Content Registered

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 5, No 4, December, 2019

Insights into Cyber Policies, Information Technology Governance (ITG) and, Multi-stakeholder Security Governance Scaling (MSGS) for Decision Makers within UK SME Aviation

Ademola, E. O.
Professor, BCS & CMI Subject Matter Expert
Principal Consultant
Power-Age Consulting
ojo_ademola@hotmail.co.uk (private)
emmanuelojoademola.academia.edu

ABSTRACT

A cyber policy can always be at an efficacy with the robust implementation of Information Technology Governance (ITG). Analysing the linkages that may exist between ITG and Information Technology Governance (ITG), together with the benefits of theorising scaling and scalability in such derivation is desirable in other to support decision making and identify framework impediments to implementing cyber policy in the SME Aviation. In this paper, we define the term cyber policy, discusses ITG and MSGS (a framework for cyber policy). We clarify the framework for cyber policy (including major reviews, strategic elements, and benefits of the cyber policymaking to different stakeholders). We also explore impediments to cyber policy implementation, evaluates frameworks and models on cyber policy implementation approaches with SME Aviation and justifies the need for secondary data in researching with the rising issues. We posited that when ITG and business policy aligned to entail lack of awareness of global and local threats to cybersecurity, inadequate security infrastructures and the need for more experts involved in decision making, there is the need for a new approach to cyber policy implementation for robust competitiveness

Keywords: Cyber Policies, Information Technology Governance (ITG), Multi-stakeholder Security Governance Scaling (MSGS), decision-makers, UK SME Aviation.

~~**Journal Reference Format:**~~
Ademola, EO (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 Behavioural Informatics, Social-Cultural and Development Research. Vol. 5 . No. 4, Pp 15-28 www.isteams/behavioralinformaticsjournal. Article DOI No - dx.doi.org/10.22624/AIMS/BHI/V5N4P2

1. INTRODUCTION

Considering the complexity that surrounds the definition of cyber policy, how could the implementation of the right industrial cyber system contribute to the robustness of multi-stakeholder governance approach? Sutton (2017) argues that a scholar and practitioner response to such an inquiry could support the argument for a working definition. Sutton's proposal would have been more intriguing if it was related to the cybersecurity capabilities of an organisation. GreenPope et al. (2010) argued that such an approach requires tightly choreographed activities across organisations in diverse locations. The strategy accentuates the responsibilities of Airports Commission, Department of Transport, Ministry of Defense (MOD) and other Aviation security organisations; under which the synergy could culminate to an actionable framework. GreenPope and colleagues related the process to cybersecurity capacity of an organisation as well as provided a comprehensive input to the implementation of any sufficing cyber policy.

Aggarwal and Reddie (2018) evaluate the role of businesses, governments, other critical stakeholders in the emergence of a definition for cyber industrial policy. By corroborating Senders (2016) view; Aggarwal and Reddie found 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. Sender's, and Brantly advised that there is a need for relevant theory to conceptualise such definition. Matten and Moon (2008) articulated that the conceptual framework is not to overlook the impact of the outcome on the social or business environment; however, O'Sullivan (2016) adduces that stakeholders may use the information from such engagement to decide on events to support and what policies to promote. Brantly (2019) asserts that "policies and laws developed for rapidly evolving or dynamic business environments often overlook the impact or lack, therefore, complexity on the potential outcomes." According to this clarification, to define cyber policy with the understanding of ITG frameworks implementation suffices. Robinson (2005) points out that when governance is effective, Information Technology (IT) becomes a valued asset, not a cost.

Notwithstanding, if a cyber-security framework could help to conceptualise definitions appropriately, Brantly (2019) alludes to cyber policy implementation as an essential element of IT and business policy alignment. For the stakeholder, such description of a cyber policy could help to advocate for its implementation (Von Solms and Van Niekerk, 2013; Brantly, 2019; Safa et al., 2016). Furthermore, such conceptual foundation could provide a pathway to solution analysis (Weimer and Vining, 2017). There might be complications in clarifying various dynamism within the use of appropriate theory and environment. For example, in the UK Aviation, the divergent of methods and their applicability to SMEs could become complicated.

However, Brantly's provision of a decisive template to define cyber policy alludes to the Von Solms and Van Niekerk, 2013's definition of cybersecurity; and provides support for Weimer' and Vining' policy solution analysis. The definition centres on the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, the organisation, and user assets (Ibid.). The view is consistent with the operational definition of cyber strategy expressed in the latest Aviation Strategy that captures the centrality and efficacy of the UK as the most significant internet economy in the G20 (Carr and Tanczer, 2018).

2. LINKAGES BETWEEN ITGS AND MULTI-STAKEHOLDER SECURITY GOVERNANCE SCALING (MSGS)

A critical analysis of the literature informed this secondary data research for this qualitative study. The identification of cybersecurity strategies indicates SMEs' decision-makers implement a protectable cyber policy (OECD, 2012). In 2005, the UK National Computing Centre published a report on developing a successful governance strategy (Manchester. National Computing Centre, 2005, pp. 5-6). The publication indicates that for an organisation to deliver an overall business goal, its investment in IT must provide full value. The report underscores that decision-makers in IT must ensure that investment must recognise that technology is incorporated fully into business strategies and direction. The publication indicates the importance of identifying and controlling critical risks as well as a full demonstration of legislative and regulatory compliance.

The report points out that ITG covers all the elements underlined. There are underlining weaknesses in the approach to implementing ITG in SMEs noting the apparent emergent of recent corporate failures. Undoubtedly, such shortcomings are not diminishing but appreciate a higher profile today than at any time in recent memory. However, Webb et al. (2006) suggested that in the attainment of a broad-reach outcome in business objectives, the definition of ITG must be context-based. The existing definitions have accentuated different things to different organisations. Notwithstanding, ITG provides a formal way to align IT and business strategy.

Accordingly, there are various regulations for organisations to be compliant within different locations of business operations. The view remains consistent with De Haes and Grembergen's (2009) assertion that IT decision-makers must achieve a full business/IT alignment maturity.

Subsequently, questions also arise due to the coherence of various elements that ITG covers. According to De Haes and Van Grembergen (2006), ITG includes alignment, value delivery, risk management, resource management and performance management. Necessarily, an organisation should identify possible stakeholders in the implementation of ITG to achieve a measurable performance of better alignment between business and IT. Banham and He (2010) argues that in SME governance, definitions of ITG converge, business expectations must expand to accommodate appropriate alignment. Considering SMEs' limited resources, Banham and He identified that proper implementation of a cyber policy could provide a possible relational pathway. The exploration between implementable ITG and multi-stakeholders' commitment irrespective of challenges arising from IT/Business alignment also in the view, according to De Haes and Van Grembergen.

Nonetheless, how could the implementation of the right industrial cyber policy contribute to the robustness of multi-stakeholder governance approach? From operation research approach, Pearce et al. (2018) assert that lean adoption could be helpful to SMEs' decision-makers to bridge the gap that exists in the implementation of ITG. The study points out that using Lean Implementation (LI) as a scaling technique could improve a lead to conceptualising ITG framework. Such an outcome might serve as an input to implementing cyber policy within SMEs in the automobile industry.

According to Pearce et al., resources are rare in SMEs for such exploration. However, Vejseli et al. (2019) argue that agile dimension to the implementation of ITG could be a contributing factor to the LI's concept. By deduction, with the UK's SME Aviation, GreenPope et al. (2010) contend that such a methodology requires firmly arranged exercises crosswise over associations in various areas. The technique involves the duties of Airport Commissions, Department of Transport, Ministry of Defense (MOD) and other Aviation security associations; under which the cooperative energy works. Aggarwal and Reddie (2018) assess the job of organisations, governments and other related partners in the rise of modern strategy by authenticating Sender's (2016) assertion. There is a developing acceleration of the geopolitical setting in digital approach substance of politically influential nation to vital challenge.

GreenPope and colleagues assert that the approach explores the implementation of cyber policy as a linkage between ITG and MSGS. Furthermore, it could anchor the widespread use of the internet as a global venue for international cybercrime. Implementation of effective Cyber policy is the linkage that exists between ITG and MSGS with the adoption of LI, considering the limited resources available to SMEs. The assertion centres on the provision of technical and security pathway to IT/business alignment (De Haes and Van Grembergen, 2006; see also De Haes and Van Grembergen, 2006 and Webb et al., 2006). Hubbard and Seiersen (2016) indicate that in measurement, implementation of an effective cyber policy (as a linkage between ITG and MSGS) will contribute to the concept of "uncertain reduction."

Security vendors McAfee Intel Security and Symantec Corporation proposed a cost implication framework which is comparable to Bernik's (2014) framework. The report points out that there is a cost implication; mainly, due to variants approach to the implementation of cyber policy. Hyman (2013) asserts that the outcome of inadequate implementation of appropriate cyber policy in organisations could become unbearable to organisations. Hyman furthers the report that Symantec Corporation accentuated that cyber breaches cost the globe $110 billion annually. As McAfee Intel Security reported worldwide cybercrime costs of $1 trillion yearly. The report highlighted differential factor in figures with those of Symantec Corporation. The former's focus on both malicious and accidental data losses for businesses worldwide depends mainly on the contribution from SMEs. The uncertain reduction approach in measurement could align assertively to the MSGS approach (Hubbard and Seiersen, 2016).

The cost-implication effect and the increase of cyber-attack on SMEs is an indication of an advanced threat to an SME's bottom line. According to GlobalData (2017) report based on UK SME's; it points out that the uptake by UK SMEs grew from 2.1% in 2014 to 13.7% in 2016 which is a considerable increase, but the coverage remains low at 13.7%. Shackelford (2012) distinguished cyber risk protection as an instrument to oversee obligation and relieve the peril of cyberattacks. Protection arrangements cover losses from cyberattacks and information breaks. Shackelford demonstrated that interest in cyber risk insurance should be an encouragement to cyber policy decision-makers. The recommendation remains emphatic as UK SMEs dependent on the digital space, and crime is moving exponentially to online. The Competition and Markets Authority (CMA), in its response to UK Aviation 2050, agrees that "There is scope to improve passenger experience and embedding protections is a step forward." This suggests that there is a greater need for cyber insurance as an MSGS technique within the cyber policy (Pal et al., 2014; see also Lelarge and Bolot, 2009 and Saini et al., 2012).

Shackelford's suggestion that an organisation's primary interest in cybersecurity is in system and framework, including firewalls, encryption, and interruption recognition. Digital hazard protection is a device used to return misfortunes that outcome from a cyberattack; however, proactive digital systems ought to consistently be the beginning stage (Shackelford, 2012). Hayes and Bodhani (2013) recognised SMEs as progressively focused on online dangers. Cybercriminals effectively search for chances to stamp these easy objectives. SMEs with restricted data innovation assets have not set fitting interests in cybersecurity. In cases in which medium-sized to huge ventures have kept up business associations with SMEs, cybercriminals have assaulted the SME as the apparent, more fragile connection. Hayes and Bodhani inferred that generally, digital strategy chiefs of SMEs don't comprehend cybersecurity as an issue for them. The discernment that cybersecurity as a test just for enormous ventures is still unavoidable in SMEs. According to Hayes and Bodhani, SMEs were progressively the objective of cybercrime. Cyber hoodlums are attempting to target the most significant investments. The inference is to the massive undertakings that could assume an obligation in giving cyber policy decision-makers support to their SME affiliations.

3. SCALING AND SCALABILITY MECHANISMS RELATED TO DECISION MAKING STRATEGY

In 2002, the OECD made recommendations for the Security of Information Systems and Networks to underscore a Culture of Security. The Security Guidelines were the first international set of fundamental principles to focus on the dynamism of security policies in an open environment. According to Azmi et al. (2018), the OECD's 2002 security policies guidelines provided a template for the organisational culture of security as well as directions for both public and private sectors to adopt scaling in appropriation to their own cybersecurity policy needs.

There are lacking guidelines as to achieving scalability either to scale up or out (OECD, 2002). Azmi and colleagues asserted that the OECD's 2012 presents the comparison of national cybersecurity strategies to accentuate "a useful source of information and inspiration in the context of the review of the Guidelines." The critique could be on the submission that the concept of MSGS might provide a balance to processes of profiling, assuring and delivering cybersecurity. To decision-makers, achieving scalability via scaling is a drive towards more robust evidence-based policy decision-making, as predicated in OECD (2012). Such an approach is also essential to achieving scalability. The guideline emphasises that this could be possible via the culture of cybersecurity as advanced in both OECD's (2002, 2012) guidelines (Azmi et al., 2018; Pawlak and Barmpaliou, 2017 and Tiirmaa-Klaar, 2016. The ITAC**'s** response to the OECD's (2012) analytical report shows that MSGS would be a helpful scaling approach for decision-makers in the achievement of scalability in SMEs.

In the OECD (2012), the scaling approach will be the bedrock to a very significant evolution in government strategies to the adoption of the multi-stakeholder model for policy development in general. According to Carr and Tanczer (2018), market failures occurs as a result of functional declines. Cyber policymakers must be cautious of the data breaches, inadequate private investments, and a continuous digital skills gap.

The authors provide an illustrative case study for the evolution of industrial cybersecurity policy. Theoretically, this is an attempt to advocate for the achievement of scalability either by scaling up or scaling out automation security architecture in UK sectors. According to The McKinsey Global Institute (2019), "Process automation at scale is now feasible for most payers." The analysis shows that Automation at scale is an approach beneficial to payers, and decision-makers across business divide either large enterprise or SMEs. Manyika (2017) indicates that Automation-at-scale could solve the problem associated with increasing cost pressure. The pushing of SMEs to significantly improve business operations even at the business experience of unexpected data breaches.

Manyika noted the benefits of scaling to payers and employers but failed to acknowledge the problem with scaling up. Decision-makers must find the right balance of resources in the implementation of cyber policy as this remains an extreme difficulty for SMEs. The concept of adding up IT critical infrastructure to achieve a business objective could be a bottleneck. For example, to add more security awareness clauses to an existing policy could directly impact on the cost of implementing such architecture. The theory of unavoidable losses - the dictate of the law of diminishing could kick in quickly. Subsequently, this could cause the value of incremental upgrades to the existing policy to grow exponentially (Porter and Kramer, 2019; see also Sandberg, 2019 and Aldrich and Wiedenmayer, 2019).

The consideration of the cost-to-benefit ratio will make scaling up a very unattractive option. Scaling out, on the other hand, implies that scaling the security application via scalability mechanism could be possible. For example, by adding more machines to the system and allowing them to share the load within the ITG implementation could have a scale-up effect. Azmi et al. (2018) assert a shared concept approach as scaling out and significantly beneficial to decision-makers. In November 2011, the UK government published its first National Cyber Security Strategy (NCSS). By implementation, the legislature had numerous proactive and responsive measures to upgrade the two of its cybersecurity abilities. The market control in this area serves as a scaling rule to help cybersecurity chiefs as the legislature will discharge speculations.

According to the Cabinet Office (2011, 2016a), £860 million for its National Cyber Security Program (NCSP) for the period from 2011 to 2016 suffices and supported its spending to £1.9 billion for its cybersecurity vision from 2016 to 2021. According to Matthews (2019), the implementation provides for evidence-based policymaking. The author focuses on the centrality of ITG implementation. MSGS advocacy could lean on collaboration by stakeholders. Such provides the strategy - an incorporated for the foundation of another National Cyber Security Centre (NCSC) that goes about as the open arm of GCHQ. UK's MOD concurred with the Cabinet Office another 25% objective for SME obtainment by 2020. The responsibility reflected in the Single Departmental Plan distributed on nineteenth February 2016. The NCSC offers an interface among government and industry and gives direction just as exhortation (Carr and Tanczer, 2018).

4. SCALING AS A SECURITY TO SUPPORT CYBER POLICY DECISION MAKERS

Ribbers et al. (2002) conclude that despite the numerous literature on ITG, the gap still exists on the practical implementation of the available models tailored to specific industrial sectors. The comprehensive theoretical frameworks mostly patterned around the theories while there is little on the actual processes involved with ITG. Mainly, the models do not suffice how the processes translate to contemporary practice. Over the last five decades, the three primary schools of thought on ITG in the literature still prevails – (1) ITG as a framework or an audit process, (2) ITG as IT decision-making, and (3) ITG as a branch of corporate governance. Nonetheless, it appears that the primary schools of thought show some emergent theories of corporate strategies. In general, it rarely includes security strategy (Lynch and Smith, 2006; see also Doyle, 1989 and Badr et al., 2010). Notwithstanding, the provisions of the main theories of corporate strategy (Ribbers et al., 2002), in the 1970s, analysis show that there is a rare correlation between the comparative industrial policy and security (Aggarwal and Reddie, 2018; see also Singh and Montgomery, 1987 and Zheng et al., 2016).

Furthermore, some writers suggest that ITG frameworks implemented by middle managers are to facilitate the associated IT management processes and related internal IT controls. (e.g. Rahimi et al., 2016; see also Bergeron et al., 2017 and Nicho et al., 2017). Such a view of ITG reinforces the needs for regulatory controls and privacy (Eastin et al., 2016). Dynamically, such reinforcement underscores a move away from achieving corporate governance through voluntary disclosure, and towards the regulation of exposure and, more generally, corporate conduct with effective industrial policy for the digital space (Aggarwal and Reddie, 2018; see also D'Elia, 2018 and Mosteller and Poddar, 2017).

The approach places huge security responsibilities on the decision-makers, in the areas of transparency, integrity and accountability in business operations, and the system of internal control (Shirazi et al., 2017; de Mingo and Cerrillo-i-Martínez, 2018). However, the approach could deal only with a small part of the total ITG obligations of decision-makers; primarily those with verification responsibility like CoBIT, ITIL, ISO/IEC 27001 (2005a), ISO/IEC 17799 (2005b), BS 7799 (2000) (Aasi et al., 2017). These structures are not elective medications of similar issues; without a doubt, there is little cover between them. Most of the writing worried about these systems is down to earth in nature; there is a rare discussion of them in scholarly literature.

CoBIT is a restrictive way to deal with executing and assessing controls in the IT setting (ITGI, 2002; Ştefănescu, 2015). It is a regularising structure that consists of 34 in general control targets. These partitioned into a chain of command of auditable procedures planned to help a sum of 318 point by point control destinations. CoBIT gives various devices to help with overseeing IT. The implementation includes that of measures and essential achievement factors for the administration procedures, and development models to push associations to benchmark their exhibition in dealing with their IT environment. The CoBIT perspective on IT administration helps to ensure that IT conveys an incentive to the business and in relieved of IT challenges (ITGI, 2002; Delgado and Velthuis, 2015).

CoBIT is helpful as a guide to operational supervisors executing an IT anticipation. Mainly as an apparatus for evaluating the arrangement of business alignment and IT targets (Mora et al., 2016; see also Sallé, 2004 and Tan et al., 2009). The emergence of digital transformation, DevOps, as well as the current business trend, underpinned by the common security issues, justify the continue evolution COBIT, to implement a re-alignment. The COBIT®2019 adopt an approach that imbibes the scaling mechanism for the framework to remain relevant.

COBIT must continue to evolve, requiring either scaling up for large enterprise or scaling down for SMEs due to more frequent and fluid updates (Olawumi and Chan, 2019). The COBIT®2019 also present symbolism of continuous security review to ensure effective version control, upgrades and scaling corresponding to the release of the most updated guidance (Leszczyna, 2018).

ITIL is designed for evaluating the IT exercises of government organisations (Sallé, 2004; Tan et al., 2009). The ITIL library is a set of "best practice" guidelines for IT administration for the executives. ITIL is worried about the fundamental of business procedures expected to give astounding IT administrations (Iden, 2009; Cater-Steel and Toleman, 2010); however, it does not fret about strategic key issues (Sallé, 2004; Tan et al., 2009). ITG reports show there is a veritable industry in programming devices, accreditation, review, preparing and counselling on ITIL ISO/IEC 27001 (2005a), ISO/IEC 17799 (2005b) and BS7799-2 (2000).

The framework helps to accentuate a scaling approach for ITG strategists as these models focus on Information Security Management. Such ITG is for specialised decision-makers to oversee, starting, executing, and keeping up data security inside their associations (Rahimi et al., 2016). Furthermore, the ISO/IEC 27001:2005 (ISO 2005a) is used as detailing for data security within the IT security framework as well as ISO/IEC 17799:2005 (ISO, 2005b) for the code of training for actualising information security within the extensive framework. ISO/IEC 27001 as a security ITG, provide business with the opportunity for information security and safety confirmed by autonomous assessor against the prerequisites of the Standard.

Notwithstanding, one ITG may not provide an alternative in implementation as there is a little element that overlaps between the three as new theories advances (Van Grembergen et al., 2004). The frameworks do not consider the broad perspective on IT administration; instead, they portray one viewpoint or other of the idea (Webb et al., 2006; Dahlberg and Kivijarvi, 2006). The COBIT®2019 structure tends to the most recent technological advances, and security requirements for ventures including other ITG; for example, ITIL, CMMI, and TOGAF. Like COBIT®5, COBIT®2019 likewise underscores explicitly on security, risk management, and data administration. The COBIT®2019 system aides guaranteeing viable EGIT, encouraging simpler, and customised usage. In that capacity, is reinforcing COBIT®'s proceeding as a significant driver of advancement and business change (Leszczyna, 2018; Olawumi and Chan, 2019).

However, the risk associated with SMEs application of the ITG frameworks in term cost could lead to the espouse of various theories. The description could produce unwanted outcomes, as the Standard does not seem to consider the strategic opportunities for decision-makers that IT could afford (Bergeron et al., 2015). The risks of IT to be mainly managed as some ITG frameworks are into practical use by the SMEs. The process could make ITG a dominant view for the decision-makers (Peterson et al., 2002). The analysis could broadly show that there is a gap between the application of ITG theories and the reality of SMEs (Bergeron et al., 2015; Wilkin, 2012). Notwithstanding, the allocation of decision rights and accountability to encourage desirable behaviour in the use of IT; the theories still give direction for implementation (e.g., Weill and Broadbent, 1998; Weill, 2004).

The theories with lower practice of ITG in SMEs espouse from the Agency theory, Stakeholder theory and Power perspective with the adoption of LI could make it plausible (Alkhoraif, 2018; Bergeron et al., 2015). The outcome of such exercise could provide the linkage between the cyber strategy with grand strategy within the design of cyber policymaking (Weber, 2018). Such a view perceives ITG as a model that focuses on the management and delivery of IT services to enterprises irrespective of the size (Peterson, 2003; see also Bergeron et al., 2015 and Alkhoraif, 2018). On the locus of the IT decision-making authority within an organisation, it remains helpful as a multi-stakeholder approach emphasised in OECD (2002, 2012).

Early works indicated a similar trend that the governance structure for a business depended on several factors (e.g. Brown, 1997; Sambamurthy and Zmud, 1999; Weill, 2004; Weill and Woodham, 2002). Brantly (2019) asserts the usefulness of complexity theory in the design of the cyber policy.

In any case, this possibility approach was perplexing and hard to apply practically speaking. The association of the variables was a staying point; numerous authors accepted that the elements would not collaborate (notably Henderson and Venkatraman, 1994; see also Weerasinghe et al., 2018 and Weerasinghe et al., 2018). With accentuation, the authors justify scaling of a type. Those authors who assumed cooperation created systems of multifaceted frameworks (e.g. Sambamurthy and Zmud, 1999; Coltman et al., 2015; Gregory et al., 2018; Brantly, 2019).

Consequentially, the measurement of performance of IT security processes and or controls is a critical operational aspect of ITG from an integrated ITG framework perspective (Dahlberg and Kivijarvi, 2006; Hubbard and Seiersen, 2016). The measurement consideration tends as one of the two operating functions of ITG to explicitly launch with business-IT alignment in the arranging stage that guidingly affected the working stage. The monitoring of IT resources, risks, and management gain traction by the selection of appropriate IT performance measurement tools, which ultimately affects the benefits, costs, opportunities, and risks (Hubbard and Seiersen, 2016). Hence, the scaling could espouse the LI as a MSGS advocated in OECD (2012).

In the deployment of ITG, the use of a mixture of structures, processes and relational mechanisms is active with the multi-stakeholder approach. The arrangements are devices and tools for connecting business and IT; methods refer to IT monitoring the procedure, while relational mechanisms relate to participation and collaboration between management (De Haes and Grembergen, 2009). ITG frameworks, as the repositories of IT-effectiveness knowledge, organisations over time develop a shared culture of behaviours, values and expectations about their IT processes (Nicho and Khan, 2017; Gregory et al., 2018).

Thus, integrating the two models to benefit assessment enable decision-makers to facilitate the functionality of scaling through the structures. Additionally, it embeds the processes of ITG measurement tools in the operating phase of integrated ITG framework (De Haes and Grembergen, 2009; see also Gregory et al., 2018 and Bergeron et al., 2015). Thus, theorising scaling is a relational mechanism in the apt of participation and collaboration among management and not entirely on measurement. Such a construct should serve as an input to cyber policy decision-making processes (Woods and Simpson, 2017).

5. EMERGING ISSUES AND NEED FOR SECONDARY DATA EXPLORATORY RESEARCH

The study of cyber policy concerning implementable ITG in SMEs literature showed that the study area is a complex and dynamic landscape. Firstly, there is no universal definition, although there is consistency in the implementation of various ITG. The description highlights a functional characterisation of cyber policy. The definition underscores correlations within the multi-stakeholder elements to understand the application of ITG in SMEs and to support cyber policy decision-makers. There are many strategic identifications of cybersecurity elements; for instance, seen diminished costs, access to sizeable IT infrastructure, cyber policy specialised decision-makers, etc.), and the long-term benefits to SMEs' decision-makers (such as implementable ITG, the flexibility of MSGS, robust internal investigation to data breach incidents, etc.).

The implementation of a protectable cyber policy stands out as SMEs remain susceptible to continuous malicious attack, especially the UK's SME Aviation. The review of literature stressed the need for an implementable cyber policy as the real linkage between ITG and MSGS (Aggarwal and Reddie, 2018; Banham and He, 2010; De Haes and Van Grembergen, 2006, 2009; GreenPope et al., 2010; Webb et al., 2006). With the accentuation on scaling and scalability mechanism in the implementation of ITG, decision-makers would find the organisational culture of security as consistently helpful as accessibility is almost effective (OECD 2002, 2012).

For decision-makers to accommodate such paradigm, the most support structure highlighted by research was the offer of a shared concept of scaling to both security scholars and practitioners to prepare decision-makers with the technical impetus in the implementation of cyber policy. However, there was literature evidence that decision-makers must be specialised security personnel to meet such obligations. There are concerns that SMEs may not have skilled cyber policymakers. They may have to recourse to the more significant enterprise security specialists to meet the need for fulfilling the highlighted goals via scaling mechanisms.

In fulfilling this role, decision-makers need both academic and expertise-based training in cyber policy. There are offers of an interface among government and industry to empower specialised security chiefs (Carr and Tanczer, 2018). The ITG systems available to SMEs were reviewed. Useful guidelines identified to evidence the need to bridge the gap that exists on the practical implementation of the available models to SMEs cyber policy decision-makers. The helpful guidelines provision paths to tailor ITG systems to specific industrial sectors.

With this essentiality, the risk associated with SMEs application of the ITG frameworks in term of the cost could help decision-makers to adopt MSGS both in the espouse of various theories with a view for strategic business alignment of goals (Bergeron et al., 2015; De Haes and Grembergen, 2009; OECD 2002, 2009; Gregory et al., 2018; Nicho and Khan, 2017; Woods and Simpson, 2017). However, the ITG implementations are helpful to decision-makers. With this approach, it focuses mostly on large enterprises. Where suggestions are available to SMEs; they were dependent on the provisions from the more massive corporation. Useful bits of advice are available to SMEs, but there are needs to accentuate the preparedness of decision-makers to implement ITGs as SMEs consistently being attacked.

6. CONCLUDING REMARKS

In this paper, we have addressed issues relating to Cyber Policies, Information Technology Governance (ITG) and Multi-stakeholder Security Governance Scaling (MSGS) for decision-makers within UK SME Aviation. A vital issue for the development and deployment of implementable cyber policy in UK's SME Aviation is the suggestions on strategic directions ought to be an outcome of the research. There are various means available to decision-makers that lean on various professional discussions and assumptions. There is a need to arrive at a deeper understanding of how to formulate helpful recommendations on cyber policy implementation challenges in the UK's SME Aviation industry.

Exploratory research will be conducted to specifically attempt to find out how the vulnerability of ITG models and MSGS correlate to supporting decision-makers. Also, to accentuate the emerging issues on the domain of strategic directions for the successful implementation of cyber policy within the UK's SME Aviation sector. The next stage of this study will detail the Research Methods in use to capture the secondary data, including details on the research strategy and the overall management of the researcher's role.

REFERENCES

1. Aasi, P., Rusu, L. and Leidner, D., 2017. IT organisational structure relationship with IT governance performance: case of a public organisation. In *Information Technology Governance in Public Organizations* (pp. 229-252). Springer, Cham.
2. 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.
3. Aldrich, H.E. and Wiedenmayer, G., 2019. From traits to rates: An ecological perspective on organisational foundings. In *Seminal Ideas for the Next Twenty-Five Years of Advances*(pp. 61-97). Emerald Publishing Limited.
4. Alkhoraif, A., 2018. Lean implementation in small and medium enterprises: Literature review. *Operations Research Perspectives*, p.100089.
5. Azmi, R., Tibben, W. and Win, KT, 2018. Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, *3*(2), pp.258-283.
6. 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.
7. Banham, H. and He, Y., 2010. SME governance: converging definitions and expanding expectations. *International Business & Economics Research Journal*, *9*(2), pp.77-82.
8. 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). IGI Global.
9. 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.
10. Bernik, I., 2014. Cybercrime: The Cost of Investments into Protection. *Varstvoslovje: Journal of Criminal Justice & Security*, *16*(2).
11. Brantly, A.F., 2019. Conceptualising cyber policy through complexity theory. *Journal of Cyber Policy*, pp.1-15. 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.
12. 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). IGI Global.
13. Coltman, T., Tallon, P., Sharma, R. and Queiroz, M., 2015. Strategic IT alignment: twenty-five years on.
14. 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.
15. D'Elia, D., 2018. Industrial policy: the holy grail of French cybersecurity strategy?. *Journal of Cyber Policy* , *3* (3), pp.385-406.
16. 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.
17. De Haes, S. and Van Grembergen, W., 2006, January. Information technology governance best practices in Belgian organisations. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (Vol. 8, pp. 195b-195b). IEEE.
18. 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.

19. 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.
20. Doyle, P., 1989. Markets and innovation. *European Management Journal*, *7*(4), pp.413-421.
21. Eastin, M.S., Brinson, N.H., Doorey, A. and Wilcox, G., 2016. Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior*, *58*, pp.214-220.
22. 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.
23. Gregory, R.W., Kaganer, E., Henfridsson, O. and Ruch, T.J., 2018. IT Consumerisation and the Transformation of IT Governance. *MIS Quarterly*, *42*(4), pp.1225-1253.
24. Hayes, J. and Bodhani, A., 2013. Cyber security: small firms under fire [InformatIon Technology Professionalism]. *Engineering & technology*, *8*(6), pp.80-83.
25. Henderson, J.C. and Venkatraman, N., 1994. *Strategic alignment: a model for organisational transformation via information technology* (pp. 202-220). Oxford University Press: New York.
26. Hubbard, D.W. and Seiersen, R., 2016. *How to measure anything in cybersecurity risk*. John Wiley & Sons.
27. Hyman, P., 2013. Cybercrime: it's serious, but exactly how serious?. *Communications of the ACM*, *56*(3), pp.18-20.
28. Iden, J., 2009. Implementing IT service management: Lessons learned from a university IT department. In *Information technology governance and service management: Frameworks and adaptations* (pp. 333-349). IGI Global.
29. 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.
30. Leszczyna, R., 2018. A review of standards with cybersecurity requirements for smart grid. *Computers & security*, *77*, pp.262-276.
31. Lynch, R.L. and Smith, J.R., 2006. *Corporate strategy*. Harlow, England: FT/Prentice Hall.
32. Manyika, J., 2017. A future that works: AI automation employment and productivity. *McKinsey Global Institute Research, Tech. Rep.*
33. Matthews, R. ed., 2019. *The Political Economy of Defence*. Cambridge University Press.
34. 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.
35. 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.
36. 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.
37. Nicho, M., Khan, S. and Rahman, MSMK, 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.
38. 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.
39. 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.
40. Organisation for Economic Co-operation and Development, 2012. *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. OECD Publishing.

41. O'Sullivan, E., 2016. *Practical Research Methods for Nonprofit and Public Administrators, Instructor's Manual (Download only)*. Routledge.
42. 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.
43. Pawlak, P. and Barmpaliou, P.N., 2017. Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy*, *2*(1), pp.123-144.
44. Pearce, A., Pons, D. and Neitzert, T., 2018. Implementing lean—Outcomes from SME case studies. *Operations Research Perspectives*, *5*, pp.94-104.
45. Porter, M.E. and Kramer, M.R., 2019. Creating shared value. In *Managing sustainable business* (pp. 323-346). Springer, Dordrecht.
46. Robinson, N., 2005. IT excellence starts with governance. *Journal of investment compliance*, *6*(3), pp.45-49. 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.
47. 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.
48. Safa, N.S., Von Solms, R. and Furnell, S., 2016. Information security policy compliance model in organisations. *computers & security*, *56*, pp.70-82.
49. Saini, H., Rao, Y.S. and Panda, TC, 2012. Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), pp.202-209.
50. Sallé, M., 2004. IT Service Management and IT Governance: review, comparative analysis and their impact on utility computing. *Hewlett-Packard Company*, pp.8-17.
51. Sambamurthy, V. and Zmud, R.W., 1999. Arrangements for information technology governance: A theory of multiple contingencies. *MIS quarterly*, pp.261-290.
52. 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.
53. 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: 8 July 2019).
54. Shackelford, S.J., 2012. Should your firm invest in cyber risk insurance?. *Business Horizons*, *55* (4), pp.349-356.
55. 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.
56. Singh, H. and Montgomery, C.A., 1987. Corporate acquisition strategies and economic performance. *Strategic Management Journal*, *8*(4), pp.377-386.
57. 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.
58. Sutton, D., 2017. *Cyber Security: A Practitioner's Guide*. BCS Learning & Development Limited.
59. 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.
60. Tiirmaa-Klaar, H., 2016. Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy*, *1*(1), pp.94-106.
61. 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). Igi Global.

62. Vejseli, S., Rossmann, A. and Connolly, T., 2019, January. IT Governance and Its Agile Dimensions. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.
63. Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security* , *38* , pp.97-102.
64. 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.
65. Weber, V., 2018. Linking cyber strategy with grand strategy: the case of the United States. *Journal of Cyber Policy*, *3*(2), pp.236-257.
66. 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.
67. Weerasinghe, K., Pauleen, D., Scahill, S. and Taskin, N., 2018. Development of a Theoretical Framework to Investigate Alignment of Big Data in Healthcare through a Social Representation Lens. *Australasian Journal of Information Systems*, *22* .
68. Weill, P. and Broadbent, M., 1998. *Leveraging the new infrastructure: how market leaders capitalise on information technology*. Harvard Business Press.
69. Weill, P., 2004. Don't just lead, govern: How top-performing firms govern IT. *MIS Quarterly executive*, *3*(1), pp.1-17.
70. Weimer, D.L. and Vining, A.R., 2017. *Policy analysis: Concepts and practice*. Routledge.
71. Williams, C., 2014. Security in the cyber supply chain: Is it achievable in a complex, interconnected world?. *Technovation*, *34* (7), pp.382-384.
72. 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.
73. Woods, D. and Simpson, A., 2017. Policy measures and cyber insurance: a framework. *Journal of Cyber Policy*, *2*(2), pp.209-226.
74. 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.