The role of B2B marketers in increasing cyber security awareness and influencing behavioural change

Dr. Peter R.J. Trim*

Senior Lecturer in Management,

Department of Management,

Birkbeck, University of London, Malet Street,

London. WC1E 7HX. United Kingdom.

Email: p.trim@bbk.ac.uk

Telephone 0044 (0)207 631 6764

Fax 0044 (0)207 631 6769

*Corresponding author.

Dr. Yang-Im Lee

Senior Lecturer in Marketing,

Westminster Business School,

University of Westminster, 35 Marylebone Road,

London. NW1 5LS. United Kingdom.

Email: y.lee@westminster.ac.uk

Telephone 0044 (0)20 3506 6893

Key words: Attitude functional theory, Behavioural change, Cyber security awareness, Persuasive communication

Declarations of interest: None.

The role of B2B marketers in increasing cyber security awareness and influencing behavioural change

ABSTRACT

Although cyberspace is providing business opportunities, it is evident that B2B marketers need to pay attention to how to reduce the vulnerabilities associated with the use of computer technology. To reduce the possibility of a data breach, senior management need to increase threat awareness through the development of a behavioural awareness programme. We address how B2B marketers can contribute to increasing cyber security awareness by relating to an individual's knowledge and attitude that influences their behaviour. By drawing on the information systems management, marketing, communication and motivational research (social psychology) literature, we explain how persuasive communication theory in conjunction with motivation theory can be used to create an awareness programme to influence behavioural change. A qualitative research strategy was deployed and the critical friendship group and the group interview method were utilized. Fourteen highly experienced security experts participated in the study. The findings indicate that the process of knowledge creation can be enhanced by deploying functional theories of attitudes as this provides a basis to categorize staff according to their level of motivation and knowledge. This means that B2B marketers can play the role of co-ordinator when devising and implementing an appropriate cyber security awareness programme to help staff counteract the actions of cyber attackers. By reducing the gap between self-efficacy and perceived expectation, the confidence level of staff will be increased and attitudinal behavioural change will occur throughout the organization.

1. Introduction

The Internet has been hailed by practising managers as a means to extend the company's market offering and at times enter new markets at speed as it provides an opportunity to interact directly with customers. B2B marketers are aware that the Internet is a mechanism for facilitating relationship building through connectivity, which can help them to alter business processes, improve client information usage and streamline supply chain activities (Lichtenthal & Eliaz, 2003; Makkonen & Vuori, 2014). Walters (2008) suggests that the Internet facilitates rapid interaction of a personalized nature between buyer and seller and provides information acquisition, distribution and storage, which reinforces the marketing decision-making process. Interactive technology does not come without a number of challenges however. The growing reliance on computer networks has been over shadowed by the intensity and sophistication of cyber attacks (HM Government, 2016) and has called into question the role that security plays within an organization.

The World Economic Forum (Vina, 2016) purports that the annual global cost of cyber crime (especially fraud and online money laundering) is a staggering US$445 billion and a growing body of evidence suggests that senior managers need to think in terms of three types of potential cyber attack (Maisey, 2014): (i) an opportunistic attack (eg., automated 'script kiddie'); (ii) a medium-level type of attack orchestrated by an organized crime group that is aimed at stealing information about customers for example; and (iii) a sophisticated, planned, coordinated and persistent attack carried out by a nation-state intelligence service.

What happened at Deliveroo in 2016 (Fortson, 2017, p.5) highlights the enormity of the problem confronting marketers: "Customers of the food delivery service were charged for phantom orders made by hackers who obtained login details for breaches of other systems". An organization's security culture can be enhanced by ensuring that staff do not click on spurious links or open bogus email attachments. An attack can originate from an external actor or from an employee (insider) or can be the result of an employee working in unison with an external hacker. Bearing in mind the sensitivity associated with monitoring employees and safeguarding customer information, it is important to remember what is at stake. For example, "it is estimated that more than 6m stolen credentials are leaked every day, either free or sold on as lists" (Fortson, 2017, p.5). Hence marketers need to think in terms of how to reduce the risks associated with a data breach because as well as the loss in business due to reputational damage, there is the likelihood that a fine will be imposed on the organization by a government regulatory body.

B2B marketers are becoming more aware of the risks involved in using the Internet, and are placing increased emphasis on managing relationships with staff in partner companies throughout the supply chain to ensure that sensitive and confidential data (eg., product specifications, sales figures and profit margins) and information (eg., sales territory agreements) is safeguarded. A data breach involving the details of contracts with suppliers might result in the company facing unexpected opposition when negotiating a deal with an existing customer company. The capability of staff in terms of data and information handling is known to affect the relationship and level of trust

between parties (Håkansson, Johanson & Wootz, 1977). Hence, a data breach is not only disruptive but has potential knock-on effects such as a reduction in the customer base as disaffected customers buy from alternative sources as a result of adverse publicity. This suggests that B2B marketers are required to communicate continuously with their counterparts in partner organizations and engage in interfunctional interaction (Ruekert & Walker, 1987). Should this be the case, the heads of the different business functions will be made aware of the need to increase cyber security awareness and assist with the coordination of various countermeasures.

To be effective, information security systems need to be designed to protect the organization's systems and structures from attack and also, make staff aware of the security threats that exist and how they can avoid increasing the organization's vulnerability to attack (Arachchilage, Love & Beznosov, 2016). The increased use of the Internet for B2B activities suggests that B2B marketers, by developing their knowledge of cyber security, will be better able to assist in-house information security staff as well as to contribute to minimizing potential knock on effects in the supply chain. This can be done by ensuring that the information flow between staff in partner organizations is carried out in a way so as to prevent computer hackers from deploying various schemes to trap people into parting with sensitive data and information. One method commonly used by fraudsters is the deployment of fake websites that contain harmful viruses, which once downloaded become active (Abawajy, 2014; Safa, Sookhak, von Solms, Furnell, Ghani & Herawan, 2015). Another method is to obtain passwords through means of social engineering, thus deceiving staff into parting with passwords that provide access

to the company's authorized network (Davis, 2007) and marketing data bases. Hence, by deploying an appropriate cyber security awareness programme that brings to the attention of staff the security policies that are in place, an organization can be made more resilient and less vulnerable to attack (Shillair, Cotten, Tsai, Alhabash, LaRose, & Rifon, 2015).

Safa et al., (2015) carried out research relating to how a user's poor Internet security behaviour increases the threat to an organization and explained why cyber security awareness is important at the organizational level in terms of limiting reputational damage. Esteves, Ramalho and De Haro, (2017) contributed to this line of thought by indicating how senior managers can become more alert to the problems associated with a cyber attack by familiarizing themselves with the type of attack that hackers are known to deploy. These are important points for top management to consider as they require guidance that includes creating a new knowledge vision for the organization (Nonaka & Takeuchi, 1995). Top management's awareness of cyber security issues will allow B2B marketers to be provided with a platform from which to play a role in helping to co-ordinate information security policy at various levels within the organization. Although security can be considered the prerogative of the information security department, B2B marketers can help co-ordinate and promote security policy throughout the supply chain and prevent hackers from gaining access to marketing data bases, through internal marketing initiatives. Dealing with cyber security issues should, therefore, be approached from the stance of interactivity and placed in a network approach as advocated by the IMP Group (Håkansson & Snehota, 1995; Makkonen &

Vuoir, 2014). By engaging more fully with staff in other business functions, B2B marketers will be more aware of the issues confronting the company, and will be able to provide advice and support. For example, conscious care behaviour (Safa et al., 2015) warrants that a user thinks through the consequences of their actions before and during working online, and is aware of the importance of building trust based relationships that are knowledge specific. Håkansson et al., (1977) argue that trust surfaces when a seller's reliability is questioned. B2B business operations involve various forms of specialized knowledge and buyers are known to avail themselves of the knowledge of staff in supplier companies especially when they are knowledge deficient (Håkansson & Wootz, 1979).

The Internet and other forms of technology aided communication can be used by B2B marketers to build trust and reliability (Walters, 2008) and a cyber security awareness programme will, we assert, help B2B marketers build on the trust based relationships that currently exist throughout the supply chain and the marketing channel. Bearing this in mind, we explain how B2B marketers can contribute to the development of a cyber security behavioural awareness programme and engage in effective communication that makes staff aware of the possible cyber threats confronting the organization. We use the theory of persuasive communication in conjunction with motivational and attitudinal theory in order to devise a cyber security awareness programme that influences behavioural change. By doing so, we add to the developing body of knowledge in the area of the interface between marketing and other business functions (Ruekert & Walker, 1987; Reid & Plank, 2000) and provide insights that build

on the view of de Swaan Arons, van den Driest and Weed (2014) that marketers are "thinkers". Also, the argument put forward by Kumar (2015, p.4) suggesting that marketing "must be an integral part of the organization's decision-making framework", resonates with us and we explain how B2B marketers can assist the development of an effective cyber security awareness programme that will raise the profile of marketers within the organization and its partners.

To extend our understanding of the communication process, we take into account the level of knowledge and motivation of staff and draw on insights into persuasive communication (Petty & Cacioppo, 1984; 1986), in conjunction with using functional theories of attitudes derived from social psychology (e.g., Katz, 1960; Fishbein & Ajzen, 1975; Ajzen, 1991; Herek, 1987; Wilcox, Kim & Sen, 2009). The reason why we adopted this approach is that the theory of persuasive communication places emphasis on the cognitive process of behavioural change associated with protecting an individual from risk/fear (Petty & Cacioppo, 1984; Boer & Seydel, 1996) and is well used in health related studies. It has also been applied recently in information security policy research (Ifinedo, 2012; Safa et al., 2015). The main advantage of using communication theory is that it allows B2B marketers to follow a specific process, develop a message and then gain feedback relating to the effectiveness of the message, so that the awareness campaign can be amended/updated through time.

Attitude functional theory (Katz, 1960; Herek, 1987; Shavitt, 1989; Eagly & Chaiken, 1993) is important because individuals have different levels of knowledge and

are dissimilar in what motivates them in terms of absorbing complex information. In addition, the work of Johnston and Warkentin (2010) is highly informative as their study provides insights into the influence of fear appeals vis-à-vis behavioural intentions. By drawing on such studies, we believe B2B marketers can better understand the reasons behind individual behavior and how a security awareness programme can overcome resistance and inertia (Tsohou, Karyda, Kokolakis & Kiountouzis, 2015). The security awareness programme outlined in this paper will, we feel, assist senior managers to understand which factors they need to take into account when establishing a communication message that encourages staff to engage in cyber security awareness issues. The outcomes, we feel, embrace an employee focus as they take into account employees' perceptions and indicate how managers can deal with 'knowing-doing gaps' (Pfeffer & Sutton, 1999; Jenkin, McShane & Webster, 2011). It is envisaged that the insights provided will generate further research that links B2B marketing management with evolving areas of significance such as safety, security and privacy (Cortez & Johnston, 2017). The recommendations made should help to provide practical B2B marketing solutions. By contributing fully to the strategic marketing intelligence decision making process and contributing to "cross-fertilization with external disciplines" (Lindgreen & Benedetto, 2017, p.1), B2B marketers will facilitate inter-function communication and help consolidate security related working routines.

2.0 Literature review

2.1 Internet usage and the need for an awareness programme

Through interactivity and connectivity, marketers improve operational efficiency, but need to reflect on the fact that criminal use of Internet technology communications is increasing (Kshetri, 2005). As well as this, B2B marketers are under pressure to improve services, reduce costs and deal with vendor operations more effectively (Lichtenthal & Eliaz, 2003). Although face-to-face meetings are known to reduce perceived risk, information is exchanged more frequently through computer to computer links and this tends to decrease the frequency of face-to-face interaction between staff. As a result, commitment and cooperation between staff is affected, and as a consequence there is a lessoning of trust between individuals (Leek, Turnbull & Naude, 2003). Lichtenthal and Eliaz (2003, p.8) note this and state: "companies know less and less about their trading partners", and as a result are placed at great risk. Esteves et al., (2017) suggest that hackers do not always attack a company's new computer system but seek a route through a vendor, a new employee or a compliance vulnerability. They recommend that managers conduct a high level "footprint" of the organization's computer systems at various times and ensure that employees know about the policies covering information sharing. B2B marketers are ideally placed to be involved in such activities owing to the fact that they manage a number of marketing data bases that contain a wide range of data and information relating to suppliers, customers and competitors for example. A data breach would increase organizational vulnerability because of diminishing trust with channel partners (Håkansson et al., 1977; Davis, 2007; Shillair et al., 2015; & Esteves et al., 2017). Safa et al., (2015) have argued, it is the users' lack of awareness and

understanding that are the main areas of concern and by increasing the knowledge level of employees, senior management have a foundation upon which to build behavioural change, and utilize further the skills of B2B marketers.

In order that a security policy is fully implemented and remains functional, B2B marketers are required to adhere to and comply with the organization's security policy. This view is supported by Arachchilage and Love (2014), who also suggest that security education helps thwart phishing attacks. It can be argued that cyber security awareness training needs to take into account online activities such as blogging, instant messaging and social networking that employees engage in while at work (Shaw, Chen, Harris & Huang, 2009). In order to be effective, training programmes are required to develop the knowledge base and raise the skill level of employees so that they increase their level of self-efficacy and respond accordingly to normative beliefs (Bulgurcu, Cavusoglu & Benbasat, 2010). We extracted definitions relating to 'normative beliefs' and 'self-efficacy' from various researchers (e.g. Bulgurcu et al., 2010; Safa et al., 2015; Tsai, Jiang, Alhabash, LaRose, Rifon & Cotton, 2016) that carried out information security studies based on the theory of planned behaviour. Hence, the term 'normative beliefs' refers to an employee's understanding of the organization's policies and their perceived social pressure regarding compliance and expected behavioural change; and as regards 'self-efficacy', this is an employee's assessment of their own level of knowledge and skills to complete tasks.

With respect to workable compliance polices, there are different types of cyber attack and staff require different advice as to how to respond proactively to them. It is also suggested that rewards (both tangible and non-tangible) should be provided to those that act in a compliant manner (Bulgurcu et al., 2010). It can be argued, therefore, that when determining how a security awareness programme is to be developed and communicated, attention is given to the level of knowledge and motivation that staff possess in relation to performing specific tasks (eg., updating customer files, responding to customer requests, undertaking a risk analysis and providing suppliers with intelligence).

2.2 Knowledge and cognitive behavioural change

Nonaka and Takeuchi (1995) explain that knowledge derived from outside the organization is utilized by internal staff to create new products, services and systems. B2B marketers perform a mediating role (e.g. that of middle manager) and a middle-up-down model of knowledge management is preferred in order to assist the knowledge development process. Such an approach allows B2B marketers to act as an integrator and motivator of knowledge creation. Should this be the case, individual managers can be empowered and held accountable for the development of tacit and explicit knowledge (Nonaka & Takeuchi, 1995; Nonaka, Takeuchi & Umemoto, 1996). The key point to note is that although individuals both absorb and develop knowledge, B2B marketers produce knowledge that is viewed as multi-dimensional in nature ranging from supply chain management to tailor made sales promotions. Furthermore, "knowledge cannot be created without an intensive outside-inside interaction. To create knowledge, the learning that

takes place from others and the skills shared with others need to be internalized – that is, reformed, enriched, and translated to fit the company's self-image and identity" (Nonaka et al., 1996, p.844). It is this that lies at the heart of organizational behavioural change.

An individual's desire to improve their "self-image" induces them to pay increased attention to how they consciously absorb and use information. Cognitive behavioural change occurs when an individual recognizes how new information might negatively or positively affect them, and how prevailing social norms/subjective norms might affect their social status or social image (Venkatesh & Bala, 2008; Tsai et al., 2016). Various studies have been undertaken regarding how technology is adopted based on the theory of reasoned action (Fishbein & Ajzen, 1975) and the theory of planned behaviour (Ajzen, 1991, 2002; Kraft, Rise, Sutton & Roysamb, 2005). Research undertaken by Venkatesh, Thong and Xu (2012) into the effectiveness of the unified theory of acceptance and use of technology (UTAUT) (Venkatesh, Morris, Davis & Davis, 2003), resulted in an extension of the model. UTAUT incorporated four constructs (performance expectancy, effort expectancy, social influence and facilitating conditions) and was extended to include three additional constructs: hedonic motivation, price value and habit; and UTAUT2 emerged (Venkatesh et al., 2012). This was an important development because habit, which incorporates experience, is interpreted from the perspective of an individual behaving as they are required to do having undergone a learning process that has conditioned them to act in a certain way (Venkatesh et al., 2012).

As regards the link between information usage and decision making, Acquisti and Grossklags (2007) indicate that people do not always have complete information, consequently, they are not always able to make an appropriate judgement or make a decision that is risk free. There is also a dichotomy between privacy attitudes and behaviour. Shortcomings and misunderstandings arise and an individual's own situation may worsen when they attempt to deal with what are in fact cumulative risks (Acquisti, 2004). Camp (2009) argues that there are several distinct methods and approaches to risk communication and that one approach is to simplify and overstate what the risk is so that a change in behaviour is forthcoming. Alternatively, it is possible to communicate more information and relate more directly to simple mental models of risk or possibly, detailed information can be communicated so that a rational response is derived from an individual in terms of their risk behaviour. Camp (2009, p.46) concludes by suggesting that: "Each metaphor offers a different solution to a different facet of the security problem. Each model communicates to end users particular images and activities if properly used". This work builds on the research into communications theory and modelling undertaken by Shannon and Weaver (1949), and Mason (Delone & McLean, 2003), and has validity as it can be used to reinforce why B2B marketers should be involved in devising appropriate cyber security awareness programmes as they can help clarify the main message and eliminate noise for example.

2.3 Increasing awareness through persuasive communication

Bada and Sasse (2014) acknowledge that a security awareness programme may be well thought through but deficient in terms of getting people to act responsibly. This is

due to a number of factors including personal characteristics, cultural differences, rewards and punishments, and media-framed messages. Taking into account that messages require interpretation due to the fact that they are complex and symbolically encoded, as well as technologically-mediated (Livingstone, 2004), it is important to note that the task-media fit model of communication (Mason & Leek, 2012) has highlighted the fact that the communication flow between individuals in a network can be disrupted and may influence a business relationship in a number of ways. Hence, B2B marketers need to pay careful attention to what messages a cyber security awareness campaign contains and how these messages are reinforced through time.

Modic and Anderson (2014) have contributed to our understanding of the social psychology of persuasion by suggesting that security awareness warnings should be non-technical and authoritative in nature. Persuasive communication theory, also known as the Elaboration Likelihood Model (ELM) (Petty & Cacioppo, 1984, 1986), is used widely by marketing academics and practitioners and has relevance in terms of explaining how people formulate a systematic information processing strategy (De Meulenaer, Dens & De Pelsmacker, 2015). The usefulness of the model is that variables that can impact certain judgements are made clear and also, the processes underlying changes in attitude are made known and so too are the resulting judgements (Petty, Rucker, Bizer & Cacioppo, 2004). It can be suggested that persuasive communication will enable employees to adopt an inward-directed approach that results in greater transparency and a commitment to increasing organizational effectiveness (Williams, 2005). Although normative beliefs may manifest in an issue being viewed as controversial (Mudrack,

2007), it should not detract from the fact that senior managers have a duty in terms of authority and leadership, in establishing compliance policy. There is wide variation in the way employees think and relate to the rules laid down, hence attention needs to be given to an individual's attitude, their reasoning patterns (Mudrack, 2007) and their capability (self-efficacy), if that is, behavioural change is to be managed effectively.

In order that information is communicated effectively to the intended audience, it has been suggested that managers should take into account the different levels of knowledge and motivation of individuals (Petty & Cacioppo, 1984, 1986). This view is supported by Acquisti (2004); Bulgurcu et al., (2010); Safa et al., (2015); and Tsai et al., (2016). These variables are important in terms of how individuals are persuaded, either via the central route or the peripheral route. When individuals have a high level of knowledge and motivation, attention needs to be given to the central route and how additional, new information is added as individuals process information in a cognitive manner. In the case of individuals that are less knowledgeable and less motivated, the peripheral route is deemed more effective because such individuals are likely to respond to emotional appeal/the attractiveness of the source.

Drawing on a rich and diverse body of knowledge relating to information processing and decision-making, Daft and Lengel (1986) argue that managers form coalitions with similar likeminded individuals but need to share their interpretation of an event/situation with a range of diverse individuals (eg., individuals that hold different views from others). By possessing information, it is argued that uncertainty is reduced

and so too is ambiguity (referred to as equivocality). Daft and Lengel (1984, 1986) explain that there are different forms of communication and that messages are transferred and absorbed in different ways through direct and indirect means. They argue that the richest form of information communication is face-to-face because it allows instant feedback (because of verbal and non-verbal cues) and is considered higher up the richness scale than normal text.

Borup, West and Thomas (2015) add to our understanding by indicating that there is insufficient knowledge regarding the richness of information provided vis-à-vis online feedback and their main contribution stems from the fact that they have undertaken mixed-methods research into the blended learning approach. They found that text was the most preferred source of feedback (Borup et al., 2015) and this it has to be said, strengthens the case for B2B marketers using a range of communication and feedback approaches, if they are to promote cyber security awareness to a wide audience. By understanding this, B2B marketers can form messages that are supported by metaphors that underpin appropriate organizational behaviour. By taking cognizance of the knowledge that exists both before and during the planning and execution of the cyber security awareness programme, B2B marketers can gain the trust and support of those receiving the message(s).

Underpinning this approach is the view that it is necessary to understand how employees change their attitude/behaviour and deal with impacts and the resulting consequences. The information provided also needs to take into account how B2B

marketers communicate and what knowledge they have in terms of using communications technology (eg., various social networks, apps, and tools). Hence security awareness is not just to be viewed in terms of how staff spend their time in the work environment, but it also requires a conscious behavioural change in the way computer communications technology is used outside the workplace. This is because hackers deploy various phishing techniques via social networking sites (eg., LinkedIn, MySpace, Facebook & Twitter) to target and trap vulnerable and non-suspecting individuals (Abawajy, 2014) who are tricked into parting with company information.

2.4 Motivational studies

In order to understand the motivational level of individuals, motivational theorists have undertaken research that explains how the motivation of individuals is related to their future intentions and as a consequence, functional theories of attitudes have been developed (Katz, 1960; Herek, 1987; Shavitt, 1989; Eagly & Chaiken, 1993). Functional theories of attitudes have been used over a number of years to comprehend the predictable intentions of individuals based on the different types of motivation that exist (Schade, Hegner, Horstmann & Brinkmann, 2016).

Shavitt (1989) and Wilcox et al., (2009) point out that motivational studies embrace attitudinal theories drawn from psychology, hence it is incumbent upon senior managers to know or make themselves aware of the various psychological functions that exist. For example, the knowledge function helps people to organize information and better understand their operating environment; the utilitarian function, relates to how

people obtain rewards or minimise punishment; the ego-defensive function, works to protect the 'self' from unpleasant situations or threats and maintain self-esteem; and the value-expressive function (self-expressive, which is one of the social functions), revolves around an individual expressing their central values and beliefs to other people through their behaviour. It is also worth noting that people adhere to self-presentation (eg., social-adjustive function, which is another social function). Therefore, behaviour is related to an individual gaining social approval and maintaining relationships with their peer group.

We believe that the application of persuasive communication theory in conjunction with attitude functional theory can help senior managers to utilize information that relates to how staff develop their level of awareness of specific types of threat, so that staff resonate with and remain motivated in terms of adopting the organization's cyber security policy. It can be argued that this approach resonates with the view of how new knowledge is created within an organization. The work of Nonaka and Takeuchi (1995) is informative in terms how an organization develops knowledge and innovates. Their example of the development of a bread making machine through observation of how the main actor (bread maker) creates bread is replicated, eventually, by a machine. Much effort is put into identifying the issues that need to be addressed when developing a bread making machine that produces bread of the highest quality. Similarly, if senior managers are to produce and implement a security awareness programme successfully, they need to identify their staff's level of knowledge and motivation as well as establish their attitude towards cyber security issues. Reflecting on

the bread making example, we produced a framework (Table 1) that synthesized the functional theories of attitudes based on knowledge and motivation vis-a-vis the context of cyber security awareness issues. We believe that Table 1 will help senior managers to recognize and identify individual staff in a systematic manner based on different levels of motivation and knowledge that exist so that appropriate training programmes can be devised to increase cyber security awareness. This will help and encourage individuals to develop their cognitive learning capability as well as nurturing a security culture. The wider implications of this approach can be derived from the following quotation from Walters (2008, p.67): "Policies therefore need to be developed regarding user data needs, information risks, and the assignment of access rights. Ideally, standardization is desirable but customization of service level agreements will be necessary because of the need to interact with multiple channel members".

Based on various studies relating to consumption motivation (e.g. Wilcox et al., 2009; Schade et al., 2016; Sharma & Chen, 2017), it can be said that when individuals are conscious of how to express themselves in terms of 'self', 'image', and social status among their peer group, they are more likely to be influenced by either the 'self-expressive' or 'social-adjustive' functions. However, when they are conscious of the need to save money, they are more likely to be influenced by the utilitarian function of attitudes. Hence, as regards the motivational aspect, we focus on the self-expressive, social-adjustive, and utilitarian functions.

Table 1: **Utilizing functional theories of attitudes to group individuals based on their knowledge and motivation towards embracing cyber security awareness issues**

Attitude	***Knowledge***	
	Low in knowledge	**High in knowledge**
Self-expressive (Value-expressive)	Highly motivated: need time and assistance to absorb complex information.	Highly motivated: able to absorb complex information and initiate certain courses of action.
Social –adjustive (Self-presentative)	Medium to low motivation: need encouragement as well as assistance to absorb complex information.	Medium to low motivation: need encouragement to absorb complex information.
Utilitarian	Low in motivation: need clear direction about punishment and rewards, and need assistance to understand complex information.	Low in motivation: need clear direction about punishment and rewards.

As regards the issue of how to establish effective communication in relation to increasing cyber security awareness within an organizational context, various researchers (e.g. Ifinedo, 2012, 2014; Safa et al., 2015; Itzchakov, Uziel & Wood, 2018) suggest that staff's ignorance, lack of awareness or mischief is due to either a lack of experience in terms of dealing with cyber/information security and involvement, misunderstanding or a lack of understanding regarding the organization's policy and its normative beliefs as well as a lack of information security self-efficacy. Therefore, we reflect on normative beliefs and self-efficacy and how these influence attitudes and link with variables of persuasive communication (eg., knowledge and motivation). It can be argued that the 'knowledge function' is an important factor in determining the way an individual's attitude is shaped and how their behaviour is influenced. Also, the knowledge function is interconnected with other functions of attitudes (Wilcox et al., 2009; Sharma & Chan,

2017). However, in order to understand fully how the knowledge function can influence attitude and instigate behavioural change in the context of cyber security awareness, it is necessary to pay attention to the gap between how an individual employee assesses their own 'self-efficacy' and their ability to deliver what their superior's expect them to in a timely manner based on understanding their organization's policy (normative beliefs). In addition, attention should be given to the motivation behind an individual's actions (eg., their ability to demonstrate their capability and progress their career or avoid punishment), as well as identifying necessary support that can be provided to help B2B marketers make daily decisions. This is because, if senior managers wish to increase staff engagement in cyber security awareness and reduce an organization's overall vulnerability, then they need to find a way to influence changes in behaviour and ensure that staff act in line with the organization's compliance policies and avoid costs associated with noncompliance for example (Bulgurcu et al., 2010).

Staff that have a high level of knowledge relating to the use of advanced communications technology and exhibit a value-expressive attitude towards cyber security awareness issues, are likely to be able to construe intense information and carry out their work in a positive manner as it involves expressing their values through reasoned argument. We denote such individuals as being highly influential. Staff engaged in monitoring network systems or carrying out routine tasks (eg., market analysis and pricing) also have a high technical knowledge and can be encouraged to raise their level of involvement by checking for fraudulent actions (eg., payments/invoices). Should this be the case, cyber security awareness will translate into

an embracing security culture that ensures problems are dealt with in real time and do not escalate into a crisis. Staff that possess a high level of knowledge but have the predisposition of a 'social-adjustive' attitude, are possibly less willing to process complex information, but will carry out the tasks required in the way that they have been asked to. In other words, such individuals exhibit a flexible/changeable behaviour depending upon their involvement with their peer group members. Less knowledgeable individuals regarding the utilization of advanced communications technology, can be motivated to increase their awareness of cyber security issues through an awareness programme, and can be provided with appropriate assistance so that they appreciate more fully the role that communications technology plays. This can be done through a different level of intensity of information and by crafting the message(s) accordingly.

Our focus is on addressing how senior managers can influence the attitude of staff and encourage them to be more aware of cyber security issues. We concur with Areni's (2003) view that when discussing complex topics (eg., security), it is important to recognize the influences associated with expertise and knowledge. An open communication style facilitates information sharing and knowledge transfer within and between organizations (Levinthal & March, 1993) as it takes into account an individual's willingness and motivation to engage in change. Rewarding staff for reporting concerns and incidents should stimulate staff and raise the profile of security within the organization. But also, constructs such as policy and law are fundamentally important in placing security in context, and making the information more meaningful to a wider audience.

3.0 Methodology

As we were seeking the knowledge of respondents in terms of their experience relating to security issues and how attitudinal behavioural change could be managed, we adopted the naturalistic enquiry method as outlined by Lincoln and Guba (1985) and the constant comparison method (Strauss & Corbin, 1990). The naturalistic enquiry method allowed the researchers to gain insights via real world examples and stories into how and why various security policies have evolved and been implemented in a B2B context. A strength of this approach was the embeddedness of the examples/stories within an organizational context that had a marketing component. The respondents in both sessions (critical friendship group and group interview) explained matters in their own words, which adhered to Denzin's (1989) approach whereby the interactions followed the form of a conversation. These research methods have been used by researchers such as Lenka, Parida and Wincent (2017) in their exploratory research and are viewed useful in terms of theory building.

By adopting the phenomenological approach (Patton, 1990), we focused on how security experts view the attitudes of staff in terms of managing security issues within an organization. We deployed a critical friendship group at first, and then, a group interview. When establishing the critical friendship group, we adhered and selected people based on the premise that the critical friend was able and willing to provide positive support (Bennett, Chapman, Cliff, Garside, Hampton, Hardwick, Higgins & Linton-Beresford, 1997) through the process of providing arguments and counterarguments. The advantage of this research strategy is that it allowed experts in different aspects of security that were

employed in different industry sectors to come together and discuss their experiences and provide insights into creating a security culture. We took into account Whetten's (1989) view regarding sensitivity to context and how important it is to develop new knowledge. This is why we placed much emphasis on selecting individuals who we considered to be the most appropriate people to participate in the data collection process (i.e. those who had experience of negotiating deals with international partner organizations or who had facilitated international business deals). The academics involved in the critical friendship group also had experience of the international negotiation process as they had worked in several industries and had been involved in various government-industry partnership arrangements and research initiatives.

Those taking part in the critical friendship group and the group interview were highly experienced security experts (academics, government representatives, law enforcement personnel, individuals from the security services sector, and senior managers from a number of companies), all of whom had in excess of twenty years work experience and possessed both practical and operational knowledge of the topics covered (Sinkovics & Penz, 2011). Fourteen people took part in the data collection process. The men and women were mostly in their late forties or early fifties and were aware of the need for increasing security and developing a security culture within their own organization as well as other industry sectors. This was because the majority of the respondents had worked both in the public sector and the private sector, and were operating at senior management level. They were in the main associated with or affiliated with various industry advisory boards and advised UK government departments on

matters of security. Recruited through personal networks over 12 months, the respondents were selected on the basis of their up-to-date knowledge of how illicit producers involved in counterfeiting, brand piracy and the production of fake websites for example, orchestrate attacks on reputable brands. The researchers had an appreciation of cyber security and security generally as they had attended a large number of security and intelligence workshops (either open to the public or closed and by invitation only). They had also attended various security and intelligence conferences over a long period of time, and had actively participated in a number of domestic and international security research networks. By attending such events, they developed an understanding of intelligence and security issues and this aided their learning process and allowed them to reflect on the information/experiences of others (Bennett et al., 1997). For example, one of the researchers had been involved in security and security related studies for two decades and had organized a number of security workshops (mainly at Birkbeck, University of London) and had established a number of critical friendship groups through time to facilitate the exchange of non-sensitive information and experiences. Through the process of forming various critical friendship groups, much had been learned about how to build bridges between academia, industry and government, and how to gain insights into how security threats manifest and change through time, and how society can be safeguarded from certain types of attack.

In fact, the respondents (critical friendship group and the group interview) were immersed in a highly interactive, supportive and caring community environment (Achinstein and Meyer, 1997; Bennett et al., 1997). Indeed, it can be argued that the

respondents possessed a shared vision and were allowed to speak freely during the sessions (except where they were restricted by their organization's policy) and were free to challenge their peers and engage in counterarguments when appropriate.

The respondents gave their permission for the sessions to be audio recorded and each respondent was assigned a number and was not referred to by name in the transcript. The researchers analyzed the data in the transcripts on a line by line basis. This also allowed the researchers to reduce the possibility of bias as all the discussions were recorded verbatim (Boyd & Westfall, 1970). During the critical friendship group and the group interview, the insights and examples provided were challenged in an open and constructive manner, and although probing occurred, each respondent was respectful of the limitations of the respondents in terms of divulging sensitive data and information. The approach was fruitful in the sense that it provided an opportunity for security experts and the researchers to discuss in depth the different challenges and reflect on the views of others.

The critical friendship group session lasted approximately 120 minutes and was managed by two researchers. The two researchers played a different role from each other. One presented a holistic security paper and the other researcher chaired the session and played the role of a critical friend and encouraged the participants to provide their interpretation and challenge the examples and stories that surfaced. The researcher that chaired the session also took notes and these were typed up after the session and then read through by both researchers to check the accuracy. The alterative examples and

stories that surfaced added depth to the discussions because they were contextually embedded and contained spontaneous episodes that gave rise to alternative examples (Boje, 1991). A number of topics were covered such as: a security culture; the link between intelligence and security; emerging business models and the strategic marketing paradigm; knowledge development and information processing; and marketing and communication. The objective was to establish the antecedents of a security culture and this was done through the process of raising questions, providing answers, and then reflecting on and challenging the assumptions relating to in-house security practices. Most importantly, the respondents considered that by engaging in critical reflection, it would allow the researchers to utilize their knowledge in terms of developing a cyber security framework and at the same time review their own practices and identify possible solutions that they could use in their own work environment (Golby & Appleby, 1997).

The group interview also took place in Bloomsbury at the University of London, two weeks after the critical friendship group, and the group interviewees were the same people that participated in the critical friendship group. The session lasted two hours and 30 minutes, and only two interviewees left before the interview had been completed as they each had another meeting to attend. The group interview method had the added advantage of allowing the researchers to explore the insights put forward by the interviewees (Brown, Collins & Duguid, 1989), and this allowed those involved to critically reflect on the linkage between the themes discussed. Three open ended questions were posed during the interview process, they were: (1) Which factors do

senior managers need to take into account when developing a sustainable cyber security awareness programme? (2) How can the strategic marketing concept be extended to incorporate security awareness issues? (3) How can B2B marketers contribute to security awareness throughout an organization? This allowed for greater conceptual density and specificity (Strauss and Corbin, 1990). It can also be noted that during the group interview session, the researchers took notes and read their notes several times thereafter.

The research strategy allowed the researchers to obtain quality data in a two-step approach outlined by Patton (1990): (i) indigenous concepts, first it was important to identify the key topics, hence during the critical friendship group the researchers identified common themes that existed across business functions: and then they underwent the process of (ii) sensitizing concepts - in the sense that the researchers posed further questions during the critical friendship group and the group interview, and then analysed the data collected. It was important to note that the arguments put forward needed to be understood from different perspectives because of the complexity of the subject. The respondents were required to reflect and offer tangible solutions (real world examples in the context of what the law would permit). This being the case, the respondents challenged their own understanding of the subject matter and substantiated the knowledge claims made (Suddaby, 2006). The respondents engaged fully in the topics covered and interacted with one another. The researchers adhered to an established code of ethical practice throughout and the names of individuals and their organizations were not disclosed. This was due to the sensitivity of the topic being researched. The

researchers made their own field notes as indicated above and compared their findings and interpretations with the insights in the transcripts (Glaser & Strauss, 1967).

4.0 *Analysis and Results*

The analysis went through various steps, such as a lengthy coding process of the transcripts to identify the themes. We applied the grounded theory approach (Strauss & Corbin, 1990), in the sense that we followed the procedure of open, axial and selective coding for consistency of the data analysis. Phrases were identified and labels were assigned. Based on the findings from the critical friendship group, 29 themes (first order) were identified by establishing relationships and patterns in the data. They were: collectivist behaviour; decision making; trustworthy behaviour; group decision making; communication; rules of the organization; corporate intelligence; the Internet; online behaviour; organizational culture; organizational behaviour; organizational learning; outsourcing; proactive behaviour; transformational leadership; managing change; individual learning; marketing strategy; planning; security culture; strategy; risk management; strategic intelligence; information exchange; risk analysis; training; loyalty; organizational resilience; and relationship management.

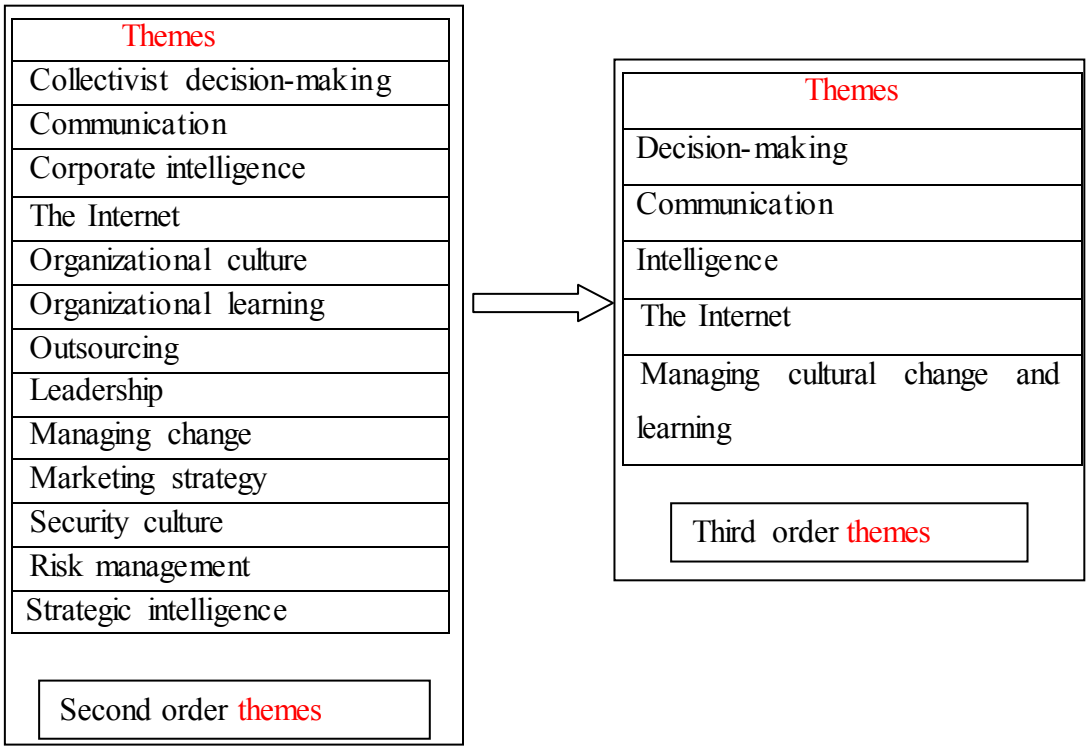
The analysis was related to the "phenomenon" in relation to "action/interaction" in the context of cyber security. After the critical friendship group, we forwarded the findings to those that had taken part in the session and we also presented the findings again to them at the start of the group interview. This was to establish a common understanding and to achieve additional feedback. It also ensured that the researchers did

not impose their views on the group and objectivity was maintained (Goldman, 1962). The interviewees were satisfied that the analysis was robust and representative. Based on the initial analysis of the critical friendship group, the researchers devised three open ended questions relating to how B2B marketers should relate to security personal involved with various security issues that affect the marketing operations of companies (as outlined above).

The researchers then proceeded with the group interview, and posed each of the three questions in turn. The usefulness of this approach was that by having the same respondents for both the critical friendship group and the group interview, they were familiar with the nature of the research and had the analysis of the critical friendship group in advance before they were involved in the group interview. The period of reflection proved useful in terms of thinking through the complex issues and challenges vis-à-vis increasing cyber security awareness. The advantage of providing the interviewees with the critical friendship group findings was that it allowed the researchers to get the respondents to establish, and identify with the "phenomenon", and validate the "phenomenon". By identifying and agreeing as to what constituted the phenomenon, the researchers were able to focus on how to manage the "intervening conditions" in order to manage the "action/interaction" in relation to establishing how to reduce an organization's vulnerability from a cyber attack. As regards the analysis of the group interview, we focused on the selective coding process and provided conceptual density (Strauss & Corbin, 1990; Lee & Trim, 2008), and revisited the data set from the critical friendship group to ensure that all the aspects were reflected on regarding the intervening

conditions. Having done so, we considered that it was necessary to reduce down the number of themes further and decided to carry out a further analysis by reinvestigating the data set to identify and better understand the phenomenon, the action/interaction, the intervening conditions, and what the consequences/outcomes were. This enabled us to identify 13 themes (second order) and then through further reduction, 5 themes (third order) (see Table 2).

Table 2: Second and third order themes **relating to developing a cyber security behavioural awareness programme**



The emerging themes (third order) were: the nature of decision-making; different forms of communication; the use of intelligence; the growing influence of the Internet; and managing cultural change and learning. To ensure the rigorousness of the data

analysis, the researchers read the group interview transcript separately a number of times and then came together to analyze the data, and then they checked what the other researcher had done. By referring back to their own notes, the researchers checked that the thematic groupings they had made note of matched those in the transcripts and this ensured that they were robust in their approach and were within the same "truth space" (Miles & Huberman, 1984a; Miles & Huberman, 1984b).

The themes and key insights from the group interview appear in Table 3. The data suggests that senior managers are required to identify organizational vulnerabilities and be aware of how employees deploy online behaviour. Hence individual managers need to look out for inappropriate behaviour and keep up with trends in online crime as indicated by Esteves et al., (2017). Any background checks carried out on potential employees will no doubt go through an ethical process. By understanding the importance that security plays in safeguarding the firm's operational capability, it can be suggested that staff will be motivated to change and adhere to the information/messages reinforced through the security awareness programme. As regards ensuring that the organization remains resilient, it emerged from the discussions that managers need to undertake risk management on a formal and continuing basis, and appropriate risk analysis tools need to be deployed. This represents a challenge because when the business environment is undergoing constant and rapid change, B2B marketers may find that the various risk analysis tools in use may be ineffective and alternative ones need to be developed.

Table 3: Themes and key insights relating to developing a cyber security behavioural awareness programme

Themes	Key insights
Decision-making	A community environment that promotes trustworthy behaviour. Establish appropriate intra-group and inter-group decision-making procedures and ensure that staff in human resource management are aware of the needs required and what systems need to be put in place.
Communication	A continual process of negotiation that convinces people what is being done is appropriate. A newsletter/workshop can be used to assist the internal process of communication. As well as the converted, disaffected people need to be incorporated in the communication process so that they are convinced of what needs to be done. The rules of the organization need to be made known and reinforced.
Intelligence	Undertake research of the operational environment and establish how information can be shared with relevant government organizations (law enforcement, security and intelligence for example). Undertake economic trend analysis and develop industry related competitive intelligence tools.
	A strategic approach should be adopted that utilizes forecasting and has a strategic intelligence focus that also focuses on resource needs. Senior managers need to be aware and understand that stakeholders may change through time and therefore strategic intelligence needs to be firmly linked with the concept of organizational resilience.
	Relationship management is perceived as necessary and underpins the customer relationship approach. Reputation management needs to be embraced by managers and they need to work with in-house intelligence and security specialists.
The Internet	Ensure that sensitive information is secure and that proper procedures are followed at all times.
	Identify organizational weaknesses and establish what aspects of employee's cyber lives (and especially their social networking on-line behaviour) may result in an organizational vulnerability. In addition, bad (insider) behaviour needs to be identified and dealt with and e-crime and various forms of threats (counterfeited products) need to be known about. A formal approach needs to be taken with regards to background checks on people recruited (both nationally and internationally).
Managing cultural change and learning	A clearly defined and benevolent organizational value system needs to be in place and loyal staff are rewarded.
	A formalized approach is adopted that is aimed at reducing friction between people and which highlights the need for cooperation and which discourages opportunistic behaviour. Career counselling, training and retraining are perceived as important and ongoing and need to be embedded in the organization's learning model, which should be aimed at raising the organizational skill base. Where possible, support can be provided for educational programmes at universities but it is important to have a hands on approach vis-à-vis content and standards.
	Various pro-active leadership approaches can be used and it is important to engage with people lower down the hierarchy. Individual managers need to think in terms of reinforcing the organization's reputation and how and why organizational behaviour should be adapted or changed. In particular, senior managers need to ensure that information security is a shared responsibility and the issues and challenges are dealt with across functions as soon as they arise.
	An appropriate organizational architecture needs to be in place so that highly

	motivated people can devise and implement change in a proactive manner.
	Risk management needs to be formalized and continual monitoring of risks is required so that actual and potential threats can be quantified and an appropriate impact analysis made. Managers need to ensure that risks are differentiated so that it is clear which risks relate to which aspects of the business and its operations. The organization's approach to risk management needs to be reviewed continually and appropriate risk analysis tools deployed.
	Priorities need to be set and attention given to cultural issues (organizational and national) and increased attention should be given to potential supply chain vulnerability.

5.0 Discussion

5.1 Establishing a security culture

It is clear from Table 3 that senior managers need to be aware of the growing importance attached to the human element of interaction with technology dimension and how the process of change is managed. The findings from the group interview highlight the fact that the security decision making process is ongoing and needs to take into account the interactions between functions (eg., intra-company and inter-company) (Håkansson et al., 1977). Inter-functional co-operation and decision-making allows security policy to be integrated into marketing policy and the use of communications technology should be monitored by IT (Information Technology) staff through the company's compliance policy and information/cyber security policy (Ifinedo, 2014). B2B marketers facilitate cooperation with internal financial staff regarding pricing, product investment and market entry decisions, and can undertake market analysis and formulate continuity of supply reports, competitor analysis reports and marketing contingency plans.

In order to synthesize the research findings with the literature review, we reflected upon the knowledge spiral concept (Nonaka & Takeuchi, 1995; Nonaka et al.,

1996). This is because cyber security is a new phenomenon and cyber attacks can affect business operations and the continuity of the business. Hence, senior managers need to know how the organization is to create new knowledge across functions and the organization's boundaries, so that staff can counteract the actions of computer hackers. In other words, as well as coordinating and communicating across functions and beyond the organization's boundaries, managers should also know how they can stimulate their staff to embrace a cyber security culture and gain additional knowledge and skills through a continual process of self development. By recognizing that staff possess a different level of knowledge and motivation (Table 1), and relate to cyber threats differently, managers can understand what needs to be done in order to bring staff up to the required level of behavioural awareness. Table 3 outlines how managers engage with staff and allow them to identify with the values of the organization. By understanding the different attitudes and the reasoning behind these attitudes, senior managers can devise appropriate training and staff development programmes within the organization to promote cyber security awareness programmes at all levels.

Based on our interpretation of the information in Table 1 and Table 3, we identified the factors that influence attitude/behavioural change of the six groups and we then formed six B2B staff groups (see Table 4). We also drew on the work of Cacioppo, Harkins and Petty, (1981) into cognitive response and provided insights (Seidman, 1991) into behavioural change. (Appendix 1 contains information relating to the definition of each group). From Table 4, the reader will note that the right hand column contains suggestions regarding how senior marketing managers can develop the message(s)/filter

information in relation to the level of knowledge and motivation by embracing and influencing the learning behaviour of each group. By differentiating between the groups in terms of their level of knowledge and motivation, senior managers can devise different types of training that contain different levels of knowledge. This is necessary because changing behaviour relates to the level of knowledge, the information possessed and the way the information or message is perceived (Acquisti & Grossklags, 2007). By making the risk explicit, staff can be influenced into changing their behaviour through the process of understanding the threats involved (Venkatesh & Bala, 2008; Tsai et al., 2016).

At this juncture, we would like to emphasize the role of the B2B marketer and consider that they undertake the role of co-ordinator (eg., through the process of social exchange), and contribute to the knowledge creation process within the organization (Nonaka & Takeuchi, 1995; Håkansson & Waluszewski, 2005). Individuals deemed to have a high motivation/knowledge as opposed to a low motivation/knowledge are likely to interpret the main message differently as they take into consideration the logic of the argument, the supporting arguments as well as the authenticity/reliability of the information source (eg., the person delivering the message) (Petty, Rucker, Bizer & Cacioppo, 2004). Those that are deemed to have a low motivation are not likely to develop a cognitive approach to understanding the information but are likely to pay attention to the attractiveness of the message and how other people identify with it (Daft & Lengel, 1986; Livingstone, 2004; Mason & Leek, 2012; & De Meulenaer et al., 2015).

Table 4: The characteristics and the influences associated with the different B2B staff groups.

Characteristics of each group	Information source for effectively influencing attitude/behavioural change
Star People that possess a high level of knowledge, are highly motivated in cyber security awareness issues. This group possesses a high self-expressive (value expressive) attitude.	*Stars* value information that comes from a reliable/credible source(s) as they are reliable and capable of dealing with complexity. The cognitive approach to problem solving is important in terms of relating the information to the source.
Adaptor People that possess a low level of knowledge but are highly motivated in cyber security awareness issues. This group possesses a high self-expressive (value-expressive) attitude.	This group appreciates both the technical and human complexities associated with cyber security challenges and try their best to improve their level of knowledge and adjust their attitude/behaviour in order to deal with the various threats that arise from time to time. *Adaptors* need and seek more explanation from credible sources and are pro-active in their approach. The cognitive approach to problem solving is viewed as important in terms of relating the information to the source.
Leader People that possess a high level of knowledge but are moderately motivated in cyber security awareness issues. This group possesses a social-adjustive attitude, and needs additional encouragement to be more involved in cyber security/cyber security awareness issues.	*Leaders* relate to information/messages that are episodic in nature and they relate affectively to the various cyber security issues and challenges as and when they occur. Their intelligence and support capability is appreciated. The cognitive approach to problem solving and the affection exhibited are just as important as the source of the information.
Semi-adaptor People who possess a low level of knowledge and are moderately motivated in cyber security awareness issues. This group possesses a social-adjustive attitude, and need encouragement to be more involved in cyber security/cyber security awareness issues. They also need assistance to comprehend matters fully.	*Semi-adaptors* relate to information/messages in episodic form and relate affectively to the various cyber security issues and challenges. *Semi-adaptors* absorb technical information/messages and require detailed information that uses limited technical jargon. The cognitive approach to problem solving is viewed as important and individuals can follow/relate to the information/message, however, further assistance is appreciated in order that they can comprehend technical information. Affection and the credibility of those associated with the information are viewed as important.
Satisfier People who possess a high level of knowledge but possess low motivation in cyber security awareness issues. This group is associated with the utilitarian attitudinal function.	*Satisfiers* possess a high level of knowledge and the capability to process information but are not motivated. Hence, in order to influence attitudinal change, the message needs to be focused on feelings (affection) in the first instance and needs to reinforce the satisfier's technical understanding. The information/message needs to be episodic based and needs to make the group feel that they should pay attention to cyber security issues. The source of the information needs to be viewed from the perspective of likability in order to stimulate the required response.
Reformer People who possess a low level of knowledge and a low level of motivation in cyber security awareness issues. This group is associated more with the utilitarian attitudinal function.	*Reformers* possess a low knowledge and are not motivated. They may well place the organization at risk because they are not vigilant and pay little attention to cyber security issues. In order that their attitude is influenced in a positive manner, the message needs to be focused on feelings (affection) at first, and reinforced by information/messages that explain in detail, with limited technical jargon, the key points that need to be understood and acted upon. The information/message needs to be simplified so that they resonate with it. The information/message needs to be episodic based and make people feel that they need to pay attention to cyber security issues. The source of the information needs to be viewed from the perspective of likability in order to stimulate the required response.

5.2 Six groups placed in a B2B context and how they contribute to cybersecurity awareness

Stars possess both a high level of knowledge regarding technology and are highly motivated and keen to be involved in cyber security awareness issues. For example, individuals in this group demonstrate that they are able to undertake market analysis, advise about inventory stock levels, and delivery methods and schedules. They communicate well and provide and receive relevant information from the right people based in different functions/organizations in real time by utilizing communications technology so that staff are able to reduce costs and improve the use of assets, and raise the quality of service for example (Lichtenthal & Eliaz, 2003). *Stars* prove highly influential in terms of establishing strong security awareness and a strong security culture. This group resonates with the metaphors and messages relating to cyber security awareness and are able to provide feedback as and when required. The *Adaptors* are highly motivated and advocate the need for cyber security awareness. However, at times they need assistance as regards understanding technical terminology. As these two groups share common characteristics and have similar values and beliefs (Katz, 1960; Snyder & De Bono, 1985) they are committed to improving the quality of their performance by adopting communications technology so that they are effective and efficient as regards adhering to the organization's cyber security policy (Safa et al., 2015). It is worthwhile to note however, that the *Adaptor* has a lower self-efficacy than a *Star*, nevertheless they are committed to performing their tasks to the standard required. Due to a lack of special knowledge to assess which communications technology is more effective, they just follow the guidelines provided by the firm. Therefore, the *Adaptor* needs to be subject to

a more detailed explanation. This means that the metaphors used to convey the message(s) should be jargon free and the message itself needs to be clear and unambiguous. The *Stars* and the *Adaptors* learn cognitively and observe continually how technology influences society. As these groups pay attention to the source of the information and its authenticity, they contribute to strategic marketing intelligence and forecasting through observing and communicating changes in customer requirements.

Leaders, although they possess a high level of knowledge and the capability to understand technology and cyber security issues, they tend not to be highly motivated or they exhibit a medium to low involvement in cyber security issues. In order to encourage them to adopt the required behavioural compliance, they need to be made responsible for issues affecting them (Ifinedo, 2014). *Semi-adaptors* tend not to be very motivated or wish only to exhibit a medium to low involvement in cyber security issues (Furnell, Khern-am-nuai, Esmael, Yang & Li, 2018). They have a lack of knowledge and find it difficult to absorb complex information. The common characteristic of these two groups is that they possess moderate interest in cyber security issues, but their level of interest and motivation changes depending upon the attitude/behaviour of other groups they identify with and whether they will be admitted to the group that they aspire to join (social-adjustive) (Smith, Bruner & White 1956; DeBono, 1987). In order to motivate these groups, attention needs to be given to how information is formulated in the sense that emotion and intellectual appeal prove stimulating, and interactive feedback is used to promote secure behaviour (Furnell et al., 2018). This suggests that senior management need to deploy various pro-active leadership approaches so that they can increase the

level of engagement with staff lower down the organizational hierarchy. By persuading staff that there are different types of risk associated with the firm's operations, it should be possible to convince staff that there is a need to continually monitor the risks identified and communicate openly, so that management can deal with the various threats in real time. Bearing these points in mind, the communication approach needs to take into account peer group association (eg., face-to-face interaction that is either physically or technologically-mediated) and the main message needs to be reinforced continuously due to the motivational level of the group members.

The *Satisfiers* possess a high level of knowledge but are not motivated to be involved in cyber security awareness issues or cyber security activities. They are apathetic and are not inclined to utilize their knowledge vis-à-vis understanding technology usage and its effect on social change. In order to attain the required behavioural change, it is important that this group is subject to fear-inducing arguments (Johnston & Warkentin, 2010). As regards the *Reformer*, this group lacks both motivation and knowledge regarding cyber security awareness issues. *Reformers* are not motivated and accept that they have a lack of knowledge regarding the subject and do not wish to be exposed and receive criticizm from their peers. They exhibit no interest in the subject of cyber security awareness. *Reformers* need to be made aware of the severity of the situation through fear appeals (Johnston & Warkentin, 2010) and they also need to be made aware of the punishments that exist for noncomplying with company policy in terms of an information breach for example. However, fear appeals may not have the desired effect because the message conveyed may be misunderstood or forgotten (Evans,

Maglaras, He & Janicke, 2016). The *Satisfiers* and the *Reformers* are not interested in cyber security but they are keen to avoid punishment or be exposed to embarrassment. In other words, we interpret the behaviour of *Satisfiers* and *Reformers* from a defensive stance as they try to disguise their lack of knowledge and/or their low self-esteem and in addition, try to be self-equable and avoid potential anxieties that arise from internal and external threats, and are keen to minimize punishments (Smith et al., 1956; Katz, 1960; Eagly & Chaiken, 1993). In order to motivate and encourage *Satisfiers* and *Reformers* to be involved in cyber security awareness issues, attention needs to be given to how the message is formed and the emotional underpinning of the message. This is particularly true as regards the *Reformer*. Referring to the *Satisfier*, the emotional approach is important but the information contained in the message should appeal to their cognitive capability as they tend to possess the capability to evaluate information in a logical manner, especially if they feel there are punishments or rewards related to the consequences of their actions (behaviour) for example. Hence, these groups value the effort put into supporting staff counselling, training and retraining, as this is perceived as a commitment to improving the skill set of staff. Those in-charge of the training programmes should ensure that the key messages used are transparent and the organization's social networking technology can be used for communication purposes (Leonardi, 2015). Staff also need to be aware of the rewards on offer as well as the punishments, because as Itzchakov et al., (2018) suggest, individuals may be governed by habit or the lack of ability to deliberate and think through a situation and act accordingly. Both, the *Satisfiers* and the *Reformers* need to be exposed to messages over a period of

time that are aimed at integrating episodic events that are reinforced by metaphors that highlight the advantage of appropriate security behaviour.

Different levels of cyber security training should be developed based on the needs of each group in terms of their level of knowledge, their motivation, their skill set and the type of support required. There are four points to consider: (i) the quality of the information received; (ii) the additional information needed but which staff do not have access to; (iii) the ability of the group members to integrate the information; and (iv) the ability of the group members to engage in critical appreciation as defined by Livingstone (2004) and Acquisti and Grossklags (2007). A pro-active approach to providing the level of support needed to bring an individual up to the required standard involves identifying future resources for training and learning support and allows structures to be put in place (Håkansson & Waluszewski, 2005). Training and support programmes can help individuals to reduce the gap between "self-efficacy" and their confidence level so that they perform their tasks appropriately (Ajzen, 2002; Bulgurcu et al., 2010). It can be argued that the process of interaction, which involves the sharing of tacit and explicit knowledge, supports organizational learning as it creates metaphors that are used to influence behavioural change.

5.3 Behavioural awareness and attitudinal change

It is clear from the forgoing that a cyber security behavioural awareness programme can be placed in the context of persuasive communication and help staff to counteract cyber threats. By paying attention to how a message is structured and how the

message is decoded, B2B marketers can use feedback through continual interactions to fine tune the metaphors used so that the desired outcome is achieved. It is for this reason that B2B marketers should take into account the seven postulates of the persuasive communication model, which are: correctness; the elaboration continuum; multiple-roles; objective-processing; biased-processing; trade-off; and attitude strength (Petty & Cacioppo, 1986; Petty et al., 2004). The postulates allow the B2B marketer to differentiate the message content so that a required change in behaviour is accommodated. Please see Figure 1.

Figure 1 can be used as a framework to establish a clear communication style/method to assist individuals in terms of recognizing the various cyber security related issues of relevance and how the threats identified are to be dealt with. More specifically, the cyber security behavioural awareness programme framework can be used by senior managers to think through the messages that are to be used to influence behavioural change. For example, by taking into account the interactions between individuals, it is possible to establish how explicit knowledge is turned into tacit knowledge and how tacit knowledge is turned into explicit knowledge (Nonaka et al., 1996). By understanding how individuals share experiences and reflect on why they are required to act in the way specified, managers can develop a common mental model relating to how cyber threats are perceived, interpreted and dealt with. The advantage of this approach is that managers can devise a sustainable knowledge creation process for dealing with evolving cyber security threats.

As regards the knowledge elaboration process, those forming the message(s) need to highlight the actual source of the information (eg., company staff, relevant government agency, media) so that an employee can check and validate matters. This is important because there will be more than one source of the information and some sources may be more influential than others. In addition, it is important to establish the truth of the message and provide evidence or draw on actual facts so that those exposed to the message accept it and change their behaviour in line with company policy.

Figure 1: Cyber security behavioural awareness programme framework encouraging staff involvement and attitudinal change

Persuasive communication (*correctness*)

A holistic view of security is required. Cyber security is viewed as a component of security and results in a shared responsibility among multiple stakeholders.

Issue-relevant information (*the elaboration continuum*)

People process information in a quantitative and/or qualitative manner and make value judgements based on high elaboration (security is perceived as necessary and an investment in protecting people as opposed to a cost and is unnecessary).

Variable and elaboration processes (*multiple-roles*)

Key variables influence attitudes towards cyber security in a number of ways because of the high personal relevance associated with cyber (individuals and organizations are actively undertaking activities online and may be vulnerable to attack). An individual's mood can be influenced by news of a cyber attack and its consequences.

The truth of a message (*objective-processing*)

Evidence is provided and people understand that cyber attacks have harmful consequences. The message perceived is that they are becoming more sophisticated, therefore putting individuals, the company and society at greater risk.

Counteracting arguments (*biased-processing*)

It is likely that arguments will be put forward suggesting that society is not at risk from cyber attack or that the threat outlined has been exaggerated. Notwithstanding, individuals are able to weigh up the facts and decide for themselves in an objective manner, and establish how real the threat is. Managers will think in terms of the organization's risk appetite and individuals will think in terms of their immediate security and the security of their family; and consider such issues as identity theft and day to day activities such as cyber bullying for example.

Examining information for merit (*trade-off*)

Both central and peripheral processes are known to influence attitudes through time because cyber attacks may occur and then, because security is tightened, not recur for some time. However, employees and people in society are aware that advanced persistent threats are well planned and implemented, and the number and frequency of sophisticated attacks are increasing and not decreasing.

Message processing (*attitude strength*)

Because cyber attacks have devastating consequences, employees and people in society understand why it is important to invest in security. In addition, people become hardened to the fact that security is an investment as opposed to a cost, and by understanding and sympathizing with people undergoing similar attacks in other countries, an international security perspective is adopted.

As discussed above, the difference in the level of knowledge and motivation of individuals affects the way the information is interpreted. Hence, it is important that senior managers pay attention to how information is structured and how the different B2B staff groups relate to it based on their knowledge, group identity, and their intention to comply with company policy. How it triggers curiosity from the perspective of the source of the information itself and how the different themes in the information account for changes in attitude/behaviour (Petty et al., 2004) are also of importance. By senior managers being able to build curiosity/intrinsic attraction into the information, it should provoke individuals into inter-group/function activity. An example of this, is the "continual process of negotiation", which is featured in Table 3. It can be suggested that a "continual process of negotiation" is needed in order to involve B2B staff and make them feel that they are part of the security process. Such a process helps to establish a common understanding of how regulations apply to the organization as well as preventing information from being leaked. The following quotation provides evidence of why B2B staff need to be fully engaged in security issues:

> "…we can talk about …how people leak information and sometimes it is done deliberately because they are disillusioned,… you have to say what is appropriate ….sometimes people leak information deliberately to cause damage, ..you know what is the disciplinary situation…" (Participant 2).

Reformers and *Satisfiers* need special attention as they are the groups most likely not to want to believe in reality and be apathetic in terms of adopting security measures. One participant in particular was very firm in their view as to why this may be the case:

> "Why people sabotage or leak information …they have stopped identifying with the organization [and] they have stopped identifying with the value system of the organization and that is why they are behaving like that .."(Participant 8).

With respect to counteracting arguments, the work of activists and anti-government and anti-business organizations cannot be ignored. The dilemma that surfaces is made clear in the following quotation:

> "This brings up one of the key issues about how we look at security issues. Do we look at every security threat or do we start to prioritize the security threat depending upon the situation? If we prioritise them, it means we put resources there to counteract that potential threat". (Participant 5).

Leaders, Semi-adaptors, Reformers and *Satisfiers* need to be made aware of the opportunity cost(s) so that they are able to understand why the company is investing in security. The following quotation is evidence of this train of thought:

> "…being aware of what we know is important, knowing how to anticipate a threat is absolutely crucial, knowing what to safeguard is key, knowing how it needs to be safeguarded is very important, assigning responsibility for security is absolutely key…" (Participant 2).

By establishing a clear understanding of what type of behaviour is acceptable, senior management can establish a set of rules, which have clear rewards and punishments (this is especially necessary for *Satisfiers* and *Reformers*). Having said this, senior management also need to create detailed information that reinforces the fact that everybody in the organization (as well as key staff in partner organizations) are required to take responsibility for their actions. By establishing a common understanding and increasing security awareness, B2B staff will take into account the different views in society and how society is absorbing change. Hence, senior management need to place security awareness in the context of organizational change and how the cultural value system encourages staff to be more open minded and proactive in terms of discussing security issues. The following quotations support this view:

> "Sometimes we have to understand that if something is fundamentally wrong within the organization ……..then somebody's got to be brave enough to stand up and say you know… we're heading in a direction we should never go, and that causes a lot of pain and a lot of conflict…." (Participant 2).

> ".. unless you change the perception of people it does not matter what models you bring in there will be no transformation …. organizational value systems have to be produced which are logical …." (Participant 5).

As regards the elaboration process, those providing information need to highlight its actual source so that an employee can validate matters and seek guidance if necessary. They also need to establish the truth of the information source and provide evidence that results in a change of behaviour and reward the individual for moving from the *Reformer/Satisfier* group to a higher order of learning group. The *Adaptors* although highly motivated, need to be given support in order to champion cyber security initiatives. How can the individuals in this group be involved? It is clear from the following statements what senior management can do:

> "Open communication is very, very important. ….We can have a newsletter that goes round and makes the key points available to people….We have to understand that people need to be trained and educated so that they have a proactive stance". (Participant 2).

> "Some organizations are now being proactive and they are putting suggestion boxes around the building to get people to give them ideas as to how they can improve systems and methods…….so maybe e-mail systems, discussion groups, informal group activity, the election of role models are all things that we can think of to change organizational value systems". (Participant 4).

By reinforcing the fact that cyber attacks are becoming more sophisticated and the level of the threat is intensifying, the *Stars* can act as message enforcers and help promote cyber security measures through word-of-mouth. This can be backed-up by electronic

word-of-mouth (eg., newsletters, bulletins, company notices and video clips) that contain episodic events that illustrate different views and complexities. Indeed, research undertaken by Siamagka, Christodoulides, Michaelidou and Valvi (2015) indicates that social media can be used in a B2B context to enhance an organization's image. Electronic word-of-mouth (eWOM) can be used to support information credibility (Hussain, Guangju, Jafar, Ilyas, Mustafa & Jianzhou, 2018) and the message processing component can be reinforced by drawing on correspondence/examples from law enforcement bodies. However, the information needs to be validated and placed within a context that B2B staff are able to understand. In-house seminars and workshops can be used to reinforce the message(s) and rewards can be used to encourage staff to report incidents quickly and thus help to strengthen security policy and harden security culture. The following quotation underpins the fact that a formalized security process and can be put in place:

> "My own company runs security seminars every year, for two days, and all the country managers have to come into it and they have to sign up to it and I have to train all the senior managers in the UK on security" (Participant 3).

As can be seen from the quotation above, senior managers also need to undergo a security awareness training programme and are held responsible for doing so (Esteves et al., 2017). This shows that the security awareness programme is ongoing and permeates through all the layers of the organization. Having a clear and well defined cyber security awareness programme in place is essential bearing in mind the vulnerabilities associated with outsourcing and offshoring. For example, B2B staff and marketers in particular, need to monitor how external vendors keep the company's confidential/sensitive data secure, and what standards they invoke in terms of buying in products (including software) from other external vendors. This can be viewed from the building relationship

perspective and embraces what is known as structural bonding (Han, Kim, Oh & Chung, 2008). Harnessing the commitment of staff in this way will increase operational effectiveness (Slater & Narver, 1995; Porter, 1996) and allow the organization to be more resilient and achieve a reliable reputation.

6.0 Conclusion

Although cyberspace is providing business opportunities, it is evident that B2B marketers need to pay attention to how to reduce the vulnerabilities associated with the use of communications technology. To reduce the possibility of a data breach, senior management need to increase threat awareness through the development of an awareness programme by relating an individual's knowledge and attitude to their change in behaviour. By drawing on functional theories of attitudes, we explained why and how staff can be catergorized according to their level of motivation and knowledge, and we linked this with persuasive communication theory, and established how B2B marketers can influence and change staff behaviour so that an organization minimizes its level of vulnerability. We did this by identifying six different groups of staff so that a security awareness programme could be tailored to help the cognitive learning process of individuals. The outcome of our research elaborates further how the knowledge spiral concept, advocated by Nonaka and Takeuchi (1995), and Nonaka et al., (1996), can be used in the context of increasing cyber security awareness and resilience. By identifying the gap between 'self-efficacy' and confidence that affects attitudes and motivation, we started to uncover the complexities associated with the various levels of learning, and the

importance of establishing a clear communication framework for consistency and transparency.

To be effective however, B2B marketers will need to explain to senior managers how and why persuasive communication theory can be used in conjunction with motivation theory, and how a cyber security awareness programme can be formed. This is so that a mechanism is put in place for keeping employees up-to-date about the current and evolving nature of cyber attacks. Hence, as well as creating awareness and offering guidance as to how to prevent cyber attacks from being successful, advice can also be provided as regards preventing disillusioned employees from causing damage to the company by accessing marketing data bases and tampering with customer data and information. The cyber security behavioural awareness programme framework outlined in this paper provides a basis upon which the behaviour of staff can be influenced so that they use communications technology without fear of putting the organization at risk. This is important because of the continual move towards doing business online and the skill and knowledge employees need to undertake their tasks.

B2B marketers are knowledgeable about building and maintaining relationships with staff in other business functions, and can develop these relationships further by contributing to the documents that outline the organization's security policy and procedures. To ensure that B2B staff view security from a holistic perspective, the security policy needs to be integrated into the organization's marketing policy so that B2B marketers are involved in the creation of knowledge, which can be utilized to turn

explicit knowledge into tacit knowledge and vice versa. As a consequence, the knowledge building process will be placed in the context of a learning organization. Furthermore, new working procedures and approaches will evolve that enable the organization to be less vulnerable to cyber attacks, which are in fact becoming more sophisticated and more persistent (HM Government, 2016). Through the process of identifying staff's level of knowledge and motivation as well as establishing their attitude towards cyber security issues, it should be possible to construct appropriate training programmes that nurtures an individual's cognitive learning capability and inspires them to gain additional knowledge and skills through a continual process of self-development. A pro-active approach to counteracting cyber threats will help senior managers ensure that security is viewed as a shared responsibility. This will assist B2B marketers because they need to develop a better appreciation of what risk management involves in order to include cyber threats in the strategic marketing intelligence process along with competitor threats for example.

6.1 Recommendations for managers and future research

It is clear that senior managers can as Williams (2005) suggests, combine an inward-directed approach (staff behavioural change) with an outward directed approach (relationship building with external stakeholders such as employees of partner organizations and law enforcement personnel) to counter the threats posed by cyber attackers. Reflecting on this view and the points above, a number of recommendations can be suggested: (1) Senior management need to adopt a more pro-active approach to cyber security awareness and integrate cyber security within the strategic marketing

intelligence planning process. (2) A range of cyber security educational and training/support programmes can be made available to employees and managers operating at different levels, so that they are made aware of the range of cyber attacks that exist. By individualizing training and ensuring that the training programme matches an individual's learning style, it should be possible to maximize the learning outcome. In addition, the support provided can uncover underlying conditions and attain relevant insights into learning needs. (3) Senior management need to promote an in-house security culture and engage with senior staff in partner organizations to ensure that they introduce and maintain appropriate security measures. For example, through the application of persuasive communication, management can develop an industry focused security awareness programme that ensures that the company's security strategy is communicated clearly throughout the organization and its partner organizations (eg., the supply chain particularly). The advantage of this is that a shared security culture will evolve that extracts expertise from the organizations concerned and individual managers will be able to mobilize "the learning of all its members in a process of continuous self-transformation" (Starkey, 1998, p.545). (4) Senior management need to ensure that risk assessment and risk analysis are incorporated within foresight planning. (5) Senior management need to ensure that a programme of continual learning is embraced that deals with risk communication, governance and compliance.

Reflecting on the above, six areas of future research can be identified. First, research can be undertaken to establish what type of cyber security training and staff development programmes need to be devised to develop the higher cognitive skill levels

of staff. Second, a study can be undertaken to establish how computer networks are transforming the company's business model and where the cyber vulnerabilities are in the supply chain. Third, research can be undertaken into how B2B marketers can assist senior management to deal with the issue of ego-depletion. Fourth, a study can be undertaken to establish how B2B marketers can devise appropriate cyber security behavioural awareness programmes in cooperation with staff in partner organizations so that security is viewed as a shared and co-operative activity and responsibility. Fifth, the communication and relationship building process is increasingly being viewed from the perspective of electronic word-of-mouth and digital communication (eg., ease of use and speed), however, it is still appropriate to use face to face communication as well because of the advantages associated with immediate feedback and the need for social interaction. Research can be undertaken to establish what is appropriate in terms of facilitating the interaction of staff in various business functions within the organization and in partner organizations. Sixth, future research can be undertaken into how B2B marketers are encouraged or discouraged from using communications technology for business purposes.

Appendix 1*: Definitions of the B2B staff groups*

The word *Star* can be traced to Latin, "stella" and Greek, "*aster",* and relates to the constellation and a character/person being considered influential to other people in terms of behaviour and/or achievements.

An *Adaptor* is somebody that adapts well to a certain situation(s) and is known to be reasonably flexible and supportive of others.

A *Leader* is someone who provides direction and takes it upon themselves to show others how to achieve something.

A *Satisfier* is an individual who is easily satisfied in terms of meeting their own expectations.

As regards a *Reformer*, we interpret this as somebody that wants to change their everyday existence and also the world in which they live.

Acknowledgements

The authors of the paper would like to express their gratitude to the reviewers of the earlier drafts of the paper for their in-depth and constructive feedback and the insights they provided.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33 (3): 236-247. http://dx.doi.org/10.1080/0144929X.2012.708787.

Achinstein, B., and Meyer, T. (1997). The uneasy marriage between friendship and critique: Dilemmas of fostering critical friendship in a novice teacher learning community, pp.1-21. *Annual Meeting of the American Educational Research Association*, Chicago, Illinois (24th to 28th March).

Acquisti, A. (2004) Privacy in electronic commerce and the economics of immediate gratification (pp.21-29). *EC' 04 Proceedings of the 5th ACM conference on Electronic commerce*" (17th -20th May). New York.

Acquisti, A., and Grossklags, J. (2007) What can behavioral economics teach us about privacy? (pp.363-380). *Digital Privacy: Theory, Technologies and Practices*. New York & London: Auerback Publications/Taylor & Francis.

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes,* 50 (2): 179-211. DOI: 10.1016/0749-5978(91)90020-T.

Ajzen, I. (2002). Perceived behavioural control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, 32 (4): 665-683. DOI: 10.1111/j.1559-1816.2002.tb00236.x.

Arachchilage, N.A.G., and Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38 (September): 304-312. http://dx.doi.org/10.1016/j.chb.2014.05.046.

Arachchilage, N.A.G., Love, S., and Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, 60 (July):185-197. http://dx.doi.org/10.1016/j.chb.2016.02.065.

Areni, C.S. (2003). The effects of structural and grammatical variables on persuasion: An Elaboration Likelihood Model perspective. *Psychology & Marketing*, 20 (4): 349-375. DOI: 10.1002/mar.10077.

Bada, M., and Sasse, A. (2014). *Cyber Security Awareness Campaigns. Why do they fail to change behaviour?* Global Cyber Security Capacity Centre: Draft Working Paper. Oxford: Oxford University. (July).

Bennett, C., Chapman, A., Cliff, D., Garside, M., Hampton, W., Hardwick, R., Higgins, G., and Linton-Beresford, J. (1997). Hearing ourselves learn: The development of a

critical friendship group for professional development. *Educational Action Research*, 5 (3): 383-402. DOI: 10.1080/09650799700200035.

Boer, Henk., and Seydel, Erwin R. (1996). Protection motivation theory. In M. Conner & P. Norman (eds), *Practicing Health Behavior: Research and Practice with Social Cognition Models*, pp.95-120. Maidenhead, BRK, England: Open University.

Boje, D.M. (1991). The storytelling organization: A study of story performance in an office-supply firm. *Administrative Science Quarterly,* 36 (1): 106-126. DOI: 10.2307/2393432.

Borup, J., West, R.E., and Thomas, R. (2015). The impact of text versus video communication on instructor feedback in blended courses. *Education Technology Research Development*, 63 (Issue 2): 161-184. DOI: 10.1007/s11423-015-9367-8.

Boyd, H.W., and Westfall, R. (1970). Interviewer bias once more revisited. *Journal of Marketing Research*, 7 (2): 249-253. DOI: 10.2307/3150117.

Brown, J.S., Collins, A., and Duguid, P. (1989). Situated cognition and the culture of learning. *Educational Researcher*, 18 (1): 32-42. Https://doi.org/10.3102/0013189X018001 032.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34 (3): 523-548.

Cacioppo, J.T., Harkins, S.G., and Petty, R.E. (1981). The nature of attitudes and cognitive responses and their relationships to behavior. In R. Petty, T. Ostrom, & T. Brock, (Eds.), *Cognitive Responses in Persuasion* (pp.31-54). Hillsdale, New Jersey: Erlbaum.

Camp, L.J. (2009). Mental models of privacy and security. *IEEE Technology and Society Magazine* (Fall), pp.37-46. DOI: 10.1109/MTS.2009934142.

Cortez, R.M., and Johnston, W.J. (2017). The future of B2B marketing theory: A historical and prospective analysis. *Industrial Marketing Management*, 66 (October): 90-102.http://dx.doi.org/10.1016/j.indmarman.2017.07.017.

Daft, R.L., and Lengel, R.H. (1984). The nature and use of formal control systems for management control and strategy implantation. *Journal of Management*, 10 (1): 43-66. Https://doi.org/10.1177/014920638401000105.

Daft, R.L., and Lengel, R.H. (1986). Organizational information requirements, media richness and structural design. *Management Science*, 32 (5): 554-571. Https://doi.org/10.1287/mnsc.32.5.554.

Davis, B.J. (2007). Situational prevention and penetration testing: A proactive approach to social engineering in organizations (pp.175-188). In A.W. Merkidze (Ed.)., *Terrorism Issues: Threat Assessment, Consequences and Prevention*. New York, NY: Nova Science Publishers, Inc.

DeBono, K. G. (1987). Investigating the social adjustive and value expressive functions of attitudes: Implications for persuasive processes, *Journal of Personality and Social Psychology*, 52 (2): 279-287. http://dx.doi.org/10.1037/0022-3514.52.2.279.

Delone, W.H., and McLean, E.R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 19 (4): 9-30. Https://doi.org/10.1080/07421222.2003.11045748.

De Meulenaer, S., Dens, N., and De Pelsmacker, P. (2015). Which cues cause consumers to perceive brands as more global? A conjoint analysis. *International Marketing Review*, 32 (6): 606-626. https://doi.org/10.1108/IMR-04-2014-0144.

Denzin, N.K. (1989). *The Research Act: A Theoretical Introduction to Sociological Methods*. Englewood Cliffs, NJ: Prentice Hall.

De Swaan Arons, M., Van den Driest, F., and Week, K. (2014). The ultimate marketing machine. *Harvard Business Review*, 92 (7/8): 54-63.

Eagly, A. H., and Chaiken, S. (1993). *The Psychology of Attitudes*. (1st ed). Fort Worth, TX:Harcout Brace.

Easterby-Smith, M., and Thorpe, R. (1997). *Research Traditions in Management Learning*. In J. Burgoyne, & M. Reynolds, (Eds.), *Management Learning: Integrating Perspectives in Theory and Practice* (pp.38-53). London: Sage Publications.

Esteves, J., Ramalho, E., and De Haro, G. (2017). To improve cybersecurity, think like a hacker. *Sloan Management Review*, 58 (3): 71-77. http://mitsmr.com/2mXYJdD.

Evans, M., Maglaras, L. A., He, Y., and Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9: 4667-4679. DOI: 10.1002/sec.1657.

Fishbein, M., and Ajzen, I. (1975). *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research*. Reading, Massachusetts: Addison-Wesley.

Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., and Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security*, 75 (June): 1-9. https://doi.org/10.1016/j.cose.2018.01.016.

Fortson, D. (2017). 90% of all attempted logins are by cyber-hackers. *The Sunday Times*, Business Section (2nd April), p.5.

Glaser, B.G., and Strauss, A.L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine.

Golby, M., and Appleby, R. (1995). Reflective practice through critical friendship: Some possibilities. *Cambridge Journal of Education*, 25 (2): 149-160. https://doi.org/10.1080/0305764950250203.

Goldman, A.E. (1962). The group depth interview. *Journal of Marketing*, 26 (3): 61-68. DOI: 10.2307/1248305.

Håkansson, H., Johanson, J., and Wootz, B. (1977). Influence tactics in buyer – seller processes. *Industrial Marketing Management*, 5 (6): 319-332. Https://doi.org/10.1016/0019-8501(76)90014-6.

Håkansson, H., and Snehota, I. (1995). *Developing Relationships in Business Networks*. London: Routledge.

Håkansson, H., and Waluszewski, A. (2005). Developing a new understanding of markets: Reinterpreting the 4Ps. *Journal of Business & Industrial Marketing*, 20 (3): 110-117. Https://doi.org/10.1108/08858620510592722.

Håkansson, H., and Wootz, B. (1979). A framework of industrial buying and selling. *Industrial Marketing Management*, 8 (1): 28-39. Https://doi.org/10.1016/0019-8501(79)90015-4.

Han, S-L., Kim, Y.T., Oh, C.Y., and Chung, J.M. (2008). Business relationships and structural bonding: A study of American metal industry. *Journal of Global Academy of Marketing Science*, 18 (3): 115-132. https://doi.org/10.1080/12297119.2008.9707520.

Herek, G. M. (1987). Can functions be measured? A new perspective on the functional approach to attitudes. *Social Psychology Quarterly*, 50 (4): 285-303. http://www.jstor.org/stable/2786814.

HM Government (2016). *National Cyber Security Strategy 2016-2021*. London: HM Government.

Hussain, S., Guangju, W., Jafar, R.M.S., Ilyas, Z., Mustafa, G., and Jianzhou, Y. (2018). Consumers' online information adoption behaviour: Motives and antecedents of electronic word of mouth communications. *Computers in Human Behavior*, 80 (March): 22-32. https://doi.org./10.1016/j.chb.2017.09.019.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security*, 31 (Issue 1): 83-95. https://doi:10.1016/j.cose.2011.10.007.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51 (Issue 1): 69-79. https://dx.doi.org/10.1016/j.im.2013.10.001.

Itzchakov, G., Uziel, L., and Wood, W. (2018). When attitude and habits don't correspond: Self-control depletion increases persuasion but not behaviour. *Journal of Experimental Social Psychology*, 75 (March): 1-10. https://dx.doi.org/10.1018/j.im.2017.10.011.

Jenkin, T.A., McShane, L., and Webster, J. (2011). Green information technologies and systems: Employees' perceptions of organizational practices. *Business & Society*, 50 (2): 266-314. Http://doi.org/10.1177/0007650311398640.

Johnston, A.C., and Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34 (3): 549-566.

Katz, D. (1960). The functional approach to the study of attitudes. *Public Opinion Quarterly*, 24 (2): 163-204. https://doi.org/10.1086/266945.

Kraft, P., Rise, J., Sutton, S., and Roysamb, E. (2005). Perceived difficulty in the theory of planned behaviour: Perceived behavioural control or affective attitude? *British Journal of Social Psychology*, 44: 479-496. DOI: 10.1348/014466604X17533.

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, 11 (4): 541-562. Doi:10.1016/j.intman.2005.09.009.

Kumar, V. (2015). Evolution of marketing as a discipline: What has happened and what to look out for. *Journal of Marketing*, 79 (1): 1-9. Https://doi.org/10.1509/jm.79.1.1.

Lee, Y-I., and Trim, P.R. J. (2008). *Strategic Marketing Decision-Making in Japanese and South Korean Companies*. Oxford: Chandos Publishing.

Leek, S., Naude, P., and Turnbull, P.W. (2003). Interactions, relationships and networks in a changing world. *Industrial Marketing Management*, 32 (2):.87-90. Https://doi.org/10.1016/S0019-8501(02)00222-5.

Leek, S., Turnbull, P.W., and Naude, P. (2003). How is information technology affecting business relationships? Results from a UK survey. *Industrial Marketing Management*, 32 (2): 119-126. Https://doi.org/10.1016/S0019-8501(02)00226-2.

Lenka, S., Parida, V., and Wincent, J. (2017). Digitalization capabilities as enablers of value co-reaction in servitizing firms. *Psychology & Marketing*, 34 (1): 92-100. DOI:10.1002/mar.20975.

Levinthal, D. A., and March, J.G. (1993). The myopia of learning. *Strategic Management Journal,* 14 (Special Issue), 95-112. DOI: 10.1002/smj.4250141009.

Lichtenthal, J.D., and Eliaz, S. (2003). Internet integration in business marketing tactics. *Industrial Marketing Management*, 32 (1): 3-13. PII: S0019-8501(01)00198-5.

Lindgreen, A., and Di Benedetto, C.A. (2017). The future of *Industrial Marketing Management*. *Industrial Marketing Management*, 67 (November): 1-4. https://doi.org/10.1016/j.indmarman.2017.09.009.

Lincoln, Y.S., and Guba, E.G. (1985). *Naturalistic Inquiry*. Newbury Park, California: Sage.

Leonardi, P. M. (2015). Ambient awareness and knowledge acquisition: Using social media to learn "who knows what" and "who knows whom". *MIS Quarterly*, 39(4), 747-762. https://dx.doi.org/10.1016/j.im.2013.10.001.

Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies, *The Communication Review*, 7 (1): 3-14. Https://doi.org/10.1080/10714420490280152.

Makkonen, H., and Vuori, V. (2014). The role of information technology in strategic buyer-supplier relationship, *Industrial Marketing Management*, 43 (6): 1053-1062. Https://doi.org/10.1016/j.indmarman.2014.05.018.

Maisey, M. (2014). Moving to analysis-led cyber-security. *Network Security* (May), pp.5-12.

Mason, K., and Leek, S. (2012). Communication practices in a business relationship: Creating, relating and adapting communication artifacts through time. *Industrial Marketing Management*, 41 (2): 319-332. Https://doi.org/10.1016/j.indmarman.2012.01.010.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69 (April): 151-156. Http://dx.doi.org/10.1016/j.chb.2016.11.065.

Miles, M.B., and Huberman, A.M. (1984a). Drawing valid meaning from qualitative data: Toward a shared craft. *Educational Researcher*, 13 (5): 20-30. Https://www.jstor.org/stable/1174243.

Miles, M.B., and Huberman, A.M. (1984b). *Qualitative Data Analysis: A Sourcebook of New Methods*. Newbury Park, CA: Sage Publications.

Modic, D., and Anderson, R. (2014). Reading this may harm your computer: The psychology of malware warnings. *Computers in Human Behavior*, 41 (December): 71-79. http://dx.doi.org./10.1016/j.chb.2014.09.014.

Mudrack, P. (2007). Individual personality factors that affect normative beliefs about the rightness of corporate social responsibility. *Business and Society*, 46 (1): 33-62. DOI: 10.1177/0007650306290312.

Murphy, M., and Sashi, C.M. (2018). Communication, interactivity, and satisfaction in B2B relationships. *Industrial Marketing Management*, 68 (January): 1-12. http://dx.doi.org/10.1016/j.indmarman.2017.08.020.

Nonaka, I., and Takeuchi, H. (1995). *The Knowledge-Creating Company*. Oxford: Oxford University Press.

Nonaka, I., Takeuchi, H., and Umemoto, K. (1996). A theory of organizational knowledge creation. *Unlearning and Learning for Technological Innovation* (Special Issue) 11 (7/8): 833-845. Https://doi.org/10.1504/IJTM.1996.025472.

Patton, M.Q. (1990). *Qualitative Evaluation and Research Methods*. (1st ed). Newbury Park, California: Sage Publications.

Petty, R.E., and Cacioppo, J.T. (1984). The effects of involvement on responses to argument quantity and quality: Central and peripheral routes to persuasion. *Journal of Personality and Social Psychology*, 46 (1): 69-81. http://dx.doi.org/10.1037/0022-3514.46.1.69.

Petty, R.E., and Cacioppo, J.T. (1986). The Elaboration Likelihood Model of Persuasion. In L. Berkowitz (Ed.), *Advances in Experimental Social Psychology*, Volume 19 (pp.123-205). New York: Academic Press. https://doi.org/10.1016/S0065-2601(08)60214-2.

Petty, R.E., Rucker, D.D., Bizer, G.Y., and Cacioppo, J.T. (2004). The Elaboration Likelihood Model of Persuasion (pp.65-89). In J.S. Seiter & R.H. Gass (Eds.), *Perspectives on Persuasion, Social Influence, and Compliance Gaining*. Boston: Pearson.

Pfeffer, J., and Sutton, R.I. (1999). *The Knowing-doing Gap: How Smart Companies Turn Knowledge into Action*. Cambridge, MA: Harvard University Press.

Porter, M. E. (1996). What is strategy? *Harvard Business Review*, 74 (6): 61-78.

Reid, D.A., and Plank, R.E. (2000) Business marketing comes of age: A comprehensive review of the literature, *Journal of Business-to-Business Marketing*, 7 (2-3): 9-186. DOI: 10.1300/J033v07n02_02.

Ruekert, R.W., and Walker, O.C. (1987). Marketing's interaction with other functional units: A conceptual framework and empirical evidence. *Journal of Marketing*, 51 (1): 1-19. DOI: 10.2307/1251140.

Safa, N.S., Sookhak, M., von Solms, R., Furnell, S., Ghani, N.A., and Herawan, T. (2015). Information security conscious care behavior formation in organizations, *Computers & Security*, 53 (September): 65-78. https://dx.doi.org/10.1016/j.cose.2015.05.012.

Schade, M., Hegner, S., Horstmann, F., and Brinkmann, N. (2016). The impact of attitude functions on luxury brand consumption: An age-based group comparison. *Journal of Business Research*, 69 (1): 314-322. http://dx.doi.org/10.1016/j.jbusres.2015.08.003.

Seidman, I.E. (1991). *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences*. (1st ed). New York: Teachers College, Columbia University.

Shannon, C., and Weaver, W. (1949)(Eds.).*The Mathematical Theory of Communication*. Urbana: University of Illinois Press.

Sharma, P., and Chan, R. Y. K. (2017). Exploring the role of attitudinal functions in counterfeit purchase behaviour via an extended conceptual framework. *Psychology & Marketing*, 34 (3), 294-308. DIO:10.1002/mar.20989.

Shavitt, S. (1989). Products, personalities and situations in attitude functions: Implications for consumer behaviour. In T. K. Srull (Ed.,), *Advances in Consumer Research*, Volume 16, (pp.300-305). Provo, UT: Association for Consumer Research.

Shaw, R.S., Chen, C.C., Harris, A.L., and Huang, H-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computer & Education*, 52 (1): 92-100. http://dx.doi.org/10.1016/j.compedu.2008.06.011.

Shillair, R., Cotten, S.R., Tsai, H-Y., S., Alhabash, S., LaRose, R., and Rifon, N.J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48 (July): 199-207. http://dx.doi.org./10.1016/j.chb.2015.01.046.

Siamagka, N-T., Christodoulides, G., Michaelidou, N., and Valvi, A. (2015). Determinants of social media adoption by B2B organizations. *Industrial Marketing Management*, 51 (November); 89-99. http://dx.doi.org/10.1016/j.imgmarman.2015.05.005.

Sinkovics, R.R., and Penz, E. (2011). Multilingual elite-interviews and software-based analysis: Problems and solutions based on CAQDAS. *International Journal of Marketing Research*, 53 (5): 705-724. DOI: 10.2501/IJMR-53-5-705-724.

Smith, M. B.., Bruner, J.. S., and White, R. W. (1956). *Opinions and Personality*. (1st ed). New Your, NY: John Wiley & Sons.

Snyder, M., and De Bono, K. G. (1985). Appeals to image and claims about quality: Understanding the psychology of advertising, *Journal of Personality and Social Psychology*, 49 (3): 586-597. http://dx.doi.org/10.1037/0022-3514.49.3.586.

Starkey, K. (1998). How can we learn from the learning organization? *Human Relations*, 51 (4): 531-546. https://doi.org/10.1177/001872679805100405.

Strauss, A., and Corbin, J. (1990). *Basics of Qualitative Research*. (1st ed). Newbury Park, California: Sage Publications.

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of Management Journal*, 49 (4): 633-642. Doi:10.5465/AMJ.2006.22083020.

Slater, S. F., and Narver, J.C. (1995). Market orientation and the learning organization. *Journal of Marketing*, 59 (3): 63-74. http://www.jstor.org/stable/1252120.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, 24 (1): 38-58. DOI: 10.1057/ejis.2013.27.

Tsai, H-y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., and Cotton, S. R. (2016). Understanding online safety behaviours: A protection motivation theory perspective. *Computers & Security*, 59 (June): 138-150. https://dx.doi.org/10.1016/j.cose.2016.02.009.

Venkatesh, V. and Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, 39 (2): 273-315. Https://doi.org/10.1111/j.1540-5912.2008.00192.x.

Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27 (3): 425-478.

Venkatesh, V., Thong, J.Y.L., and Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36 (1):157-178.

Vina, G. (2016). Patients in limbo after cyber attack. *Financial Times*, 3rd November, page 2.

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. DOI: 10.1016/j.indmarman.2007.06.010.

Whetten, D.A. (1989). What constitutes a theoretical contribution? *Academy of Management Review*,14 (4): 490-495. Https://doi.org/10.5465/amr.1989.4308371.

Wilcox, K., Kim, H.M., and Sen, S. (2009). Why do consumers buy counterfeit luxury brands? *Journal of Marketing Research*, 46 (2): 247-259. https://doi.org/10.1509/jmkr.46.2.247.

Williams, C.C. (2005). Trust diffusion: The effect of interpersonal trust on structure, function, and organizational transparency. *Business and Society*, 44 (3): 357-368. DOI: 10.1177/0007650305275299.