Decision.
132. Ştefănescu, M.V. (2015). The information technology role in the dynamics and evolution of SMEs in Timis County, Romania. Procedia Economics and Finance, 32, pp.1107-1113.
133. Sutton, D. (2017). Cyber Security: A Practitioner's Guide. Swindon: BCS Learning & Development Limited.
134. Tan, W.G., Cater-Steel, A. and Toleman, M. (2009). Implementing IT service management: a case study focussing on critical success factors. Journal of Computer Information Systems, 50(2), pp.1-12.
135. Thompson, K. and Nesci, C. (2016). Over-riding concerns: Developing safe relations in the high-risk interspecies sport of eventing. International review for the sociology of sport, 51(1), pp.97-113.
136. Tiirmaa-Klaar, H., (2016). Building national cyber resilience and protecting critical information infrastructure. Journal of Cyber Policy, 1(1), pp.94-106.
137. Timmers, P. (2018). The European Union's cybersecurity industrial policy. Journal of Cyber Policy, 3(3), pp.363-384.
138. Van Grembergen, W. and De Haes, S. (2018). Introduction to the Minitrack on IT Governance and its Mechanisms. Available at: https://scholarspace.manoa.hawaii.edu/bitstream/10125/50500/paper0613.pdf (Accessed: 20 December 2020)
139. Van Grembergen, W., De Haes, S. and Guldentops, E. (2004). Structures, processes and relational mechanisms for IT governance. In Strategies for information technology governance (pp. 1-36). Pennsylvania: IGI Global.
140. Vejseli, S., Rossmann, A. and Connolly, T. (2019), January. IT Governance and It Agile Dimensions. In Proceedings of the 52nd Hawaii International Conference on System Sciences
141. Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38 , pp.97-102.
142. Walliman, N. (2017). Research methods: The basics. Oxon: Routledge. Webb, P., Pollard, C. and Ridley, G. (2006), January. Attempting to define IT governance: Wisdom or folly?. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) (Vol. 8, pp. 194a-194a). IEEE.
143. Weber, V. (2018). Linking cyber strategy with grand strategy: the case of the United States. Journal of Cyber Policy, 3(2), pp.236-257.
144. Weerasinghe, K., Scahill, S.L., Taskin, N. and Pauleen, D.J. (2018). Development of a Taxonomy to be used by Business-IT Alignment Researchers. Development, 6 , pp.26-2018.
145. Weerasinghe, K., Pauleen, D., Scahill, S. and Taskin, N. (2018). Development of a Theoretical Framework to Investigate Alignment of Big Data in Healthcare through Social Representation Lens. Australasian Journal of Information Systems, 22 .
146. Weill, P. and Ross, J.W. (2004). IT governance: How top performers manage IT decision rights for superior results. Boston: Harvard Business Press.
147. Weill, P. (2004). Don't just lead, govern: How top-performing firms govern IT. MIS Quarterly executive, 3(1), pp.1-17.

ISBN- 978-978-57388-7-2

148. Weill, P. and Broadbent, M. (1998). Leveraging the new infrastructure: how market leaders capitalize on information technology. Massachusetts: Harvard Business Press.
149. Weimer, D.L. and Vining, A.R. (2017). Policy analysis: Concepts and practice. Oxon: Routledge.
150. Wilkin, C. (2012). The role of IT governance practices in creating business value in SMEs. Journal of Organizational and End User Computing (JOEUC), 24(2), pp.1-17.
151. Williams, C. (2014). Security in the cyber supply chain: Is it achievable in a complex, interconnected world?. Technovation, 34 (7), pp.382-384.
152. Woods, D. and Simpson, A. (2017). Policy measures and cyber insurance: a framework. Journal of Cyber Policy, 2(2), pp.209-226
153. Zarvić, N., Stolze, C., Boehm, M. and Thomas, O. (2012). Dependency-based IT Governance practices in inter-organisational collaborations: A graph-driven elaboration. International Journal of Information Management, 32(6), pp.541-549.
154. Zheng, N., Wei, Y., Zhang, Y. and Yang, J. (2016). In search of strategic assets through cross-border merger and acquisitions: Evidence from Chinese multinational enterprises in developed economies. International Business Review, 25(1), pp.177- 186.