Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: www.tandfonline.com/journals/tbit20

An investigation into network theory and how the SDP logic model facilitates compliance and the safe handling of information

Yang-Im Lee & Peter R. J. Trim

To cite this article: Yang-Im Lee & Peter R. J. Trim (14 Jun 2025): An investigation into network theory and how the SDP logic model facilitates compliance and the safe handling of information, Behaviour & Information Technology, DOI: 10.1080/0144929X.2025.2507689

To link to this article: https://doi.org/10.1080/0144929X.2025.2507689

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2025.2507689

An investigation into network theory and how the SDP logic model facilitates compliance and the safe handling of information

Yang-Im Lee[a] and Peter R. J. Trim[b]

[a]School of Management and Marketing, Westminster Business School, University of Westminster, London, UK; [b]Birkbeck Business School, Birkbeck, University of London, London, UK

ABSTRACT

Social media communications technology (SMCT) helps managers to extend their networks and share information. Information security is essential as regards trust and compliance. This study explains how a secure digital platform (SDP), as an organisational intervention, instils confidence in managers to utilise SMCT and engage in information sharing that facilitates resource utilisation. A theoretical SDP framework was developed by utilising network theory in conjunction with the logic model approach. An online survey (n = 207) was analysed using SEM, AMOS. The results show that a designed-in governance mechanism (DGM) plays a pivotal role in ensuring compliance (DC); at the same time, a DGM positively influences the intention to use an SDP. Also, the subjective norm (SN) positively influences the intention to use an SDP. The deployment of an SDP positively enhances business capability through the use of SMCT. This is the first study that empirically tested how governance establishes the policies and frameworks that ensure compliance, which results in strengthening an SDP and enhances business capability. The finding of this study helps managers and platform developers understand the importance of establishing governance policy and its implementation in digital network platforms to influence/facilitate safe information sharing to enhance business capability.

ARTICLE HISTORY
Received 19 September 2024
Accepted 8 May 2025

KEYWORDS
Communications technology; Logic model; Network theory; Organisational intervention; Secure digital platform

1. Introduction

Social media communications technology (SMCT) provides managers with the opportunity to establish close relationships with customers (Daowd et al. 2020), suppliers, sellers and third parties (Constantinides, Henfridsson, and Parker 2020) through information sharing (Surucu-Balci, Iris, and Balci 2024). The acquired information and intelligence can feed into the new product development process (Liu et al. 2024). SMCT helps business-to-business managers extend their networking capability, manage innovation (Ogilvie et al. 2018) and increase resource capability by linking various organisational activities (Mola et al. 2023). This highlights the role that SMCT plays in how a firm can strengthen its capability to contribute to delivering value to its customers and achieve the desired marketing outcomes.

Nevertheless, the environment in which SMCT can be deployed presents challenges due to continuous innovative developments in technology (Moqaddamerad and Ali 2024) as well as a lack of standards and regulations (Surucu-Balci, Iris, and Balci 2024) that govern information use. An organisation's resource capability is affected by information sharing through successful supply chain integration (Bodendorf, Dentler, and Franke 2023), which is of growing importance. However, there is limited research regarding how to improve resource capability by reducing barriers associated with using SMCT through the deployment of governance and compliance. This is the gap in knowledge to be addressed. Hence, we explore the issue of governance and compliance – how senior managers put in place a system for governance and how this assists staff to be compliant. This approach is relevant. Bulgurcu, Cavusoglu, and Benbasat (2010) point out that reducing risk not only depends on the technology itself but also relates to staff compliance behaviour (Riahi and Islam 2024).

To undertake this research, we utilise the network theory in conjunction with the logic model approach. Network theory deals with issues that arise from mechanisms and processes that interact in network structure to yield certain outcomes (Borgatti and Halgin 2011). The work of Borgatti and Halgin (2011) is useful as they

CONTACT Yang-Im Lee y.lee@westminster.ac.uk Senior Lecturer in Marketing, School of Management and Marketing, Westminster Business School, University of Westminster, 35 Marylebone Road, London, NW1 5LS UK

Supplemental data for this article can be accessed online at https://doi.org/10.1080/0144929X.2025.2507689.

discuss two different network models – 'Granovetter's strength of weak ties theory' and 'Burt's structural hole theory', which help us to identify what are the important aspects that need to be given attention to have a successful network platform that enhances performance.

Safeguarding customer data remains a priority. The issue of client-customer trust and the issue of customer retention (Capestro et al. 2024) hinges on compliance with penalties for a data breach. Drawing upon network theory, we develop a framework relating to how senior managers can put in place governance mechanisms (e.g. type of digital platform), procedures (e.g. guidelines) and processes (e.g. reporting systems) to reduce the risks associated with data/information breaches. In addition, in relation to developing network capacity and forming resource ties for additional resources, Peng and Turel (2020) indicate the potential opportunity to be linked with detrimental resources too. This highlights the importance of planning and managing the process of adoption of digital technology, and the execution of information sharing as an ongoing process (Ebrahim and Rangan 2014).

For the evaluation of performance for improvement, a logic model allows evaluators and stakeholders to be involved in the early stage of a project and evaluate if the objectives set are linked with their underlying foundation and principles (Helitzer et al. 2010). Helitzer et al. (2010) point out that a logic model is also grounded in behaviour change theory – in the sense that developing a logic model allows stakeholders and evaluators to share their understanding of and vision of the programme. This is an important aspect in relation to attitudinal change toward dealing with risk and communicating risk. According to Venkatesh and Davis (2000) and Mola et al. (2023), the intention to use new technological tools is influenced by the perceived usefulness of the tool in relation to the task to be undertaken as well as the social influence (i.e. social norm (SN)) exerted. On the other hand, Issaoui, Örtensjö, and Islam (2023) point out that the issue of a sense of control and accessing necessary resources affects the intention to use new tools. This relates to the issue of providing relevant training (referred to as 'MTE'). Through applying the logic model approach, an evaluator can appraise how the guidelines and reporting system influence behavioural change and the programme's effectiveness through the linkage between programme elements and their outcomes (Helitzer et al. 2010); as well as devising effective action plans and systems to effectively deal with perceived risk and actual risk (Jordan 2010). In other words, the use of a logic model helps managers understand how and why intervention is needed and monitored through an SDP.

SMCT enables organisations to become more efficient as it helps information flow, improves staff decision-making and develop new knowledge-based systems (Gupta et al. 2023). Furthermore, digitalisation is known to reflect sustainability through the continuity of business operations (Ghobakhloo et al. 2024). This suggests that managers need to take cognisance of the fact that a collective behavioural response is representative of the logic model approach and is dependent upon a consensus of opinion regarding critical issues (Julian 1997). This implies that for the information security policy to be effective, security needs to be viewed as essential and staff at all levels need to show their commitment by upgrading their information security skills and knowledge base through time.

Riahi and Islam (2024) argue that in order to have a robust information security strategy in place, it is vital that technological solutions are combined with social mechanisms, which take into account social factors. Therefore, understanding what constitutes the human aspects of information security and how intervention involving security awareness development and training programmes help employees to be compliant is crucial. Knowledge is accumulated through increasing security awareness and overcoming security issues (Riahi and Islam 2024). This implies the importance of writing down the information security (IS) policy that provides formal procedures, as well as serving as a reference for best practice.

As regards information security, Mola et al. (2023) point out that employees are not always prepared to follow strict security policy. Hence, their actions place both themselves and the organisation at risk. This raises questions about the way in which information is communicated within and between organisations, and the role that governance plays (Fenwick, McCahery, and Vermeulen 2019). Bulgurcu, Cavusoglu, and Benbasat (2010) view that if staff comply with information security policy, their attitude and behaviour can be influenced. Cram and Wiener (2018) argue that in relation to the influence associated with control, employee legitimacy perception is the key aspect. This raises questions relating to responsive behaviour. In addition, Moqaddamerad and Ali (2024) suggest addressing employees' mental model (prior beliefs that are formed based on what they know) and addressing knowledge gaps in relation to learning is important. Especially, how the barriers (e.g. lack of knowledge and lack of awareness regarding regulation) affect an employee's compliance behaviour relating to security policy. Beas and Salanova (2006) indicate that attitude and self-confidence are influential. This raises the issue of how barriers can be reduced and focuses

attention on research into how business-to-business managers utilise SMCT to enhance business capability and ensure that employees are compliant. Hence, the main research question identified is: How can organisational intervention help business-to-business managers to use SMCT to reduce barriers and increase business capability through a secure digital environment? To address this, we answer two questions:

Q1: What aspects do senior managers need to consider to ensure that staff harness SMCT for business purposes?

Q2: What do senior managers need to build into SMCT usage to promote compliant behaviour for business?

Our study aims to make a theoretical contribution to network theory in the context of how the deployment of an SDP, positively influences business capability through the use of SMCT. In doing so, through the logic model approach, we explain why senior managers need to enhance an organisation's intervention (i.e. SDP) to increase business capability. This study tested hypotheses using SEM, AMOS and data from 207 online responses from business-to-business managers. The result reveals that SDP supports positively enhancing business capability through the use of SMCT. The SDP is influenced by DGM and SN. It is important to note that the DGM plays a pivotal role in ensuring compliance (DC) and, at the same time influences the development of an SDP. Interestingly, the relationship between training (MTE) and the intention to use an SDP is positive but not significant. This may relate to the fact that the main concern of respondents in the use of SMCT for business purposes relates to how information sharing activity is supported by governance and compliance. As an SDP already takes these issues into consideration through a designed-in approach, the respondents felt that MTE was no longer needed. The findings provide valuable insights for managers and platform developers associated with business-to-business operations. By understanding this, managers and platform developers can evaluate the effectiveness of how inputs are utilised and how outputs are evaluated to achieve desired outcomes.

2. Literature review and hypotheses development

2.1. Network theory and social media communications technology (SMCT)

Previous research relating to a digital platform being a strategy has focused mainly on manufacturing and interoperability (processes and structures in a network), and limited attention is given to the business-customer interface (Setia, Venkatesh, and Joglekar 2013). To address this, we reflect on the work of Borgatti and Halgin (2011:, 1170) regarding network theory, especially the points: 'establishing the boundaries of the groups' and the type of 'ties' ('state-type ties'), as business-to-business managers need to think in terms of how mechanisms and processes within a network structure interact to increase the use of a digital platform.

According to Borgatti and Halgin (2011:, 1168), 'network theory refers to the mechanisms and processes that interact with network structures to yield certain outcomes for individuals and groups'. Borgatti and Halgin (2011) focus their attention on established social network theories: 'Granovetter's strength of weak ties theory' and 'Burt's structural holes theory'. Reference is made to two different models (i.e. ties as pipes that affect the flow of the network and ties as bonds that affect the coordination of the network). One of the key aspects of network theory is the ability of the individual to propagate connectivity and to create opportunities to facilitate trade between the parties – either by identifying new opportunities or acquiring new resources/skill sets that add value. By reflecting on the work of Borgatti and Halgin (2011), two different issues in relation to successful network performance emerge: (i) structures and mechanisms that facilitate processes, which are external and affect an individual actor's performance/intention – this can be interpreted as governance and compliance policy in this research; and (ii) skill, knowledge and emotion, which can be viewed as internal, and which affect an individual actor's judgement and performance/intention, which can be interpreted as training and the subjective norm.

Drawing on this view of network theory, for organisational intervention relating to digital platform usage to improve business operations, attention needs to be given to how to develop network capacity and how to form 'resource ties' to access additional resources (e.g. information, material, advice/knowledge that is specific to accomplish a particular task) (Quinn and Baker 2021). In relation to expanding resource capability through social networks, developing a secure digital environment vis-à-vis structures, mechanisms, and processes will enable an organisation to consolidate its networks and increase its resource capability. However, it should be noted that although SMCT is efficient in terms of information sharing (Daowd et al. 2020), researchers (e.g. Kim and Dennis 2019; Van der Walt, Eloff, and Grobler 2018) suggest that there is scepticism among some managers regarding the use of SMCT for information sharing. Also, Peng and Turel (2020) point out that network ties can tap into detrimental

resources as well as beneficial resources. In addition, Lewis (2024) suggests that digital networks have different characteristics from traditional social networks as the interactions occur online and need more thought in terms of what constitutes a 'tie'. This suggests that business-to-business managers need to take cognisance of the fact that 'boundaries' in network theory need to be overcome in order that an SDP can be implemented whereby the resource 'ties' do not have risk associated with them. Because boundaries can prevent staff sharing information, attention should be given to the way in which governance and compliance are reflected in terms of an SDP (Bonina et al. 2021). Bonina et al. (2021) suggest, software tools and governance and regulations help establish a relationship that maintains distance between the ecosystem members and the owner of the platform. Also, the subjective norm (interpreted as peer pressure on an individual to act or think in a certain way) influences the attitude and behaviour of staff and results in the development of a secure engagement strategy through information sharing.

2.2. Logic model and secure digital platform

To improve information sharing through the use of digital technology while retaining customer retention and trust (Capestro et al. 2024), it is important to plan and manage the process of adoption and execution of digital technology, which is complex and affected by various factors (e.g. structures, mechanisms, skill and knowledge) as well as how to deal with risks in the short to long term (Surucu-Balci, Iris, and Balci 2024). In relation to planning and managing the development of an SDP for safe information sharing and performance improvement, the use of a logic model proves advantageous. Compared to the technology acceptance models, which are used to predict users' perception of technology/a systems' success/effectiveness in measuring information system usage (Salovaara and Tamminen 2009), the logic model, which is grounded in behaviour change theory, allows evaluators to be involved at the early stage of programme design and engage with stakeholders and assess if the programme has achieved its objectives (Helitzer et al. 2010). Involving stakeholders early in the design of a programme is vital because stakeholders possess different views of what needs to be done to achieve certain outcomes (Longmeier and Murphy 2021) and may have a different appreciation of the resources needed (inputs) to achieve the outcomes. It is essential, therefore, that as regards programme performance, short-term and mid-term outcomes are mapped against long-term impact (Longmeier and Murphy 2021). Reflecting back to criticism of technology acceptance models, Taherdoost (2018) points out that because researchers do not distinguish between the affective component of attitudes in relation to cognitive component/beliefs, there are different orientations involving internal antecedents (eg., attitudes and values) and external issues (eg., norms and institutional constraints). This suggests that in the case of technology acceptance models, the evaluative process may not measure performance in a uniform way or in a way that allows outcomes to be assessed that meet stakeholder expectations.

Institutional theory is also considered less useful because it does not focus enough on the differences across organisations (Meyer and Höllerer 2014). Subjective interpretation plays a key part but there has been an overemphasis on the outcomes of institutional processes as opposed to 'the sources of dynamics of those processes' (Suddaby 2015, 94). According to Hinings, Gegenhuber, and Greenwood (2018, 53), 'Institutional theory emphasises that organisations are not purely rational systems of producing goods and services, adapting to an environment of suppliers, consumers, and competitors. Importantly, they are themselves social and cultural systems that are embedded within an 'institutional' context of social expectations and prescriptions about what constitutes appropriate ('legitimate') behaviour. For most organisations, the crucial context is that of the organisational field, and critical actors within the field include regulators, professional associations and the media … ' By placing emphasis on sociocultural aspects in relation to organising innovation, it can be suggested that certain actions underpinned by engagement strategies are eradicated or diluted, and this affects the commitment of stakeholders. For example, digital innovations are increasingly challenging our understanding of institutional arrangements in relation to legitimacy and regulation; consequently, existing values, and indeed norms and practices (Hinings, Gegenhuber, and Greenwood 2018) are being reinterpreted as different types of business models that evolve and require more enhanced forms of regulation.

Ebrahim and Rangan (2014) suggest that senior managers need to determine the organisation's goals and operating model and measure short-term and long-term impacts vis-à-vis the relevance of the causal logic model (input → activities → outcomes → impact). Logic models are used by knowledgeable and skilled staff to structure the evaluation of the anticipated outcomes of a programme (Renger and Titcomb 2002) and are useful for evaluating multiple objectives. The inputs represent the resources used in a programme to achieve the goals set and the outputs are derived from

the activities and services (Gagiu and Rodriguez-Campos 2007), and an evaluation considers the problem(s) to be solved and the scope of the programme (Gagiu and Rodriguez-Campos 2007). According to McLaughlin and Jordan (1999), measurement strategies monitor the causal linkage or relationships and influences of the intervening external factors.

The logic model approach can be viewed as a beneficial measurement tool because it allows managers to assign resources, evaluate outcomes and devise correct action when necessary. Bearing in mind that security systems are broad-based and deal with detection through monitoring (Morin et al. 2009, 285), managers need to be proactive in terms of identifying potential vulnerabilities that can be exploited by an attacker. The logic model approach can be used to link outcomes with system effects and establish how perceived risk and actual risk are to be dealt with (Jordan 2010). This is achieved through the designed in capabilities that depict the relationships between the programme components and the changes in behaviour that are linked with the gaps in the components of the programme (Helitzer et al. 2010). By mapping out the components of the programme, managers can identify real and potential blockages, but these need to be communicated within a specified time period so that the agreed change will allow the key performance indicators to be evaluated (Jordan 2010). Reflecting on the fact that measurement occurs at various time intervals, it is clear that there is a need to study the immediate impact (mediating factors) so that the implementation of the programme components (activities/outputs) is linked with the behavioural outcomes (Helitzer et al. 2010) and the desired results are achieved. Visualisation can be used to represent the logic model in pictorial form. Visualisation not only helps the designers of a logic model to outline and explain how it can be evaluated (Jones et al. 2020) but it also allows partner organisations to better understand how their capabilities can be mapped into the model.

We acknowledge that organisational intervention (eg., training for skill enhancement, knowledge development and/or emotional support (viewed as an internal consideration to an individual)), and an SDP (e.g. structures and mechanisms that facilitate processes (viewed as an external consideration to an individual), represent an important aspect of network theory. Therefore, we argue that organisational intervention that is planned and managed through the utilisation of a logic model can enhance information security through the process of safeguarding customer data. Thus, an SDP will provide business-to-business managers with an opportunity to implement an effective engagement strategy as it will provide them with confidence and thus erode barriers.

An SDP should also take into account the issue of usability in relation to effectiveness and efficacy and practicality (e.g. reliability) (Dey, Newman, and Prendergast 2011) in relation to the safe handling of information as well as facilitating task relevance (Venkatesh and Davis 2000). Bulgurcu, Cavusoglu, and Benbasat (2010) and Surucu-Balci, Iris, and Balci (2024) argue that information sharing among and between business partners through digital platforms is affected by enabling factors (e.g. security, transparency, environment, traceability and trackability, and efficient information sharing) and barriers (e.g. lack of knowledge, awareness of privacy and the issue of mistrust, and limited knowledge of regulation and inadequate support). Also, Moqaddamerad and Ali (2024) point out that cognitive inertia is a challenge to new ways of managing and can affect the way people think in terms of developing their knowledge. This is because new management thinking is inhibited, and as a result, an individual's reasoning capability is distorted, and they are not able to sense novel opportunities. Moqaddamerad and Ali (2024) also explain that although sensemaking is important and influences learning, it does not have an influence on business model innovation, whereas learning influence does affect innovation. Equally, Mola et al. (2023) suggest that inertia and resilience are important factors that influence behaviour and behavioural change. Thus, for this research, we argue that an SDP contains antecedents such as designed-in governance and designed-in compliance, subjective norm, and training, which positively influence the use of SMCT to enhance an organisation's business capability.

2.2.1. A secure digital platform (SDP)

Social media communications technology (e.g. social networks, blogs, and computer meditated communication) is viewed as a means by which relationships with customers can be cultivated and an organisation's competitive advantage leveraged (Agnihotri et al. 2016). Gregory et al. (2018) suggest that SMCT reinforces strategic capability through staff utilising analytics and customised interaction. This view is reinforced by Jha and Verma (2024) who argue that organisations develop different strategies for different platforms. The level and type of engagement with their audience differs depending upon the requirements of the audience. This brings to the fore the skills and capabilities of managers (Walters 2008).

As regards digital platforms and relationship building, Zoppelletto, Orlandi, and Rossignoli (2020) indicate that digital platforms can facilitate interactions

among/between users as well as identify new ways of doing business through connecting with various stakeholders. In relation to different types of platforms (Gawer, 2014) and how a digital platform operates, Rangaswamy et al. (2020, 73) indicate that platform users are independent parties, which allows them to retain residual ownership rights. Li et al. (2019, 1448) state that a platform is known to have 'a modular architecture and provide an interface that facilitates multilateral transactions and exchanges among users and providers of complementary products and services'.

Rangaswamy et al. (2020) indicate that different types of constraint can be deployed to influence the behaviour of both users and partners in an ecosystem. An ecosystem can be defined as nodes of connectivity within an industry and the accompanying structures that facilitate interaction. An ecosystem is representative of cooperative relationships that are reinforced by a governance mechanism (Li et al. 2019), which facilitates connectivity within an industry. Therefore, a shared set of standards and processes aids information flow and its utilisation (Nambisan, Zahra, and Luo 2019).

Accessing usable data for analysis, Murphy and Sashi (2018) address the issue of how managers can develop a positive reputation that allows them to establish trustworthy relationships. Trustworthiness bestows confidence in a person to perform/deliver in the way expected, therefore, customers are prepared to share information (Gupta et al. 2023). Hence, we are of the view that a *secure digital platform allows an organisation to customise its connectivity and interactions and share information safely in real time*.

Jabee and Alam (2016) indicate that users need to be more aware of privacy risks when using social media network sites. Even though users of social media sites can set defaults, fundamental problems can stem from the structure and design of the digital platforms themselves. Van der Walt, Eloff, and Grobler (2018) identify a key issue in the form of inadequacy of design, which allows fraudsters to open an account by impersonating somebody or stealing someone's identity. In addition, there are also machine generated risks such as fake faces and/or voices to impersonate people. Bearing this in mind, we suggest the following hypothesis:

> **Hypothesis 1**: A secure digital platform positively enhances business capability through the use of SMCT.

2.2.2. A designed-in governance mechanism (DGM) and designed-in compliance (DC)

Previous research in relation to information technology (IT) governance has focused on either a functional profile and its transformation or the evolutional changes of IT governance, which relate to organisational structures and processes relating to decision making and accountability (Browne and Grant 2005). A governance mechanism defines the tasks, roles, and responsibilities that control interaction, which helps the owner of the platform to implement 'agreement and rules' that help the complementors – 'who complete the platform's value proposition' – to innovate in an acceptable way (Mei, Zheng, and Zhu 2022, 499).

The IT governance policy that senior management put in place needs to reflect how staff use SMCT, how they align the firm's strategy with it, how they prioritise issues, identify necessary resources, and assess responsibilities and accountability (Gregory et al. 2018). Furthermore, Surucu-Balci, Iris, and Balci (2024) point out that optimum governance enables an organisation to achieve economic efficiency as digital information sharing minimises the cost of a transaction. Hence, attention needs to be given to how employees view control and its legitimacy because they may have a positive or negative view of control (Cram and Wiener 2018). Bearing these points in mind, we define a designed-in governance mechanism (DGM) as: *a secure digital communications platform that has designed-in structures, processes and relational mechanisms, is adaptive and implements up-to-data regulatory changes*. A DGM is, therefore, incorporated within an organisation's ecosystem.

In essence, a governance mechanism is associated with the security of information that is viewed from a managerial perspective (internal to the organisation) and a contractual relationship perspective (in relation to the supply chain and links with external organisations) (Gupta et al. 2023). Governance influences the way staff share information and how information is controlled (Li, Yu, and Kunc 2024). A platform is designed for increasing collaboration and aiding innovation; however, it has to be recognised that the needs of users differ.

The adoption of SMCT in a business-to-business context is a conscious decision (Hartwick and Barki 1994; Venkatesh and Davis 2000) and consequently, senior management need to put in place a digital communications strategy that results in the successful use of SMCT through time (Tiwana and Kim 2015). By implementing the latest governance mechanism (Hatch and Schultz 2010; Issaoui, Örtensjö, and Islam 2023), cognisance can be taken of how the regulations change through time and what requirements need to be built into the governance mechanism to appease external stakeholders.

Compliance requires managers to adhere to the General Data Protection Regulation (GDPR), which covers

data collection and the consent and protection of data, with fines imposed if organisations do not comply (Bhalavat et al. 2024). For an organisation to be compliant and ensure privacy, then changes in staff attitudes and behaviour toward compliance are important as they will prevent data breaches. In relation to staff's behavioural change, Trim and Lee (2019) argue that senior managers can influence and manage staff's behavioural change by establishing a compliance policy that takes into account the variations in the way in which staff relate to the rules in place, the given tasks to be undertaken, and the organisation's overall strategy, which require different advice in relation to how staff are required to respond proactively to identified risks. Building on the work of Trim and Lee (2019) designed-in compliance (DC) can be defined broadly as: *in accordance with an up-to-date governance mechanism, a firm's legal responsibility and information sharing policy ensure that staff comply with industry standards and regulations*. It is important to remember, however, that IT governance needs to be organisation specific. Hanafizadeh, Hossravi, and Tabatabaeian (2020) point out that senior management need to set the conditions relating to who has access to a digital platform. Also, they need to ensure that the security policies in place are adhered to. If senior management integrates an organisational specific governance policy that reflects industry compliance requirements into the organisation's digital platform, it will increase the perceived suitability of the platform and reduce the level of risk. Bearing these points in mind, we put forward the following hypotheses:

Hypothesis 2: A designed-in governance mechanism positively influences the intention to use a secure digital platform.

Hypothesis 3: A designed-in governance mechanism positively influences compliance behaviour through designed-in compliance policy in relation to information security within a firm.

2.3. The influence of the subjective norm (SN)

Reflecting on the use of SMCT, Dey, Newman, and Prendergast (2011) link usability to emotional, social and practical issues and concerns, and it is because of this that user action needs to be linked with security and the safe handling of information generally. Bonina et al. (2021) explain that cost and risk can be transferred from the employer to the worker through access and availability of information and resources. This is an interesting observation. In relation to why people want to access information and the effect it has on emotions, Jia, Liu, and Lowry (2024) point out that the need to satisfy social needs and gain social approval is considered important. Similarly, Kusumastuti et al. (2022) carried out a study relating to why people in a smart city use smart city platforms and point out that a sense of belonging and seeking reputation enhancement affect the intention to seek information on smart city platforms. To identify an effective organisational intervention, Venkatesh and Davis (2000) extended their earlier work on perception, which incorporates usefulness and intention, by relating to the nexus of social influence and cognitive instrumental processes (eg., job relevance and output quality). In their research, they place emphasis on predicting how external social factors influence behaviour (e.g. social norms). This work was supported further by Pentina, Koh, and Le (2012), who focused on the impact of social influences and the need for intervention (eg., to help individuals cope with a situation). Similarly, Mola et al. (2023) explain that individual staff behaviour is influenced by various aspects such as norms that are external to the organisation, an organisation's values and habits, as well as local politics in interpersonal relationships. Staff behaviour can also be influenced by cognition in terms of compliance and legitimacy (Mola et al. 2023). Because the attitude towards a particular behaviour is a learned tendency and requires an individual to evaluate matters in a particular way, it can be argued that if a change occurs in the evaluation process, behavioural change results (Safa et al. 2015). Hence, we look at the influence of the subjective norm (SN) in relation to how business-to-business managers safeguard the interaction process involving the sharing of information through using SMCT.

Venkatesh and Davis (2000) articulated that the SN includes direct determinant behavioural intention. This line of argument stems from research undertaken in studying the process of the internalisation of information and how willing an individual is to accept their co-worker's suggestion(s) about how a particular system should be used vis-à-vis an expected positive outcome. The influence associated with the SN can be considered effective, especially when the referent can either reward or punish (non)behaviour (Trim and Lee 2019). Bearing this in mind and noting that we were undertaking research into SMCT and an SDP, we defined the subjective norm (SN) as *social pressure on an individual in terms of their behaviour and how people who are important to them perceive them vis-à-vis whether they should or should not use the required system*. This view of the SN implies that the power of expertise and credibility impacts how an individual evaluates either positively or negatively an event/

situation (Leonard, Cronan, and Kreie 2004) and how it influences conscious change in their beliefs and behaviour. It should be noted that the knowledge gained through specialised training, education or observation, and direct or indirect experience gained, not only increases an individual's knowledge and capability but can be considered influential in terms of helping an individual to decide upon a course of action (Tannenbaum et al. 2015). Bearing this in mind, we identified the following hypothesis:

Hypothesis 4: The subjective norm positively influences the intention to use a secure digital platform.

2.4. The influence of training (MTE)

Kraft et al. (2005) argue that individuals will only be motivated to perform the duties that they are confident of performing, and this is a key consideration as regards SMCT. Issaoui, Örtensjö, and Islam (2023) point out that staff are concerned about issues such as the lack of awareness and trust, loss of control, loss of confidentiality, unauthorised access, legal uncertainties and regulatory challenges when they use cloud-based services. Staff may not have a realistic appreciation of their own ability to undertake a task(s) because they lack confidence and/or experience. Hence, senior managers should consider that staff 'lack complete volitional control over the behavior of interest' (Ajzen 2002, 666). Referring to control, we adhere to the view that control is specifically about an individual's perception of several factors including the availability of knowledge, resources, and opportunities, which are needed for them to undertake specific duties in a certain way. These factors affect intention and relate to how an individual values the opportunity of receiving training and increasing their effectiveness and efficiency.

In addition, the concept of self-regulation takes into account self-control. Self-evaluation and self-control manifest in actions that an individual is prepared to put into a task to achieve a goal/outcome through attempting to increase what they perceive as necessary resources and controls (Job, Dweck, and Walton 2010). Of importance is how individuals attempt to increase their knowledge and skill in relation to the use of SMCT when undertaking their allocated tasks within a limited period. In other words, individuals regulate their limited resources to achieve the best possible results they can; however, over demand of an individual's resource capability (knowledge, skill and time) leaves an individual fatigued and lacking in confidence.

For the purpose of this research, we acknowledge that *keeping training up-to-date and relevant, supports users in their work activities as it enriches the quality of outputs and drives effectiveness. The benefits of this approach go beyond business efficiency as systems users experience positive self-evaluation and increased self-confidence.* Organisational support needs to be viewed in terms of the implementation of new systems, which have different levels of complexity associated with technology and business process knowledge. As regards the sharing of knowledge and exchanging experience via SMCT tools such as Wikis, Blogs, and Webinars; it is acknowledged that opportunities will occur for joint learning and increased levels of social networking (Walters 2008) and the effective use of digital platforms. Hence, we put forward the following hypothesis:

Hypothesis 5: Specific IT training positively influences the intention to use a secure digital platform.

The five hypotheses outlined above have been integrated into a research framework. Please see Figure 1.

3. Methods

3.1. Research strategy

The research focused on how a secure digital platform (SDP), as an organisation's intervention, instils confidence in business-to-business managers to utilise SMCT and engage in information sharing. Hence, the main research question identified was: how can organisational intervention help business-to-business managers use SMCT to reduce barriers and increase business capability through a secure digital environment? To test the research framework that was drawn from network theory and related to the issue of governance through procedures and processes, we placed procedures and processes in the context of a digital platform and linked them to the implementation of governance and compliance. We also tested issues relating to planning and managing human behavioural change through SN and MTE and explained matters through the utilisation of the logic model approach. Owing to the fact that the subject matter contained a number of distinct but related subtopics in relation to business and information security and the target population was widely dispersed throughout the UK, we decided to use a quantitative research approach and collect data through an online questionnaire.

3.2. Questionnaire development and data collection

Prior to the collection of data, two separate pilot tests were undertaken. First, we asked four UK based experts in the business-to-business information security field if

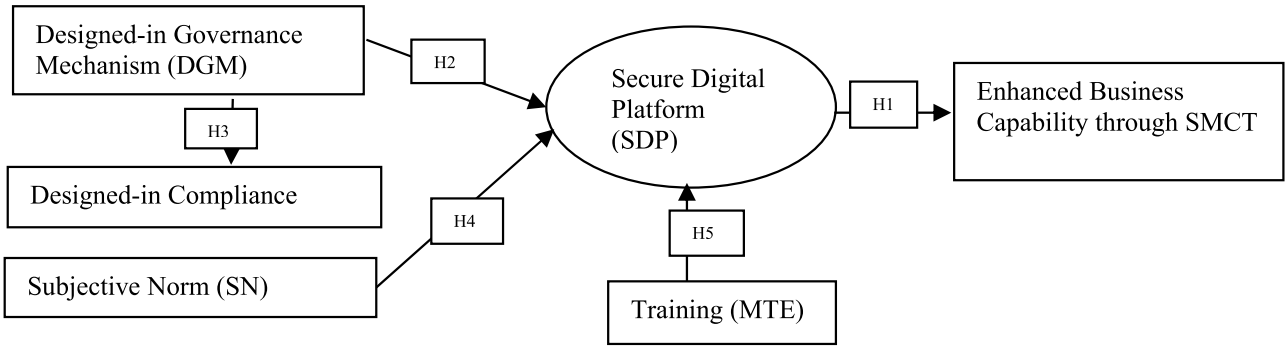

Figure 1. Research framework.

the questions, the structure and the definitions in the questionnaire were appropriate. Based on the responses received, we made minor amendments to the questionnaire (eg., the connection of the sub-topics and questions in each sub-topic (eg., from SMCT → SDP → SN → DGM → DC → MTE to *SMCT → SDP → MTE → DMG → DC → SN*)). Furthermore, items 3, 4 and 5 in SN were reordered in the form 4, 5, and 3, respectively. The second pilot test involved 12 UK based business-to-business information security experts and checked the way the questions were worded and if they were placed in the correct sequence (overall structure and layout of the questionnaire) (Schwarz et al. 2017) as this would reduce the likelihood of the risk of common method bias.

The measures used were partially developed from the existing literature such as Agnihotri et al. (2016); and Murphy and Sashi (2018). The items were adapted from several existing studies such as Venkatesh and Bala (2008); Bulgurcu, Cavusoglu, and Benbasat (2010); and Safa et al. (2015). The scales adopted were mostly drawn from a number of relevant but different academic sources as well as feedback received through the pilot tests, and this helped to avoid common method bias (Jakobsen and Jensen 2015). Furthermore, attention was given to the scale anchors so that the respondent focused on scale consistency versus the individual items (Schwarz et al. 2017). Following the advice given, we deployed a 7-point Likert scale representing 1 = very strongly disagree to 7 = very strongly agree. The questionnaire, constructs, definitions and measurement items are presented in Appendix 1 ('Appendix 1: Questionnaire, constructs, definitions and measurement items and factor loadings').

Prior to the researchers gathering primary data via the survey, approval had been obtained from the appropriate university ethics research officer in-charge of maintaining ethical research standards. Google Drive was used to create the questionnaire and the business-to-business managers identified to participate in the data collection exercise received an e-mail seeking their participation in the study. Once they had given their permission, they were sent an email (individually) that explained the purpose of the research, the ethical code of conduct and a URL link to the questionnaire. LinkedIn was used and 1,011 business-to-business managers (who were based in UK companies) were approached in three different phases to complete the questionnaire. The respondents who completed the questionnaire were employed in a business-to-business function and were based in different industries, including banking, communications technology, insurance and retailing, throughout the UK.

3.3. Data analysis

The research was social science based and incorporated psychological aspects that addressed how barriers could be reduced in the context of SMCT usage in a business-to-business context. We considered that structural equation modelling (SEM) was suitable as it includes the residual error that is associated with the independent variable (Tabachnick and Fidell 2014). Also, SEM allows the researcher to investigate relationships between the latent variables and observed variables; as well as to derive answers that involve the multiple regression analysis of factors. SEM in SmartPLS focuses on predicting variance in observed variables (Hair et al. 2021). However, as we were looking at the overall model fit in the hypothesised model relationship (Figure 1: Research framework) through reproducing the observed covariance matrix (Safa et al. 2015), AMOS (version 29) was considered appropriate to analyse the relationships among the constructs (independent, dependent variables). Also, AMOS is a graphic approach to the analysis of confirmatory factor analysis based on mean and covariance structures, which enables researchers to assess both relationships among variables and their mean levels within the research framework (Byrne 2010). The researchers were able to test the proposed

model as well as specific relationships among the variables (Hair et al. 2010). To calculate sample size, G-power was used, which suggested a sample size of 123 or 146 depending on whether α (1-β) is .09 or .095 respectively. For this study, the sample size was 207, and 6 constructs were identified with a total of 24 items. The sample size can be considered adequate.

3.3.1. Demographic characteristics of the respondents

The response rate was considered satisfactory bearing in mind we targeted business-to-business managers with a specific knowledge of and an understanding of information security in relation to business operations. A total of 1,011 business-to-business managers were contacted over three different periods and a response rate of 28.9% (282 business-to-business managers) was achieved. Out of the 282 responses, 75 questionnaires were deemed to be unusable as they were incomplete, and this resulted in 207 usable questionnaires only. Table 1 contains the respondents' demographic characteristics, the size of the firm and the sector in which the respondent worked.

Table 1. Respondents' demographic characteristics, the industry and the size of a firm.

Gender		%
	Male	68.1
	Female	31.9
Age	Age	%
	22-25	4
	26-30	4
	31-35	8
	36-40	9
	41-45	7
	46-50	21
	51-55	14
	56-60	9
	61-65	17
	66 +	3
	Nonresponse	3
Mean age	48.85 years old	
Education	Qualification	%
	College (A level/further education)	10.6
	Undergraduate degree	13.5
	Graduate degree	60.4
	Other (eg., professional qualification)	14
	Did not say	1.4
Industry	Sector	%
	Consultant	13
	Public sector (e.g., resilience & defence)	9
	Finance	13
	IT & Communication	31
	Marketing/Advertising	10
	Services (education, retail, travel)	24
Size of the firm	Number of staff	%
	less than 500	37.7
	between 500 to 10,000	37.7
	over 10,000	24.6

Most of the respondents held senior positions such as CEO, director of digital marketing; head of marketing, and head of innovation. Some worked in business development and channel marketing. It was noted that 50.7% of the respondents stated that their organisation was highly information intensive, and 42.5% of the respondents said that their organisation was somewhat information intensive. In addition, 95.2% of the respondents indicated that their organisation had an established information security policy in being. The mean for the hours worked per day using a computer was 9 (8.9).

3.4. Results

3.4.1. Reliability, validity, and model fitness

For factor analysis, Tabachnick and Fidell (2014) suggest that the coefficients of the interrelationships among the items should be greater than .3. Jöreskog, Olsson, and Wallentin suggest that the loading factor of an item in the different main components should be above .5. If Bartlett's test is significant ($p < .05$), and the minimum value of the KMO index is .6 (or above), it is considered good for factor analysis (Bartlett 1954; Kaiser 1974). The result of the KMO and Bartlett's test for this research is .877 ($p = 000$), which suggests that there is a very good indication of intercorrelations among the variables. The result of the principal component analysis (PCA), based on the Eigenvalue being greater than 1 and direct oblivion for factor extraction revealed the presence of five components explaining 34.7%, 45.2%, 54.3%, 61.8% and 66.5% of the variance. Furthermore, the result of the Cronbach Alpha coefficients was above .7 (DeVellis 2012), which indicates that internal consistency is good (DC - .911; DGM -. 881, Training (MTE) - .855, SMCT - .807, SN - .847, and SDP - .756). (See 'Appendix 1: Questionnaire, constructs, definitions and measurement items and factor loadings'). Hence, we decided to progress to measurement analysis using AMOS.

3.4.2. Measurement model

The measurement analysis in SEM is based on Confirmatory Factor Analysis (CFA) and establishes an acceptable level of goodness-of-fit and construct validity of the research framework (Hair et al. 2010). The variables of interest are latent variables (unobserved variables), such as Social media communications technology (SMCT); Secure digital platform (SDP); Subjective norm (SN); Training support (Training); Designed-in governance mechanism (DGM); and Designed-in compliance (DC).

To examine the model fit, we used different standards including the Chi-square test (CMIN (X^2) – minimum

discrepancy), Chi-square with degree of freedom (X^2/df), Tucker and Lewis Index (TLI), Comparative Fit Index (CFI), and Root Mean Square Error Approximation (RMSEA). We also took into account other standards to evaluate the model fit CMIN/DF (X^2/df) < 3 (MacCallum, Brown, and Sugwara 1996). RMR (Root Mean square Residual) represents the average value across all standardised residuals, and if RMR is small or equal ≤ 0.5 it is a good fit. The RMSEA considers the error of approximation in the population. If the value of RMSEA is less than .05, it shows a good fit, and if the value is high, like .08 there is a reasonable fit (Brown and Cudeck 1993). As regards incremental fit indices or comparative fit indices such as TLI (Tucker-Lewis Index) and CFI (Comparative Fit Index), estimate the relativeness between the estimated model fit to the alternative baseline model that assumes all observed variables are uncorrelated (Byrne 2010). TLI takes into account model complexity and compares the normed value of X^2 for the null and specified model. If the TLI value is above .90 (TLI > .90), it is considered a good fit. Also, if CFI is above .90 (CFI ≥ .90) this is associated with a good fit. Parsimony Normed Fit Index (PNFI) adjusts the Normed Fit Index (NFI) and Parsimony Goodness Fit Index (PGFI) (Byrne 2010). According to Bagozzi and Yi (1988); Kline 2005; Hoang, Igel, and Laosirihongthong (2006), if X^2/df ≤ 3, RMSEA ≤ 0.08, CFI ≥ 0.90 and TLI > 0.90, PNFI > 0.50 and PGFI > 0.50, the model and data have a good fit. The measurement result for this study shows the indices meet the recommended values: CMIN/DF (X^2/df) = 1.374; RMR = .043; CFI = .971; TLI = .962; PNFI = .690; PGFI = .633; RMSEA = .043. In other words, the six-factor model (Social Media Communications Technology (SMCT), Secure Digital Platform (SDP), Designed-in Governance Mechanism (DGM), Designed-in Compliance (DC), Subjective Norm (SN), and Training (MTE)) yielded a good fit, and it suggests the measurement of the model is satisfactory.

The threshold for Composite Reliability (CR) is bigger than .7 (CR > 0.7), and the Average Variance Extracted (AVE) is bigger than .5 (AVE > 0.5), which assesses convergent validity; and Maximum Shared Variance (MSV), which assesses discriminant validity and is satisfactory if the value of MSV is smaller than AVE (MSV < AVE), and the Square Root of AVE is greater than the inter-construct correlations (Hair et al. 2010). The test shows that all the items meet the recommended AVE value (AVE > 0.5); CR value of .07. Also, the discriminant test result shows that all of the constructs have been accepted as the MSV values are below the value of AVE. In addition, the threshold for discriminant validity should ideally be less than 0.85, and maximally less than 0.9 (Henseler, Ringle, and Sarstedt 2015). Table 2 shows the results of the convergent and discriminant validity analysis.

We also tested the common method bias by using the common latent factor (CLF), and the result showed that chi-square = 147.1, df = 24, the p-value = .00, which means there was significant shared variance. Hence, we retained CLF when testing the structural model and used common method bias corrected measures (Serrano et al. 2018).

3.4.3. Structural model test

To test the hypotheses, structural equation modelling was applied to test the relationship among the latent and observed variables in the proposed research framework. Also, to test the model's parameters, the maximum likelihood method was applied.

To test the theoretical framework, different fit indices were applied. The result shows CMIN/DF (X^2/df) = 1.391; CFI = .968; TLI = .960; PNFI = .709; PGFI = .652; RMSEA = .044. Brown and Cudeck (1993); Hoang, Igel, and Laosirihongthong (2006); and Byrne (2010) suggest that for a good fit model if X^2 /df ≤ 3, RMSEA ≤0.08, CFI ≥ 0.90 and TLI > 0.90 PNFI > 0.50 and PGFI > 0.50. Based on the result, it can be said that the proposed theoretical framework is a good fit.

The squared multiple correlation was .40 for enhancing business capability through the use of SMCT. This shows that a 40 per cent variance in enhancing business capability through the use of SMCT is accounted by the secure digital platform (SDP). The secure digital platform (SDP) shows 33.4 per cent variance that is accounted by designed-in governance mechanism (DGM), subjective norm (SN) and training (MTE). Variance in designed-in compliance (DC) was 53 per cent, which is accounted by the designed-in governance mechanism (DGM).

This study assessed the impact of a secure digital platform (SDP) on enhancing business capability through the use of SMCT. The impact of a secure digital platform (SDP) on enhancing business capability through the use of SMCT was positive and significant (β = .631, t = 5.670, p < 0.001), hence supporting hypothesis 1. The impact of designed-in governance on secure digital platforms is positive and significant (β = .359, t = 3.984, p < 0.001), which supports hypothesis 2. Also, the impact of designed-in governance on compliance behaviour relating to information security through designed-in compliance is positive and significant (β = .728, t = 8.848, p < 0.001), which supports hypothesis 3. The impact of the subjective norm on the intention to use a secure digital platform (SDP) is positive and significant (β = .263, t = 3.715, p < 0.001), and supports hypothesis 4. The impact of specific IT training on the

Table 2. Convergent and discriminant validity analysis.

	CR	AVE	MSV	MaxR(H)	DC	SDP	MTE	DGM	SN	SMCT
DC	0.946	0.813	0.497	0.954	**0.902**					
SDP	0.791	0.559	0.360	0.797	0.427	**0.748**				
MTE	0.896	0.689	0.219	1.044	0.394	0.346	**0.830**			
DGM	0.895	0.682	0.497	0.901	0.705	0.449	0.468	**0.826**		
SN	0.925	0.713	0.167	0.950	0.343	0.409	0.279	0.347	**0.845**	
SMCT	0.814	0.523	0.360	0.820	0.369	0.600	0.249	0.397	0.356	**0.723**

intention to use a secure digital platform (SDP) is positive but insignificant ($\beta = .108$, $t = 1.5864$, $p = 0.113$). Hence, hypothesis 5 is rejected. The hypotheses result is presented in Table 3.

4. Discussion and conclusion

This is the first study that empirically explains why and how an SDP as an organisational intervention contributes to enhancing business capability. Previous studies focused on how staff's security awareness is enhanced and affects the complaint behaviour of staff (Bulgurcu, Cavusoglu, and Benbasat 2010); the appropriateness of usability that affects practicality as well as a user's emotion (Dey, Newman, and Prendergast 2011); and task relevance (Venkatesh and Davis 2000). Recently, Surucu-Balci, Iris, and Balci (2024) highlighted factors that affect the deployment of a digital information system which include security, transparency, environment, traceability and trackability, and efficient information sharing as well as issues that affect information sharing such as a lack of knowledge, a lack of awareness of privacy, and issues of trust, regulation, and support from stakeholders, which were derived from a systematic literature review. Through this empirical study, we answered two questions in relation to the application of network theory in conjunction with the logic model approach in the context of SMCT use and information sharing. The two questions posed were: Q1: What aspects do senior managers need to consider to ensure that staff harness SMCT for business purposes? Q2: What do senior managers need to build into SMCT usage to promote compliant behaviour for business? The results of this study show that the deployment of an SDP positively influences the use of SMCT ($\beta = .631$, $p < 001$), which affects enhancing business capability. In other words, in answering the first question, in order to strengthen the development of an SDP, senior managers need to pay attention to governance mechanisms such as the type of digital platform, procedures (e.g. guidelines) and processes (e.g. reporting systems) so that it does reduce barriers such as a lack of knowledge, a lack of awareness regarding regulation, and inadequate support and increases information sharing that strengthens resource ties for additional resources. In relation to question 2 regarding how senior managers can promote staff compliance behaviour, the result shows that DGM strongly positively influences staff compliance behaviour ($\beta = .728$, $p < 001$). Also, DGM positively influences the intention to use the SDP ($\beta = .359$, $p < 001$), alongside SN ($\beta = .263$, $p < 001$). In other words, the DGM plays an important role in the development of an SDP. This suggests that it is important for senior managers to set organisational goals and relate them to the scope of the programme and the expected outcomes (Ebrahim and Rangan 2014; Helitzer et al. 2010).

Table 3. Result of the hypotheses test.

Hypothesis	Outcome	Std β	t-value	p-value	Result
H1	SDP → SMCT	.631	5.670	0.000	Accepted
H2	DGM → SDP	.359	3.984	0.000	Accepted
H3	DGM → DC	.728	8.848	0.000	Accepted
H4	SN → SDP	.263	3.715	0.000	Accepted
H5	MTE → SDP	.108	1.5864	0.113	Rejected

As indicated above, the DGM also positively influences staff's compliance behaviour through DC. Concerns of respondents relate to their responsibilities for information sharing with in-house staff and staff who are external to the company as well as complying with legal regulations. In other words, senior managers also need to monitor the currentness of DMG and comply with current industry standards. Thus, our research highlights the significance of DGM in ensuring compliance (DC) as well as positively influencing the intention to use an SDP. It contributes to deepening our understanding of the deployment of network theory relating to SMCT usage and information sharing, as well as the application of the logic model in managing and devising a strategy to improve the resource capability of an organisation. It should also be noted that although training (MTE) has a positive relationship with the intention to use a secure digital platform (SDP), it is not significant ($\beta = .108$, $p = 0.113$). The implication of this is if DGM is adaptive and implements up-to-date regulatory changes systematically and is placed appropriately in the structures and processes, it will automatically reduce staff's concerns about their lack of

awareness of risk, a sense of loss of control, loss of confidentiality and legal uncertainty, for example (Issaoui, Örtensjö, and Islam 2023).

4.1. Theoretical contributions

The research makes a number of theoretical contributions. First, we extend network theory in the context of an SDP. By applying network theory in a digital platform context, we explained that through the adoption of an SDP, an organisation intervenes to expand its networks and increase resource ties to access additional resources. Previous research highlights the importance of communication flow and structural connectivity (Borgatti and Halgin 2011), which affects accessing additional information (Quinn and Baker 2021), as well as the benefits of SMCT in expanding social networks through information sharing (Daowd et al. 2020). It also highlights scepticism in relation to using SMCT (Kim and Dennis 2019). We took these aspects and expanded them further by integrating designed-in governance and designed-in compliance into a platform (SDP) that facilitates network expansion opportunities and information sharing for additional resources to enhance business capability through the use of SMCT. Hence, this is a unique contribution to network theory development.

In doing so, second, we also explain how the logic model can be applied in managing the SDP. In relation to risk reduction, it is important to recognise that reducing risk is not only achieved through technology alone but also reflects staff behaviour (Bulgurcu, Cavusoglu, and Benbasat 2010; Surucu-Balci, Iris, and Balci 2024). As regards staff behavioural change relating to information handling and reducing risk, existing research highlights the importance of nurturing a security-oriented organisational culture (Surucu-Balci, Iris, and Balci 2024) as well as the need to address issues such as a sense of control, accessing necessary resources and lack of knowledge through training (Issaoui, Örtensjö, and Islam 2023). The findings of this research align with the findings of previous research relating to the importance of nurturing a security culture involving social norms that influence behavioural change. The results show that an SDP is reinforced by SN ($\beta = .263$ $p = 0.000$), which helps nurture and reinforce engagement. Furthermore, the perception of an individual who they think is important to them, as well as the behaviour of other people whom they think are prestigious, affects their behaviour and change and positively influences their intention to use a secure digital platform. However, in relation to training that helps them to improve their lack of knowledge relating to industry regulations for example, it was not supported – although training has a positive relationship with the intention to use an SDP, it was not significant ($\beta = .108$, $p = .113$). This may be due to the fact that an SDP has already designed-in governance that incorporates industry regulations. This is an interesting finding, which suggests that an SDP fulfils the requirements of staff undertaking their task in a controlled environment, which increases their confidence. This implies the importance of integrating the views and needs of stakeholders at the SDP development stage, and continual monitoring to ensure the resources are utilised.

Hence, third, in relation to influencing and managing the behavioural change of staff through designed-in systems and continual monitoring, it is important to address the implication of an employee's mental model – prior knowledge and what they know (Moqaddamerad and Ali 2024), and how industry regulatory changes affect communication and information sharing with staff in external organisations. Therefore, through this research, we highlight the importance of not only continuous monitoring but also how evaluators can be involved at an early stage of a project and establish realistic objectives, a common understanding with stakeholders, and a means to assess how the programme is to achieve the objectives as well as staff behavioural change (Trim and Lee 2019).

Fourth, reflecting on how the respondents value the importance of having guidance relating to the sharing of information in terms of achieving set tasks and strengthening trust-based relationships, we feel it is pertinent to add an extra component, which we labelled 'consequences'. The 'consequences' can be viewed as a resilient business operation and partnership arrangement that increases community well-being. Hence, the logic model approach, which is in place within organisations, allows senior managers to evaluate the organisation so that the IT/information systems policy (eg., security awareness) and the organisation's strategic direction is in harmony (Ebrahim and Rangan 2014).

The usefulness of network theory in relation to reducing risks and increasing an organisation's resource capability can be viewed from two different aspects. First, the degrees of flexibility of the structures and mechanisms that are in place in relation to established codes of conduct can be evaluated. Second, the external network dimension that facilitates the transfer of knowledge/information between staff in different organisations; as well as the organisational controls that are in place such as non-disclosure agreements are strengthened. As an SDP incorporates governance and compliance policy with the integration of structures, mechanisms and processes, organisational staff are able to interact freely

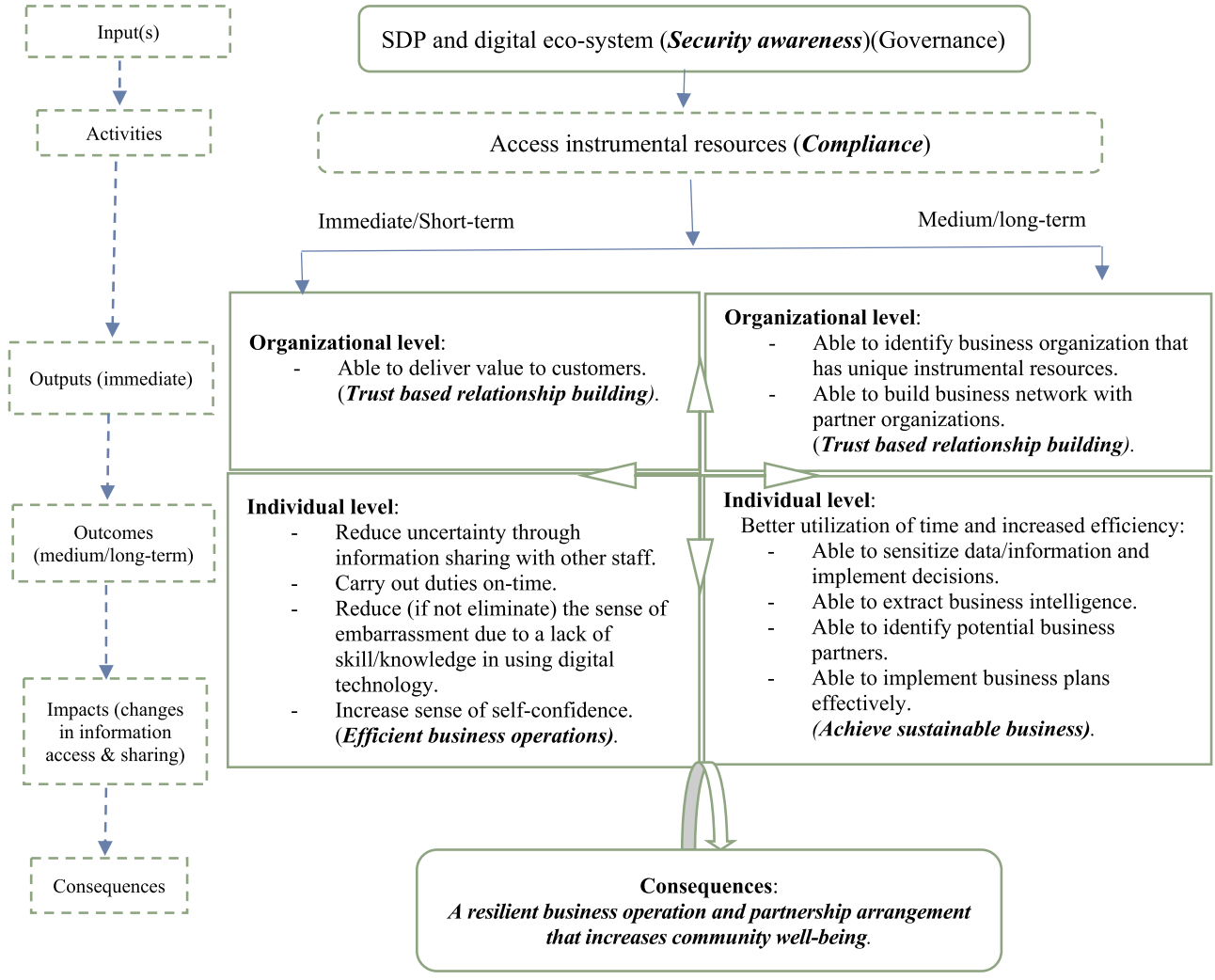

Diagram 1. SDP logic model in relation to increasing business capability and utilising network associations.

(vertically and horizontally) with staff in external organisations. Using an SDP, staff can utilise existing 'resource ties' effectively as well as access additional resources in the firm's network so that business capability is enhanced (Morgan, Feng, and Whitler 2018). In other words, by placing an SDP in the context of network theory, it allows us to deepen our understanding of how technology can be utilised to increase intra – and inter-organisational activity in terms of staff accessing and sharing information as well as gaining access to needed resources. The transparency gained helps employees to counteract tensions and avoid conflicts emanating from the issue of the control of information vis-à-vis the completion of specific business tasks. Such transparency not only reduces possible conflict between and among individuals/groups but also increases openness. Diagram 1 (Diagram 1: SDP logic model in relation to increasing business capability and utilising network) outlines how an SDP can be used to increase business capability and help staff utilise network associations.

As can be noted from Diagram 1, business-to-business managers can use the logic model approach to establish how network theory can help them utilise SMCT to increase the organisation's business capability through the process of sharing information with appropriate stakeholders, which reinforces the fact that interlinked digital platforms are necessary for devising an effective digital ecosystem. The outputs and outcomes listed in Diagram 1 highlight the need for staff to identify various resources that are to be utilised, and which aid the business decision-making process. One of the outcomes in the immediate/short-term is to increase an individual's self-confidence and, in the medium/long-term, achieve the effective implementation of business plans.

The logic model outlined in Diagram 1 integrates governance and compliance into a framework that helps staff based in partner organisations to integrate the organisation's systems/systems components more effectively, and integrates the governance mechanisms of partner

organisations in a way that reduces the risk of conflict between the parties (Agndal, Arvidsson, and Nilsson 2023). Staff know that their actions fall within sanctioned behaviour, and this increases their confidence. Increased confidence allows staff to sensitise information better and they are better able to identify business intelligence that contributes to achieving sustainable business. As an employee gains confidence, they have a positive emotional experience and benefit from an improved attitude (Borgatti and Halgin 2011) towards sharing information and identifying and utilising limited resources to achieve specific organisational objectives.

4.2. Managerial implications

To fully utilise the benefits of SMCT in a business context, senior managers need to integrate an SDP into the network structures of suppliers and marketing channel partners so business-to-business managers can exchange appropriate information and expedite business deals with relevant parties. For an organisation's intervention to work effectively, senior business-to-business managers pay attention to the currentness of DGM and DC and the relatedness of the changes in industry regulations. Also, continual interaction with staff and monitoring of staff behavioural change is needed, which solidifies the information embedded in trust-based relationships that harness business intelligence. An SDP can be regarded as facilitating the implementation of business plans and market entry strategies through digital strategy development, which requires a commitment to upgrading the skill base of staff. Thus, senior business-to-business managers need to be knowledgeable in terms of how different SMCT apps increase interoperability, consolidate business operations with partner organisations, and allow staff to handle unforeseen issues (eg., vulnerabilities) and challenges. The consequence of this is a resilient partnership arrangement that increases community well-being. Thus, the various parties concerned need to put in place an agreement as to how information is to be shared, in what form the information will be transferred and stored, and who else will have access to it. This will ensure that appropriate governance is provided, and compliance is viewed as ongoing and supported by various forms of intervention.

4.3. Conclusion

The logic model approach can be used to evaluate security awareness by holding accountable senior business-to-business managers, who are responsible for formulating and implementing security awareness programmes across the partnership arrangement. By identifying and putting in place appropriate organisational security subsystems, senior managers can increase the resiliency of the organisation and its partners and ensure that data, computer systems and networks are protected against various forms of attack. Meetings held at regular intervals allow senior managers to utilise existing resources and monitor and evaluate change brought about by advances in digitalisation. They can also forecast changes that bring about government intervention. By studying change in the digital operating environment, senior managers can link resource needs with resource availability and invest in appropriate systems and network connections. This should ensure that the security subsystems in place are integrated within the organisation's digital strategy, and governance and compliance play a prominent role. As regards information sharing, if individual staff go through self-reflection on the importance of data/information privacy as well as recognise the need for self-learning, then it is more efficient and effective in terms of compliance behavioural change compared with learning through predesigned training.

4.4. Limitations and future research

Our research has limitations that offer several opportunities for future research. A future study can be undertaken that explains how government policy is transforming traditional platforms into universally oriented digital platforms. The objective of such research would be to establish how digital platform developers and managers align organisational strategy with government objectives. This can be considered useful as it would help explain how a nation is driven to adopt initiatives such as business smart operations. Also, research can be undertaken that explains how business-to-business managers lower down the organisation's hierarchy can overcome their fears and inhibitions and develop confidence to use an SDP bearing in mind that the traditional view of corporate governance is being superseded by a community-driven governance approach resulting from increased digital transformation (Fenwick, McCahery, and Vermeulen 2019). Research can also be undertaken to understand how an SDP contributes to defining overarching general rules (Nitzberg and Zysman 2021) that are used to reinforce governance and compliance policy throughout the supply chain. The objective is to further explain how resources are obtained and shared within networks.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Agndal, H., A. Arvidsson, and U. Nilsson. 2023. "Managing Appropriation Concerns and Coordination Costs in Complex Vendor Relationships: Integration and Isolation as Governance Strategies." *Industrial Marketing Management* 113 (June): 116–127. https://doi.org/10.1016/j.indmarman.2023.05.023.

Agnihotri, R., R. Dingus, M. Y. Hu, and M. T. Kruch. 2016. "Social Media: Influencing Customer Satisfaction in B2B Sales." *Industrial Marketing Management* 53:172–180. https://doi.org/10.1016/j.indmarman.2015.09.003.

Ajzen, I. 2002. "Perceived Behavioural Control: Self-Efficacy. Locus of Control, and the Theory of Planned Behaviour." *Journal of Applied Social Psychology* 32 (4): 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x.

Bagozzi, R., and Y. Yi. 1988. "On the Evaluation of Structural Equation Model." *Journal of the Academy of Marketing Science* 16 (1): 74–94. https://doi.org/10.1007/BF02723327.

Bartlett, M. S. 1954. "A Note on the Multiplying Factors for Various chi Square Approximations." *Journal of the Royal Statistical Society* 16 (2): 296–298. https://doi.org/10.1111/j.2517-6161.1954.tb00174.x

Beas, M. I., and M. Salanova. 2006. "Self-efficacy Beliefs, Computer Training and Psychological Well-Being among Information Workers." *Computers in Human Behavior* 22 (6): 1043–1058. https://doi.org/10.1016/j.chb.2004.03.027.

Bhalavat, D., A. Doshi, N. Keni, and P. R. Shah. 2024. "Automated Compliance: A Privacy-Focused Solution for GDPR and DPDPA Adherence." In *13th International Conference on System Modeling & Advancement in Research Trends (SMART)*, 831–837. Moradabad, India (6th to 7th December): IEEE.

Bodendorf, F., S. Dentler, and J. Franke. 2023. "Digitally Enabled Supply Chain Integration Through Business and Process Analytics." *Industrial Marketing Management* 114 (June): 14–31. https://doi.org/10.1016/j.indmarman.2023.07.005.

Bonina, C., K. Koskinen, B. Eaton, and A. Gawer. 2021. "Digital Platforms for Development: Foundations and Research Agenda." *Information Systems Journal* 31 (6): 869–902. https://doi.org/10.1111/isj.12326.

Borgatti, S. P., and D. S. Halgin. 2011. "On Network Theory." *Organization Science* 22 (5): 1168–1181. https://doi.org/10.1287/orsc.1100.0641.

Brown, M., and R. Cudeck. 1993. *Alternative Ways of Assessing Model Fit*. Newbury Park, CA: Sage.

Browne, A. E., and G. G. Grant. 2005. "Framing the Frameworks: A Review of IT Governance Research." *Communications of the AIS* 15 (38): 696–712.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly* 34 (3): 523–548. https://doi.org/10.2307/25750690.

Byrne, B. M. 2010. *Structural Equation Modelling with AMOS: Basic Concepts, Applications, and Programming*. 2nd ed. New York: Taylor & Francis Group.

Capestro, M., C. Rizzo, T. Kliestik, A. M. Peluso, and G. Pino. 2024. "Enabling Digital Technologies Adoption in Industrial Districts: The key Role of Trust and Knowledge Sharing." *Technological Forecasting and Social Change* 198:123003. https://doi.org/10.1016/j.techfore.2023.123003.

Constantinides, P., O. Henfridsson, and G. G. Parker. 2020. "Introduction—Platforms and Infrastructures in the Digital Age." *Information Systems Research* 29 (2): 381–400. https://doi.org/10.1287/isre.2018.0794.

Cram, W. A., and M. Wiener. 2018. "Perceptions of Control Legitimacy in Information Systems Development." *Information Technology & People* 31 (3): 712–740. https://doi.org/10.1108/ITP-11-2016-0275.

Daowd, A., M. M. Kamal, T. Eldabi, R. Hasan, F. Missi, and B. L. Dey. 2020. "The Impact of Social Media on the Performance of Microfinance Institutions in Developing Countries: A Quantitative Approach." *Information Technology & People* 34 (1): 25–49. https://doi.org/10.1108/ITP-03-2018-0135.

DeVellis, R. E. 2012. *Scale Development: Theory and Application*. Thousand Oaks, CA: Sage.

Dey, B., D. Newman, and R. Prendergast. 2011. "Analysing Appropriation and Usability in Social and Occupational Lives." *Information Technology & People* 24 (1): 46–63. https://doi.org/10.1108/09593841111109413.

Ebrahim, A., and V. K. Rangan. 2014. "What Impact? A Framework for Measuring the Scale and Scope of Social Performance." *California Management Review* 56 (3): 118–141. https://doi.org/10.1525/cmr.2014.56.3.118.

Fenwick, M., J. A. McCahery, and E. P. M. Vermeulen. 2019. "The End of 'Corporate' Governance: Hello 'Platform' Governance." *European Business Organization Law Review* 20 (1): 171–199. https://doi.org/10.1007/s40804-019-00137-z.

Gagiu, P. C., and L. Rodriguez-Campos. 2007. "Semi-structured Interview Protocol for Constructing Logic Models." *Evaluation and Program Planning* 30 (4): 339–350. https://doi.org/10.1016/j.evalprogplan.2007.08.004.

Gawer, A. 2014. "Bridging differing perspectives on technological platforms: Toward an integrative framework." *Research Policy* 43: 1239–1249.

Ghobakhloo, M., H. A. Mahdiraji, M. Iranmanesh, and V. Jafari-Sadeghi. 2024. "From Industry 4.0 Digital Manufacturing to Industry 5.0 Digital Society: A Roadmap Toward Human-Centric, Sustainable, and Resilient Production." *Information Systems Frontiers*, https://doi.org/10.1007/s10796-024-10476-z.

Gregory, R. W., E. Kaganer, O. Henfridsson, and T. J. Ruch. 2018. "IT Consumerization and the Transformation of IT Governance." *MIS Quarterly* 42 (4): 1225–1253. https://doi.org/10.25300/MISQ/2018/13703.

Gupta, S., S. Modgil, B. Bhushan, U. Sivarajah, and S. Banerjee. 2023. "Design and Implementation of an IIoT Driven Information System: A Case Study." *Information Systems Frontiers* 27 (2): 523–537. https://doi.org/10.1007/s10796-023-10451-0.

Hair, J. F., W. C. Black, B. J. Babin, and R. E. Anderson. 2010. *Multivariate Data Analysis: A Global Perspective*. New Jersey: Pearson.

Hair, J. F., G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and S. Ray. 2021. *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R, Structural Equation Modeling: A Multidisciplinary Journal, Classroom Companion: Business*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-80519-7

Hanafizadeh, P., B. Hossravi, and S. H. Tabatabaeian. 2020. "Rethinking Dominant Theories Used in Information Systems Field in the Digital Platform era." *Digital Policy, Regulation and Governance* 22 (4): 363–384. https://doi.org/10.1108/DPRG-09-2019-0076.

Hartwick, J., and H. Barki. 1994. "Explaining the Role of User Participation in Information System use." *Management Science* 40 (4): 440–465. https://doi.org/10.1287/mnsc.40.4.440.

Hatch, M. J., and M. Schultz. 2010. "Toward a Theory of Brand co-Creation with Implications for Brand Governance." *Journal of Brand Management* 17 (8): 590–604. https://doi.org/10.1057/bm.2010.14.

Helitzer, D., C. Hollis, B. U. Hernandez, M. Sanders, S. Roybal, and I. Van Deusen. 2010. "Evaluation for Community-Based Programs: The Integration of Logic Models and Factor Analysis." *Evaluation and Program Planning* 33 (3): 223–233. https://doi.org/10.1016/j.evalprogplan.2009.08.005.

Henseler, J., C. M. Ringle, and M. Sarstedt. 2015. "A new Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modelling." *Journal of the Academy of Marketing Science* 43 (1): 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Hinings, B., T. Gegenhuber, and R. Greenwood. 2018. "Digital Innovation and Transformation: An Institutional Perspective." *Information and Organization* 28 (1): 52–61. https://doi.org/10.1016/j.infoandorg.2018.02.004.

Hoang, D., B. Igel, and T. Laosirihongthong. 2006. "The Impact of Total Quality Management on Innovation: Findings from a Developing Country." *International Journal of Quality and Reliability Management* 23 (9): 1092–1117. https://doi.org/10.1108/02656710610704230.

Issaoui, A., J. Örtensjö, and M. S. Islam. 2023. "Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance." *Future Business Journal* 9 (1): 107–120. https://doi.org/10.1186/s43093-023-00285-2.

Jabee, R., and M. A. Alam. 2016. "Issues and Challenges of Cyber Security for Social Networking Sites (Facebook)." *International Journal of Computer Applications* 144 (3): 36–40. https://doi.org/10.5120/ijca2016910174.

Jakobsen, M., and R. Jensen. 2015. "Common Method Bias in Public Management Studies." *International Public Management Journal* 18 (1): 3–30. https://doi.org/10.1080/10967494.2014.997906.

Jha, A. K., and N. K. Verma. 2024. "Social Media Platforms and User Engagement: A Multi-Platform Study on one-way Firm Sustainability Communication." *Information Systems Frontiers* 26 (1): 177–194. https://doi.org/10.1007/s10796-023-10376-8.

Jia, Y., L. Liu, and P. B. Lowry. 2024. "How do Consumers Make Behavioural Decisions on Social Commerce Platforms? The Interaction Effect Between Behaviour Visibility and Social Needs." *Information Systems Journal* 34 (5): 1703–1736. https://doi.org/10.1111/isj.12508.

Job, V., C. S. Dweck, and G. M. Walton. 2010. "Ego-Depletion – is it all Your Head?" *Implicit Theories About Willpower Affect Self-Regulation. Association for Psychological Science* 21 (11): 1686–1693.

Jones, N. D., T. Azzam, D. L. Wanzer, D. Skousen, C. Knight, and N. Sabarre. 2020. "Enhancing the Effectiveness of Logic Models." *American Journal of Evaluation* 41 (3): 452–470. https://doi.org/10.1177/1098214018824417.

Jordan, G. B. 2010. "A Theory-Based Logic Model for Innovation Policy and Evaluation." *Research Evaluation* 19 (4): 263–273. https://doi.org/10.3152/095820210X12827366906445.

Julian, D. A. 1997. "The Utilization of the Logic Model Level Planning and Evaluation as a System Device." *Evaluation Program and Planning* 20 (3): 251–257. https://doi.org/10.1016/S0149-7189(97)00002-5

Kaiser, H. 1974. "An Index of Factorial Simplicity." *Psychometrika* 39 (1): 31–36. https://doi.org/10.1007/BF02291575.

Kim, A., and A. R. Dennis. 2019. "Says who? The Effects of Presentation Format and Source Rating on Fake News in Social Media." *MIS Quarterly* 43 (3): 1025–1039. https://doi.org/10.25300/MISQ/2019/15188.

Kline, R. 2005. *Principles and Practices of Structural Equation Modelling. Second Edition*. New York: The Guildford Press.

Kraft, P., J. Rise, S. Sutton, and E. Roysamb. 2005. "Perceived Difficulty in the Theory of Planned Behaviour: Perceived Behavioural Control or Affective Attitude?" *British Journal of Social Psychology* 44 (3): 479–496. https://doi.org/10.1348/014466604X17533.

Kusumastuti, R. D., N. Nurmala, J. Rouli, and H. Herdiansyah. 2022. "Analyzing the Factors That Influence the Seeking and Sharing of Information on the Smart City Digital Platform: Empirical Evidence from Indonesia." *Technology in Society* 68:101876. https://doi.org/10.1016/j.techsoc.2022.101876.

Leonard, L. N. K., T. P. Cronan, and J. Kreie. 2004. "What Influences IT Ethical Behaviour Intentions-Planned Behaviour, Reasoned Action, Perceived Importance, or Individual Characteristics?" *Information and Management* 42 (1): 143–158. https://doi.org/10.1016/j.im.2003.12.008.

Lewis, K. 2024. "Digital Networks: Elements of a Theoretical Framework." *Social Networks* 77:31–42. https://doi.org/10.1016/j.socnet.2021.12.002.

Li, J., L. Chen, J. Yi, J. Mao, and J. Liao. 2019. "Ecosystem-specific Advantages in International Digital Commerce." *Journal of International Business Studies* 50 (9): 1448–1463. https://doi.org/10.1057/s41267-019-00263-3.

Li, L., H. Yu, and M. Kunc. 2024. "The Impact of Forum Content on Data Science Open Innovation Performance: A System Dynamics-Based Causal Machine Learning Approach." *Technological Forecasting and Social Change* 198:122936. https://doi.org/10.1016/j.techfore.2023.122936.

Liu, Y., J. Z. Zhang, S. Jasimuddin, and M. Z. Babai. 2024. "Exploring Servitization and Digital Transformation of Manufacturing Enterprises: Evidence from an Industrial Internet Platform in China." *International Journal of Production Research* 62 (8): 2812–2831. https://doi.org/10.1080/00207543.2023.2235020.

Longmeier, M., and S. Murphy. 2021. "Framing Outcomes and Programming Assessment for Digital Scholarship Services: A Logic Model Approach." *College & Research Libraries* 82 (2): 142. https://doi.org/10.5860/crl.82.2.142.

MacCallum, R., M. Brown, and H. Sugwara. 1996. "Power Analysis and Determination of Sample Size for

Covariance Structure Modelling." *Psychological Methods* 1 (2): 130–149. https://doi.org/10.1037/1082-989X.1.2.130

McLaughlin, J. A., and G. B. Jordan. 1999. "Logic Models: A Tool for Telling Your Program's Performance Story." *Evaluation and Program Planning* 22 (1): 65–72. https://doi.org/10.1016/S0149-7189(98)00042-1.

Mei, J., G. Zheng, and L. Zhu. 2022. "Governance Mechanisms Implementation in the Evolution of Digital Platforms: A Case Study of the Internet of Things Platform." *R&D Management* 52 (3): 498–516. https://doi.org/10.1111/radm.12494.

Meyer, R. E., and M. A. Höllerer. 2014. "Does Institutional Theory Need Redirecting?" *Journal of Management Studies* 51 (7): 1221–1233. https://doi.org/10.1111/joms.12089.

Mola, L., R. Kaminska, N. Richebé, and A. Carugati. 2023. "Social Strategies for Information Technology Adoption: Social Regulation Process of Mandated Enterprise Social Network Systems." *Technological Forecasting and Social Change* 192:122936. https://doi.org/10.1016/j.techfore.2023.122570.

Moqaddamerad, S., and M. Ali. 2024. "Strategic Foresight and Business Model Innovation: The Sequential Mediating Role of Sensemaking and Learning." *Technological Forecasting and Social Change* 200:123095. https://doi.org/10.1016/j.techfore.2023.123095.

Morgan, N. A., H. Feng, and K. A. Whitler. 2018. "Marketing Capabilities in International Marketing." *Journal of International Marketing* 26 (1): 61–95. https://doi.org/10.1509/jim.17.0056.

Morin, B., L. Mé, H. Debar, and M. Ducassé. 2009. "A Logic-Based Model to Support Alert Correlation in Intrusion Detection." *Information Fusion* 10 (4): 285–299. https://doi.org/10.1016/j.inffus.2009.01.005.

Murphy, M., and C. M. Sashi. 2018. "Communication, Interactivity, and Satisfaction in B2B Relationships." *Industrial Marketing Management* 68 (January): 1–12. https://doi.org/10.1016/j.indmarman.2017.08.020.

Nambisan, S., S. A. Zahra, and Y. Luo. 2019. "Global Platforms and Ecosystems: Implications for International Business Theories." *Journal of International Business Studies* 50 (9): 1464–1486. https://doi.org/10.1057/s41267-019-00262-4.

Nitzberg, M., and J. Zysman. 2021. *Algorithms, Data and Platforms: The Diverse Challenges of Governing AI. BRIE Working Paper 2021-1*. Berkeley: University of California.

Ogilvie, J., R. Agnihotri, A. Rapp, and K. Trainor. 2018. "Social Media Technology use and Salesperson Performance: A two Study Examination of the Role of Salesperson Behaviors, Characteristics, and Training." *Industrial Marketing Management* 75:55–65. https://doi.org/10.1016/j.indmarman.2018.03.007.

Peng, G., and O. Turel. 2020. "Network Ties in the Outside-in Strategy: Contingencies of Resource Endowments and Absorptive Capacity." *Industrial Marketing Management* 91 (September): 373–384. https://doi.org/10.1016/j.indmarman.2020.09.017.

Pentina, L., A. Koh, and T. T. Le. 2012. "Adopting Social Networks Marketing by SMEs: Exploring the Role of Social Influences and Experience in Technology Acceptance." *International Journal of Internet Marketing and Advertising* 7 (1): 65–82. https://doi.org/10.1504/IJIMA.2012.044959.

Quinn, R. W., and W. E. Baker. 2021. "Positive Emotions, Instrumental Resources, and Organizational Network Evolution: Theorizing via Simulation Research." *Social Networks* 64 (October): 212–224. https://doi.org/10.1016/j.socnet.2020.08.007.

Rangaswamy, A., N. Moch, C. Felten, G. van Bruggen, J. E. Wieringa, and J. Wirtz. 2020. "The Role of Marketing in Digital Business Platforms." *Journal of Interactive Marketing* 51 (1): 72–90. https://doi.org/10.1016/j.intmar.2020.04.006.

Renger, R., and A. Titcomb. 2002. "A Three-Step Approach to Teaching Logic Models." *American Journal of Evaluation* 23 (4): 493–503. https://doi.org/10.1177/109821400202300409.

Riahi, E., and M. S. Islam. 2024. "Employees' Information Security Awareness (ISA) in Public Organisations: Insights from Cross-Cultural Studies in Sweden, France, and Tunisia." *Behaviour and Information Technology* 44:79–101. https://doi.org/10.1080/0144929X.2024.2311734.

Safa, N. S., M. Sookhak, R. Solms, S. Furnell, N. A. Ghani, and T. Herawan. 2015. "Information Security Conscious Care Behaviour Formation on Organizations." *Computers and Security* 53:65–78. https://doi.org/10.1016/j.cose.2015.05.012.

Salovaara, A., and S. Tamminen. 2009. "Acceptance or Appropriation? A Design-Oriented Critique of Technology Acceptance Models." In *Future Interaction Design II*, edited by H. Isomäki, and P. Saariluoma, 157–173. London: Springer London. https://doi.org/10.1007/978-1-84800-385-9_8.

Schwarz, A., T. Rizzuto, C. Carraher-Wolverton, J. L. Roldán, and R. Barrera-Barrera. 2017. "Examining the Impact and Detection of the "Urban Legend" of Common Method Bias." *ACM SIGMIS Data Bases: The DATABASE for Advances in Information Systems* 48 (1): 93–119. https://doi.org/10.1145/3051473.3051479.

Serrano, A. C., E. Reynaud, H. M. Yasin, and Z. A. Bhatti. 2018. "How Perceived Corporate Social Responsibility Affects Employee Cynicism: The Mediating Role of Organizational Trust." *Journal of Business Ethics* 151 (4): 907–921. https://doi.org/10.1007/s10551-018-3882-6.

Setia, P., V. Venkatesh, and S. Joglekar. 2013. "Leveraging Digital Technologies: How Information Quality Leads to Localized Capabilities and Customer Service Performance." *MIS Quarterly* 37 (2): 565–590. https://doi.org/10.25300/MISQ/2013/37.2.11.

Suddaby, R. 2015. "Can Institutional Theory be Critical?" *Journal of Management Inquiry* 24 (1): 93–95. https://doi.org/10.1177/1056492614545304.

Surucu-Balci, E., Ç Iris, and G. Balci. 2024. "Digital Information in Maritime Supply Chains with Blockchain and Cloud Platforms: Supply Chain Capabilities, Barriers, and Research Opportunities." *Technological Forecasting and Social Change* 198:122978. https://doi.org/10.1016/j.techfore.2023.122978.

Tabachnick, B. G., and L. S. Fidell. 2014. *Using Multivariate Statistics*. Boston: Pearson Education.

Taherdoost, H. 2018. "A Review of Technology Acceptance and Adoption Models and Theories." *Procedia*

Manufacturing 22:960–967. https://doi.org/10.1016/j.promfg.2018.03.137.

Tannenbaum, M. B., J. Hepler, R. S. Zimmerman, L. Saul, S. Jacobs, K. Wilson, and D. Albarracin. 2015. "Appealing to Fear: A Meta-Analysis of Fear Appeal Effectiveness and Theories." *Psychological Bulletin* 141 (6): 1178–1204. https://doi.org/10.1037/a0039729.

Tiwana, A., and S. K. Kim. 2015. "Discriminating IT Governance." *Information Systems Research* 26 (4): 656–674. https://doi.org/10.1287/isre.2015.0591.

Trim, P. R. J., and Y.-I. Lee. 2019. "The of B2B Marketers in Increasing Cyber Security Awareness and Influencing Behaviour Change." *Industrial Marketing Management* 83: 224–238. https://doi.org/10.1016/j.indmarman.2019.04.003.

Van der Walt, E., J. H. P. Eloff, and J. Grobler. 2018. "Cybersecurity: Identity Deception Detection on Social Media Platforms." *Computers & Security* 78:76–89. https://doi.org/10.1016/j.cose.2018.05.015.

Venkatesh, V., and H. Bala. 2008. "Technology Acceptance Model 3 and a Research Agenda on Interventions." *Decision Sciences* 39 (2): 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x.

Venkatesh, V., and F. D. Davis. 2000. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies." *Management Science* 46 (2): 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926.

Walters, P. G. P. 2008. "Adding Value in Global B2B Supply Chains: Strategic Directions and the Role of the Internet as a Driver of Competitive Advantage." *Industrial Marketing Management* 37 (1): 59–68. https://doi.org/10.1016/j.indmarman.2007.06.010.

Zoppelletto, A., L. B. Orlandi, and C. Rossignoli. 2020. "Adopting a Digital Transformation Strategy to Enhance Business Network Commons Regeneration: An Explorative Case Study." *The TQM Journal* 32 (4): 561–585. https://doi.org/10.1108/TQM-04-2020-0077.