Enhancing cyber security behavior: an internal social marketing approach

Hiep Cong Pham
School of Business and Management, RMIT University Vietnam, Hanoi, Vietnam

Linda Brennan and Lukas Parker
School of Media and Communication, RMIT University, Melbourne, Australia

Nhat Tram Phan-Le and Irfan Ulhaq
School of Business and Management, RMIT University Vietnam, Hanoi, Vietnam

Mathews Zanda Nkhoma
School of Business and Management, RMIT University Vietnam, Ho Chi Minh City, Vietnam, and

Minh Nhat Nguyen
School of Business and Management, RMIT University Vietnam, Hanoi, Vietnam

Received 29 January 2019
Revised 22 May 2019
29 July 2019
29 August 2019
Accepted 5 September 2019

Abstract

Purpose – Understanding the behavioral change process of system users to adopt safe security practices is important to the success of an organization's cybersecurity program. This study aims to explore how the 7Ps (product, price, promotion, place, physical evidence, process and people) marketing mix, as part of an internal social marketing approach, can be used to gain an understanding of employees' interactions within an organization's cybersecurity environment. This understanding could inform the design of servicescapes and behavioral infrastructure to promote and maintain cybersecurity compliance.

Design/methodology/approach – This study adopted an inductive qualitative approach using in-depth interviews with employees in several Vietnamese organizations. Discussions were centered on employee experiences and their perceptions of cybersecurity initiatives, as well as the impact of initiatives on compliance behavior. Responses were then categorized under the 7Ps marketing mix framework.

Findings – The study shows that assessing a cybersecurity program using the 7P mix enables the systematic capture of users' security compliance and acceptance of IT systems. Additionally, understanding the interactions between system elements permits the design of behavioral infrastructure to enhance security efforts. Results also show that user engagement is essential in developing secure systems. User engagement requires developing shared objectives, localized communications, co-designing of efficient processes and understanding the "pain points" of security compliance. The knowledge developed from this research provides a framework for those managing cybersecurity systems and enables the design human-centered systems conducive to compliance.

Originality/value – The study is one of the first to use a cross-disciplinary social marketing approach to examine how employees experience and comply with security initiatives. Previous studies have mostly focused on determinants of compliance behavior without providing a clear platform for management action.

Information & Computer Security
Vol. 28 No. 2, 2020
pp. 133-159

2056-4961
DOI 10.1108/ICS-01-2019-0023

Internal social marketing using 7Ps provides a simple but innovative approach to reexamine existing compliance approaches. Findings from the study could leverage proven successful marketing techniques to promote security compliance.

Keywords Behavior change, Cyber security, 7P marketing mix, Human factors in security, Internal social marketing, Security compliance, Social marketing mix

Paper type Research paper

Introduction

The risks to an organization's sensitive information are constantly changing, and the loss of sensitive information continues to be a very real global concern. Juniper Research predicts that data breaches will cost US$8tn globally by 2022 (Fischer *et al.*, 2017). Organizations often implement a wide range of measures to ensure the security of information and associated computer resources. However, in recent years, cyber-incidents are becoming more frequent, more organized, costlier, and altogether more dangerous (Ismail, 2018).

Organizations seeking to establish secure environments must decrease risks from both internal users and external threats (Furnell and Rajendran, 2012). Internal risks can be alleviated by information technology security activities, such as policies and procedures. This includes instructions that an employee should be aware of, and comply with, to reduce information risks. User access to appropriate guidelines should reduce security risks (Tsohou *et al.*, 2015), but a majority of organizational security problems are indirectly caused by employees who violate or neglect the policies of their organizations. Employee compliance choices are therefore critical to maintaining a secure cyber environment (Warkentin *et al.*, 2007). Due to the ever-changing nature of information security risks, the effectiveness of a security program requires ongoing voluntary compliance from employees. Thus, the identification of organizational and personal (human) factors that motivate self-regulated maintenance of cybersecurity compliance is essential to any security training and communication program (Pham *et al.*, 2016b). The challenge for organizations is to develop infrastructure and programs to promote and maintain the requisite user behaviors to increase cybersecurity (Pham *et al.*, 2016a; Pham *et al.*, 2017).

Persuading people to undertake activities that are onerous or uncomfortable has been the subject of much research in the field of social marketing (Stead *et al.*, 2007; Truong, 2012). As defined by the National Social Marketing Center, social marketing is "an approach used to develop activities aimed at changing or maintaining people's behavior for the benefit of individuals and society as a whole" (Hopwood and Merritt, 2011). Internal social marketing (ISM) is the use of social marketing within organizational contexts to align, motivate, and coordinate employee behaviors (Smith and O'Sullivan, 2012). This is consistent with Rafiq and Ahmed's (2000) conceptualization of internal marketing, applied to social issues within organizations. ISM has demonstrable impact on driving the desired behaviors of internal stakeholders, notably in increasing pro-environmental behavior, health-related behavior, and service quality (Previte and Russell-Bennett, 2013; Smith and O'Sullivan, 2012). ISM can be employed as a potential solution to security compliance concerns when it comes to individual users (Pham *et al.*, 2016a). ISM builds beneficial exchanges between organizations and employees that are founded on understanding the employees' needs, requirements, interests, and motivations, accepting these exist, and can be addressed. ISM also shapes the system of interactions to ensure that both the organizational and individual goals are achieved (Smith and O'Sullivan, 2012). ISM uses the mutual exchange of value as a foundational principle for the co-creation of social good (Smith and O'Sullivan, 2012). Using ISM, organizations can persuade employees to pay a "price" such as time, effort or

convenience, in exchange for performing pro-social duties (Bate and Cannon, 2011; Thackeray *et al.*, 2007).

Given that ISM has been used successfully within organizations to enhance organizational performance, the principles of ISM can be extended to cybersecurity compliance. By concentrating on employees' orientations towards cybersecurity, ISM can highlight the benefits associated with following security guidelines, policies and practices, which are often perceived as valuable by employers but not by employees (Safa *et al.*, 2015). Furthermore, ISM helps organizations to identify influencing factors that may encourage employees to follow security policies. Understanding employees' perspectives allows organizations to develop effective communication and other strategies to deliver security behavior.

This paper presents an ISM approach which employs a marketing mix to provide a comprehensive understanding of how system users interact with various elements of a cybersecurity system. The study illustrates how a program based on the 7Ps marketing mix can promote and establish a behavioral infrastructure and devise a servicescape designed to enhance cybersecurity compliance. The paper aims to present a new conceptual framework for consideration by those aiming to reduce security risks.

The remainder of the paper is structured as follows: The next section provides a critical review of the ISM approach and servicescapes in the context of cybersecurity; followed by a description of the ISM 7Ps marketing mix; subsequently the research methods, data analysis and findings. Implications and suggestions for future research conclude the paper.

Internal social marketing and 7Ps marketing mix in cybersecurity

ISM and cybersecurity behavioral infrastructure

To understand ISM, it is necessary to first define its foundational theories: internal marketing and social marketing. Internal marketing is an effective strategy to enhance organizational capabilities and competencies, by influencing employees' attitudes and behaviors towards organizational goals (Smith and O'Sullivan, 2012). Social marketing adopts the concepts and techniques of commercial marketing to influence target audiences to adopt or sustain behavior in pursuit of social goals such as in increasing pro-environmental behavior, health-related behavior, and service quality (Binney *et al.*, 2006). ISM combines social and internal marketing, applying internal marketing to influence employees' attitude and behavior towards organizational changes, but to aiming to achieve social, rather than commercial, objectives (Brennan *et al.*, 2015).

The behavior development process of an individual can be mapped and managed under the framework of the servicescape (Bitner, 1992; Grönroos, 1984) (Figure 1). In the servicescape framework, the behavior development process results in a behavioral environment, in which a behavior is produced from the interaction between people, processes and physical environments (Christmas *et al.*, 2009; van Doorn *et al.*, 2010). The servicescape has also been termed 'behavioral infrastructure' (Lockrey *et al.*, 2018). The term behavioral infrastructure includes broader systemic issues that occur and fall outside the manageable and controllable servicescape environment (e.g. government, cultural, economic). In a servicescape, people are both a contributor to the problem and contributors to any solutions; and management is a process of managing the environment in which the behaviors occur (Brennan *et al.*, 2015).

Servicescapes are co-created between customers and organizations (i.e. employees and organizations seeking to enhance cybersecurity). By engaging affected people in the change processes throughout the entire servicescape, outcomes can be agreed upon, concerns addressed, and jointly decided actions and behavioral infrastructures can be created (Brennan *et al.*, 2015). In the cybersecurity context, a co-created environment is more likely to be sustainable because all parties agree on the requirements of a safe and secure cyber

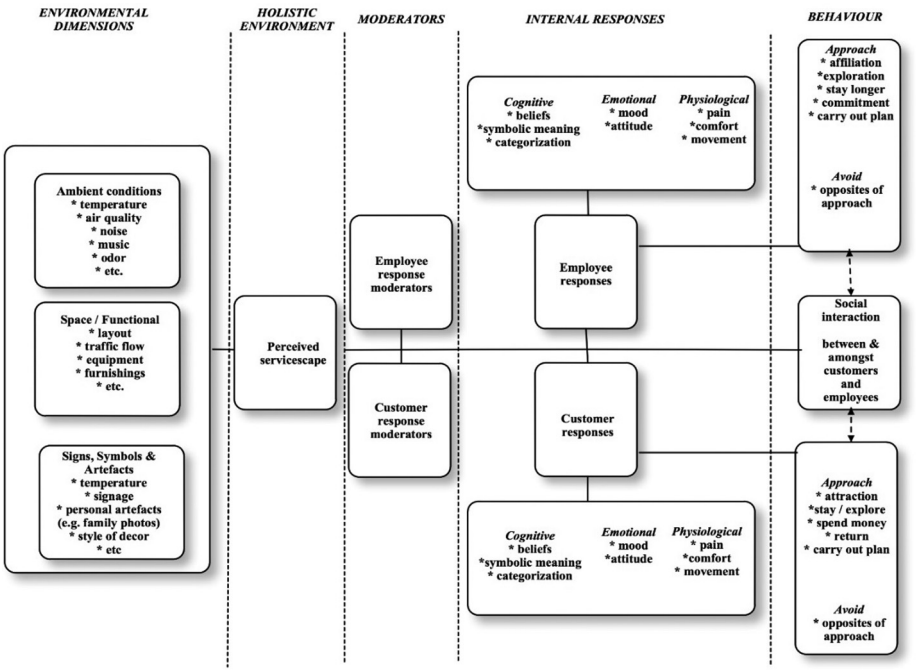

Figure 1.
Servicescapes in ISM

environment and accept their roles within that environment. A well-designed servicescape will therefore be able to motivate and engage people to overcome barriers and adapt new behaviors required for safe cybersecurity practice. A mutually agreed behavioral framework limits the potential for conflict and creates an environment that is both self-determined and sustained over time.

Motivating people to behave in accordance with organizational policies is required to protect information assets (Safa and Von Solms, 2016). Intrinsic motivation factors (such as enjoyment and interest) will motivate and maintain self-regulation, whereas extrinsic motivation factors (such as punishment or reward) have transient effects on self-regulation (Ryan and Deci, 2000). While self-regulation is the ideal situation, when it comes to cybersecurity, organizations cannot leave it to employees to be completely autonomous. Hence, employees and organizations must co-create an environment whereby individuals are able to actively monitor their personal efforts to evaluate and respond to security risks. However, organizations are challenged to develop a work-climate that permits people to self-regulate their compliance behavior. The role of ISM is to create interactions between participants in an organizational system that enable co-creation of a desired behavior (Brennan *et al.*, 2015).

ISM is concerned with employees' perspectives and actions that management can undertake to develop the requisite behavioral outcomes. To encourage and lead employees to regularly practice cybersecurity compliance, an organization needs an approach that helps to build understanding of employees' motivations and behaviors within the social system (Brennan *et al.*, 2015). ISM is premised on the tools and techniques of commercial marketing applied to the organizational context. The ISM planning process is presented in Figure 2.

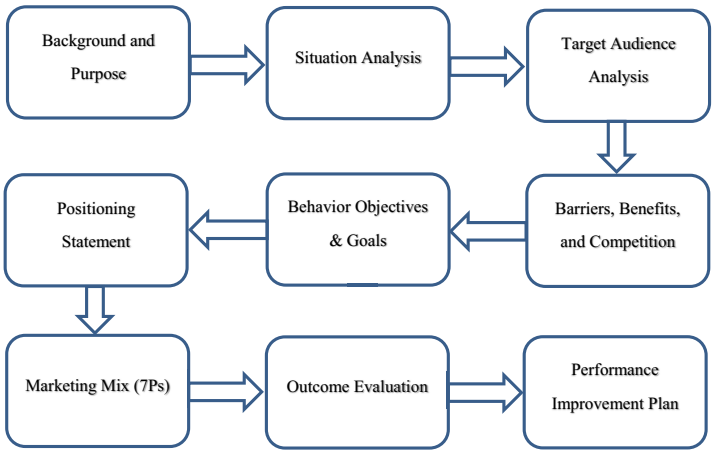

Figure 2.
ISM process

The ISM planning process follows nine systematic, and typically sequential, steps.

Step 1: reviewing the background and purpose of the ISM plan. This step establishes the social aspect that the project will address, factors that have led to the development of the plan, and the anticipated benefits of a successful campaign.

Step 2: assessing the current situation and environment. In this step, a SWOT analysis (strengths, weaknesses, opportunities and threats) is undertaken of the internal and external environment. This includes the identification of organizational (internal) strengths to maximize and weaknesses to minimize. It incorporates factors such as available resources, expertise, and management support. Similarly, organizational and environmental elements (external) that represent either opportunities to capitalize on or threats to prepare for are also identified. This step helps understand the specific situation and wider environment that an ISM campaign has to work with to succeed.

Step 3: analyzing target audience. This step involves obtaining a rich understanding of the target audiences, who are critical to the success of, and affected by, the campaign. This includes identification of their demographics, related behaviors, social networks, or state of change. Understanding the target audience enables better pinpointing of the positioning and marketing mix strategies in later steps to best engage these people.

Step 4: identifying barriers, benefits and competition of the target audience. By this point, both the audience and desired behavior are clear. The next step is to determine what the target audience is currently doing or prefers to do (the competition), what will motivate them to adopt the desired behavior, and what are the costs and benefits of performing the desired behavior.

Step 5: setting behavior objectives and goals. These will guide the marketing mix strategies; provide direction for evaluating outcomes and improvement in subsequent steps.

Step 6: creating a positioning statement. Positioning is the act of describing a program so that it clearly states the desired behavior relative to competing behaviors that the target audience should adopt. The positioning statement guides the development of the marketing mix that follows.

Step 7: developing a strategic marketing mix (7Ps) to facilitate the achievement of the marketing (behavior) objectives and goals. The elements of marketing mix serve as a set of determinants of the 7Ps (independent variables) used to influence behavior (the dependent variable). The next section shows how these elements might work in a cybersecurity context.

Step 8: evaluating the outcomes of the ISM campaign. This phase assesses the adequacy of resources employed to influence target audience's behavior, how the target audience responds to the marketing mix, the overall impact of the program or activities, achievement of goals, and the return of the investment.

Step 9: reviewing performance and developing improvement plan. This review identifies what refinements should be made and what priorities should be set to improve future campaign outcomes should the ISM program run again.

Appendix shows a detailed description of each of these steps in the ISM planning process.

The following section focuses on describing the marketing mix elements (step 7) of the social marketing plan.

Marketing mix (7Ps) in internal social marketing

A marketing mix in social marketing are any activities designed to achieve the objectives and goals of the marketing program. These activities are often conceptualized as "the 4Ps": product, price, promotion, and place. In services, this is expanded to "the 7Ps", adding physical evidence (or environment), processes, and people (Booms and Bitner, 1981). The 7Ps marketing mix has proven to efficiently enable organizations to understand their clients' behaviors and has been used in ISM to develop strategies or servicescapes that affect employee behaviors (Brennan *et al.*, 2015). In this paper, we identify the 7Ps as product, price, promotion, place, physical evidence, process and people. In ISM, the 7Ps provides a framework of activities that can be deployed to motivate employees to behave in the way that benefits both the organization and employees.

In the original marketing mix theory of Borden (1964), there were 12 marketing elements: product planning, pricing, branding, channels of distribution, personal selling, advertising, promotions, packaging, display, servicing, physical handling and research and analysis. There are of course, many elements to the management of marketing that do not neatly fit in with the conceptualization of the 7Ps. However, it is a rubric that works at categorizing the system of activities that are involved with ensuring that customer needs are met. The 7Ps framework is also useful in services because it permits a focus on the intangible aspects required to provide a service. The three additional Ps – people, processes, and physical evidence – were added to include a customer orientation, including a consideration of the unique marketing elements of service marketing that the 4Ps marketing framework does not account for (Anitsal *et al.*, 2012). *People* reflects customers (and interactions between customers, other customers and employees) who are the target of the marketing campaign (Ivy, 2008). *Processes* considers the systemic procedures used to recruit and retain customers and engage them in the service co-creation process (Grönroos, 2004). *Physical evidence* includes the 'hard' aspects of the servicescape that support the provision of the service (Russell-Bennett *et al.*, 2013). For example, a medical facility requires rooms for consultation, the doctor should appear professional and feel safe and clean. The physical evidence in this scenario is the office, the doctors' clothing, computers, medical certificates and awards on the walls, etc. The physical environment facilitates customer satisfaction and co-creation. To continue the medical facility analogy, the waiting room could be disordered, or there could be a computerized queuing system accessed upon entry, each of these alternatives leads to a perception of the quality of the service. The combination of the marketing mix leads to an overall perception of the quality of the experience.

ISM often uses a 7Ps framework to design a servicescape that meets the needs of the employee and achieves the organization's goals (Brennan *et al.*, 2015). In cybersecurity, these elements could be designed so as to enhance employee engagement with the product (i.e.

participating in the creation of a secure and safe cyber-environment). Furthermore, when it comes to cybersecurity, there is a more macro-social goal – one of creating a safer cyberworld for all. As such, ISM can more effectively motivate employees and support organizational security compliance objectives.

Each element P in the 7Ps marketing mix is now presented in the following section.

Product. A social marketing product is a behavior change or a shift in attitude, which is often more complex than a commercial product (Hopwood and Merritt, 2011). It is likely intangible and it requires a high level of involvement and effort on the part of consumer or customer (McDermott *et al.*, 2005). Customers must first perceive that they have a genuine problem to recognize their need for the solution (Weinreich, 2006). Furthermore, the benefits of the social marketing product are rarely immediate or direct (McDermott *et al.*, 2005). An ISM product is intangible and often takes the form of a solution to a problem. In the case of cyber security, the employees need to realize the relevancy of the given policy, understand the process, and have a strong motivation to comply (Pham *et al.*, 2019). To enact change, the organization must identify the conscious and unconscious factors and the personal, environmental and social approach to influence those factors (Bada *et al.*, 2015).

However, customers, in this case employees using IT systems, must first perceive that they have a genuine problem before they can recognize the need for a solution (Weinreich, 2006). In cybersecurity, the product is the compliance behavior of employees towards security policies and procedures, to create a safe and secure cyber-environment for themselves, and for the organization. These behaviors may comprise, but are not limited to, compliance with policies, conducting risk assessments, and reporting incidents (Coventry *et al.*, 2014). Changing behavior in cybersecurity requires more than providing policy and instructions. Employees need to realize the relevance of the given policy, understand the process, and have a strong motivation to comply (Bada *et al.*, 2015). Furthermore, they need to be able to comply with policy and be able to behave appropriately when required. That is, there must be motivation, opportunity and ability in order for desired behavior to occur (Brennan *et al.*, 2015). These factors, along with Bada *et al.*,'s (2015) personal, social and environmental factors, provide the barriers and facilitators for change. This leads us to the concept of "price". Price is the "cost(s)" associated with required behavior. For example, overcoming barriers "costs" time and effort.

Price. Price in social marketing is the costs-benefits trade-off associated with the required behavior (Hopwood and Merritt, 2011). Price relates to the costs that the target audience has to 'pay' and the barriers they have to overcome to adopt the desired behavior (Gordon, 2013). These costs can be psychological, cultural, social, temporal, practical, physical and financial (Gordon, 2013). The costs of performing a particular behavior are not necessarily monetary or even considered as purchase decisions or choices. People use heuristics or short cuts that save them time and effort thus 'saving' on the cost of a behavior. Sometimes these are engrained habits and descriptive norms that are easier to follow than learning something new or challenging (Brennan *et al.*, 2014). Consequently, encouraging an employee to pay a higher price in time and effort (i.e. increasing their ability) involves a paralleled increase in motivation and/or opportunity.

Employees' security costs for compliance are usually non-monetary, such as effort and time, and dealing with the costs associated with any disciplinary actions for non-compliance. To ensure the safety of information, employees have to acquire enough information security knowledge, spend time on practicing and remaining aware of protecting information (inconvenience) rather than only tend to their primary tasks (productivity). If the value of effort and time spent on protecting information is higher than the benefits of securing information, then compliance with cybersecurity will be at risk. On

the other hand, the price for organizations in implementing cybersecurity measures can be in the form of financial cost, such as the cost of providing training courses, building information security infrastructure or hiring human resources, Costs for organizations can also be non-financial, for example negative publicity, or compliance issues due to security compromises. Furthermore, there is the risk to commercial reputation and potential costs associated with leaks of high value information in a competitive environment, as well as costs associated with penalties for illegal activities (such as downloading unlicensed software). Thus, there are costs for both the organization and the employee. Balancing the respective costs and benefits requires shared understanding of the value of the proposed compliance activities to both parties.

Promotion. Promotion is the use of communication tools and techniques to foster positive social behaviors. Promotion can be any form of communication designed to persuade someone to behave in a particular way (Brennan *et al.*, 2014). Promotion can be interpersonal (e.g. personal transactions, word of mouth, seminars) and non-personal (e.g. advertising, public communications, direct e-mail). ISM tends to use existing organizational communications networks (Smith and O'Sullivan, 2012). Consequently, these networks might already be very cluttered with organizational communiqués and engaging the audience with a targeted message can be therefore problematic.

In cybersecurity, interpersonal promotion might be dissemination of security information during induction and orientation or training and development, where non-personal forms of promotion might be staff bulletin boards or email warnings. Promotion materials, such as guidance, certification, evidence of consequences, can be designed to generate positive behavior towards cybersecurity practice. For example, screens displaying severity and type of cyberattacks, warning signs, even small things such as cups on desks with logos promoting cyber safety, or the uniforms of IT staff as they wander around the building troubleshooting IT issues for users. Anything that promotes the message at the time that the audience is making their cost-benefit tradeoffs may nudge the behavior in the right direction (Spotswood *et al.*, 2012).

Place. Place has a number of different connotations in ISM. First, it refers to channels of distribution of service or products (Previte and Russell-Bennett, 2013). Secondly, it refers to ensuring that the product is delivered to the right person at the right time (Brennan *et al.*, 2015). Place in the social marketing mix can also refer to accessibility to the product, which can be perceived both as availability and affordability (Gordon, 2013). Affordability can be monetary and non-monetary (discussed under the element of price). Accessibility is anything that provides a barrier or facilitator for the behavior, making the behavior more or less doable depending on the circumstances (Brennan *et al.*, 2014). Thus, to change behavior, the easiest thing to do may be to change accessibility or availability and make the desired behavior easier to achieve. Environmental influences reflect the design of the environment, the physical environment such as the workplace, and the technology, but also economic factors (Coventry *et al.*, 2014). This study focuses on how supporting and necessary cybersecurity resources can be effectively distributed to the users at the place and time they need.

Physical evidence. Physical evidence in ISM pertains to a tangible aspect that may be either developed or used as a physical tool to initiate behavior change in a particular environment (Wasan and Tripathi, 2014). That is, it is the visible elements of service design (front stage) (Russell-Bennett *et al.*, 2013). Physical evidence can be the environment (buildings, workspaces, equipment, etc.), or it can be more micro level and behavioral; for example, how people talk to each other about issues and problems around the water cooler.

Elements of a physical environment are made up from its ambient conditions; spatial layout and functionality; and signs, symbols, and artifacts (Zeithaml, 2000).

Proper security practice can be established when employees are able to access relevant safe cyber information through signage, symbols or instructions at the time of using such service. In ISM, these elements are effective when used together. For example, a permanent sign on the door designed to remind users to lock their computer before leaving the office (physical evidence), versus a pop-up warning before opening a suspicious attachment (promotion). Such timely information generates and improves awareness of employees about information security compliance (Safa *et al.*, 2015; Safa and Von Solms, 2016). Furthermore, cybersecurity threats not only come from outside when employees act carelessly on information protection, they also happen internally when employees may opportunistically use others' negligence to steal and/or leak confidential information. Consequently, providing a safe cybersecurity environment requires consideration of the virtual and physical world in which secure or unsecure actions occur. The physical environment and the physical evidence within the environment provide the supportive behavioral infrastructure needed for security.

Process. Process pertains to the methods that create services, and which deliver benefits and value to customers through service design and process management (Grönroos, 2004). Service design and process management are two interconnected wheels of service quality that have a mutual effect on sustaining a behavior (Grönroos, 2004). Service design concerns itself with solving existing problems with innovative solutions, whilst, process management pays attention to day-to-day operations of the services (Bardhan *et al.*, 2010). Service design takes a longer-term strategic view of change and process management is more operational and immediate. Important to the distinction between services design and service process in the ISM context is that processes are invisible - backstage - the user does not see them working. While they support the achievement of the behavioral goals, the user does not necessarily know they exist (Russell-Bennett *et al.*, 2013).

Cybersecurity processes represent a set of systematic procedures that affect the execution of cybersecurity operations. Users must be able to rely on a clear and efficient set of instructions and associated procedures to fulfill their responsibilities. If the procedure of requesting and resolving IT solutions is time-consuming, employees might skip necessary tasks due to work pressures (Pham *et al.*, 2016b). Therefore, any support processes should be designed to encourage self-service (Liljander *et al.*, 2006; Ruiz *et al.*, 2017), but without risk to the system. That is, the user must actually be able to undertake the IT solution. However, this approach requires information security artefacts, guidelines and handbooks to be readily available and easily accessible to employees and/or appropriate levels of training having already been undertaken. Most of the time, non-compliant behaviors are due to the lack of user ability, thus, complex security processes need to be broken down in to short and achievable steps (Pham *et al.*, 2016b). Where possible, processes can be designed to ensure users either do not have to engage in cybersecurity (invisible and backstage processes), or, where user intervention is required, the processes are designed to ensure timely and effective availability of the necessary support. As complex and intensive training is not likely to be available in a cybersecurity emergency, emergent strategies will come from the combination of process and the other marketing mix elements. Security procedures and processes are sometimes considered as a burden for employees or they may be a stressful process (Coventry *et al.*, 2014; Pham *et al.*, 2019). The cybersecurity process needs to be designed to balance between security needs and usability. If the process leans too far in either direction, then this can lead to a super secure system that no one can use, or an unsecure system that everyone can use, even hackers (Bada *et al.*, 2015).

People. People, in the 7Ps framework, is the management of human resources to deliver the desired behavioral outcome (Previte and Russell-Bennett, 2013). People can be internal and external to the organization. In Bittner's original conceptualization (Figure 1), this was seen as customers (external) and employees (internal). In organizational cybersecurity contexts, the denotation of inside and outside can be extended to organizational units; employees and management or supervisors, for example. Or, where management and the IT team may operate outside the immediate environment of the user employee. The social interactions between these groups of people can produce behaviors such as complying with security requirements, advocating against behaviors that may lead to hacking, not engaging in unsecure behaviors, and so on.

In the cybersecurity context, the people factor consists of IT staff, who support processes and provide the guidelines on solving information security problems, and other user employees with their requests, knowledge and experience, and interactions with the environment. Human interactions within the cybersecurity system contribute to the outcome of any security program (i.e. whether safe or unsafe behaviors are modeled and shared). Another interaction among stakeholders is the commitment and support from supervisors, which has been considered as a key factor for the effective compliance of cybersecurity within an organization (Barton *et al.*, 2016; Bulgurcu *et al.*, 2010). Supervisory support is an important factor for compliance among employees, reinforcing positive attitudes and feelings of employees (Shafiq *et al.*, 2013). Supervisory support and commitment from managers can set a good example for employees for information protection, and positively influence the effort and responsibility towards the expectations for a secure environment (Barton *et al.*, 2016; Raineri and Paillé 2016).

Study method

Given that this study aims to describe phenomena, it adopted an inductive qualitative approach. The study conducted in-depth semi-structured interviews (group and one-on-one) with employees in several Vietnamese organizations regarding the use of IT, user perceptions of cybersecurity initiatives, and their compliance behavior. Their responses were categorized under the 7Ps marketing mix framework outlined above.

Inductive methods permit a reflexive approach to research design and data collection and analysis. It is suitable for complex contexts where there are more unknowns than knowns (as is often the case in social marketing) (Brennan *et al.*, 2015). In this context, qualitative methodologies are suitable to gain an understanding of the lived experiences and personal insights of users regarding the effectiveness of different cybersecurity.

The study employed a purposive sampling technique (Mazlina and Rozilawati, 2016) to recruit participants, because personal and private responses from users about their own companies' security initiatives were required (Belk, 2007). Participants were sought in a diverse range of roles, to provide wider perspectives on the marketing mix elements in security contexts. In the first stage the authors contacted key informants from various firms located in Ho Chi Minh City, Vietnam to nominate employees who may be suitable for the study. The authors then checked if participants were willing to be interviewed. Thirty participants from eight firms participated in semi-structured interviews (Table I). Interview questions were open-ended, enabling the researchers to discover, comprehend, and get the insights of the participants (Denzin and Lincoln, 2018). Throughout the interview process, researchers tried to be a discussion partner, who only listened and helped participants to make their reflections clearer (Marshall and Rossman, 2014). The interviews were conducted in both English and Vietnamese (dependent on the language background of the participant),

Organization	No. of participants	Position	Pseudonyms
Software retailer	3	Software designer	Hung, Huong, Ha
Financial firm 1	4	Auditors	Lan, Linh, Luong, Lang
Financial firm 2	4	Financial specialist	Dung, Dang, Dinh, Dong
Financial firm 3	1	Marketing staff	Phuoc
	1	Compliance officer	Phung
	4	Financial specialist	Phuong, Phuc, Phu, Phi
Financial firm 4	3	Financial specialist	Tuong, Ta, Toan
	1	Market researcher	Tu
Agriculture exporting firm	1	Investor relation associate	Tinh
University	2	Lecturer	John, Jason
	2	Professional staff	Bao, Binh
Marketing firm	2	Advertising designer	Cao, Canh
	2	Marketing staff	Cuong, Cu

Table I.
Participant profile

recorded, transcribed, and translated. Any potentially identifying details were removed prior to analysis.

Before conducting interviews, interview questions based on the 7Ps mix had been developed. For examples, to explore the *Price* factor, the question was asked: "To what extent does completing cybersecurity activities affect your main tasks? Would you be willing to skip security steps to finish your main tasks?" To explore the mix of People, authors asked: "What are your expectations from the IT teams (abilities, skills, enthusiasm and engagement)? How about the department atmosphere?". To clearly demonstrate how each "P" in the 7Ps framework can be employed in security contexts, a definition of each P – product, price, promotion, place, physical evidence, processes, and people – was clearly explained to the participants. Open questioning about the issues allowed for the potential to include things that did not fit into the 7Ps framework. Furthermore, due to the inherent complexity and opacity of some security concepts, participants were shown a set of photos depicting each of the 7Ps, such as signs and symbols of virus warnings, security slogans at work, or photos of teamwork (to depict workplace atmosphere). These photos helped to reduce the ambiguity of the interview questions and more clearly elicit the participants' experience and thoughts towards cybersecurity issues at work.

The data collected from interviews was open coded into the pre-defined 7Ps themes by keywords, phrases and their intended meanings (Saunders *et al.*, 2012). Such coding also established any significant interactions among the 7Ps elements. Inter-rater reliability was achieved through the consensus review among three IT experts in the results of coding and classifications. The entire data transcribing, coding and classifications were performed with the help of text analysis software NVivo 11.

Findings

Product as cybersecurity compliance

Proper cybersecurity behavior, as an important organizational "product", was acknowledged by this study's participants as a means to protect their work, safely share information within the organization and in general, and to make them feel confident about safely performing their job. Despite a relatively high awareness of cybersecurity, there was a considerable gap between users' descriptions of what is necessary and their reported behaviors. Many participants also had varying perceptions of cybersecurity needs from.

One participant explained security compliance should be considered as a must-do task that requires little acceptance from the employees:

> [. . .] when an employee goes to work, he works for the company, so if he has personal computing needs, he should use his personal computer at home. IT Security teams do not necessarily have to balance between work and personal needs, instead they have to prioritize security tasks. Staff have to follow. (Lang, financial analyst, financial firm 1)

Another participant looked at security compliance as bureaucratic and time-wasting tasks, with little benefit to users:

> I see that security compliance is only that you have to comply with the organization's requirements. However, I don't understand why I need to do that. It's very much bureaucratic and time-wasting exercise. (Jason, lecturer, university)

A few participants cited barriers to performance coming from internal factors, such as: the nature of their jobs, relative levels of knowledge, and lack of technical skills or personal experience. External factors included the complexity of security processes and the lack of availability of support infrastructure. Hence, while each participant recognized the "product" of cybersecurity, it is pertinent that not all wanted to "buy" it. Many offered excuses as to why the product was not for them:

> We don't have an IT background and most of us will just follow the required security processes without thinking much about it. For example, when we login to a program, we need an ID and password. That is all we do. Most of us don't think about if we click on a URL link, what may happen and how it may affect Internet security. That is a little too much for us. (Dang, financial specialist, financial firm 2)

Participants also raised the issue that security behavior should also apply to people who monitor security, indicating their concern about internal security risks where IT staff could have high levels of access to employee data:

> I am more concerned with internal security risks than external ones. Information systems can be protected from outsiders, but I don't know what IT staff can do to users' data, as they can access it at any time. (Dung, financial specialist, financial firm 2)

Organizations may impose clear expectations of security compliance from the employees; however, we found that participants put forward their different views of what proper behavior should be expected from users and the organization. A wide range of other elements – participants' work background, IT knowledge, and the organizations' security environment – can all contribute to diverse interpretations of security behavior (the product) from the participants. These other elements are further explored in other the Ps in the 7Ps framework in the following sections.

Price of exercising security measures

Many participants agreed that compliance with information security systems is time-consuming and something that decreases their work effectiveness and productivity. The price of cybersecurity was considered as the time employees have to spend time on training programs and day-to-day security tasks, such as scanning for viruses and reading repeated notifications. If participants are unfamiliar with the cybersecurity tasks, they might take significantly greater amounts of time and effort to complete them, thereby shifting the burden of associated compliance costs to those least likely to be able to "afford" them:

> Security tasks are time consuming. Some require just a couple of minutes while others virtually take forever. For example, password changes can not include the previously used ones and if I

> forget to change the password after the expiration date, I would be unable to log in the computer hence requiring IT staff to unlock the account. (Phi, financial specialist, financial firm 3)

Some participants also complained that restricted security access controls negatively affected their work performance. A group of staff at a bank argued that blocking access to social networks and e-commerce sites could reduce their productivity, as they felt more productive when being able to balance work and life at work. A marketing staff member found that she could not open the sites needed for her creative work and had to use another site that was not as useful. Hence, she had to resort to a personal laptop to get the information she needed to do her work.

> IT usually blocks and restricts all the needed websites which has a negative effect on my work performance. Therefore, I often use my personal laptop then connect to the public internet to download the needed information because I cannot continue my work without that information. (Phuoc, marketing staff, financial firm 3)

Costs to users can also be in the form of disciplinary actions for non-compliance such as formal warnings or job dismissals. Participants from the financial firms supported such strict deterrent measures, while others from non-financial firms thought they were impractical and could not be enforced. One participant who explained the potential effectiveness of organizational punishment suggested that it depended on whether the policy was clearly communicated to employees to make people aware of the position that the organization takes on cybersecurity:

> For short term, I think there should be a clear punishment policy for non-compliance. I think, without it, staff will ignore the policy completely. Gradually, employees will become more aware of doing the right things in cybersecurity. (Dong, financial specialist, financial firm 2)

It is clear that balancing a secure environment with work productivity remains a challenge for organizations. There is inherent risk in using an unsecure environment to be able to maintain productivity levels. If people see the cybersecurity product as secondary to their roles and responsibilities and not a primary activity, they will find another way to achieve their targets. These workarounds may mean that employees pay insufficient attention to the potential risks generated by the unsecured methods. If the price of effort and time spent on protecting information is higher than the benefits of secure information, then compliance will be at risk.

Promotion and security behavior

All interviewed organizations customarily used traditional non-personal communication promotions, including emails and formal training sessions, for disseminating security policies and expected behavior. However, according to many participants, this traditional policy-led communication was not an effective way to continuously drive behavioral change. This is because, at the training sessions, the ideas discussed were often too abstract and therefore forgotten by the time users needed to employ safe security practices. In other words, the knowledge was provided at the wrong time and was not specifically useful. Effective promotion should allow users to engage with security requirements at the right time and in the right place, as most participants only undertook recommended security measures if such measures directly influenced their job (i.e. if they did not need to engage with the policy to do their job, they didn't engage with it at all). As one participant explained:

> We only read policy because it related to our work and we know that we will have to face that problem and therefore need to know what to do to solve it. (Phu, financial specialist, financial firm 3)

All participants stated that the written policies – promotions – should be short and simple and should deliver clear guidance. The main reasons participants skipped reading policy documents were due to the complexity of information, the use of jargon, and the seemingly huge amount of technical knowledge required to understand it. These findings are consistent with Brennan *et al.*,'s (2015) recommendation that policy should have a clear statement, which is transparent and articulated in terms that the individual can engage with. Another participant agreed:

> The policy documents should provide clear guidance about what is right and wrong to allow all employees to follow it exactly and prevent them from making mistakes. (Tu, Market researcher, financial firm 4)

In terms of promotional formats, most participants favored more creative and visual representations of the policy that relate to specific information security risks and actions required by users, which were more likely to be viewed by the employees. Instead of forcing people to read the whole document with a lot of complex instructions, visual displays with eye-catching symbols and signs enabled employees to better comprehend and remember the key messages that organizations want to deliver. Furthermore, well-designed symbols and signs of security risks around office areas can also better gain the attention of employees:

> I think most people will not read written policies unless it is done with graphic information, which makes it more interesting and simpler to comprehend. (Bao, professional staff, university)

One participant provided an example of a creative promotional campaign about cinema etiquette at a cinema, which was consistent with this idea:

> I think it is a very good example that when you go to the cinema, the rules of movie watching etiquette are shown through short fun video clips [before the movie], which is very entertaining and even a child can remember that. Therefore, educational cartoon videos which can be sent through staff emails or shown on LCD displays around working areas can be useful to get people's attention. On my work computer's standby screen, it shows a beautiful photo depicting our company values, which is very efficient on helping us to remember the message. (Lan, auditor, financial firm 1)

Using fun and awareness-raising games is another promotional option to create enthusiasm and interest towards information security issues. A few participants suggested interesting and interactive games to attract their attention, raise awareness and motivate them to change behavior. This is consistent with suggestions by Hastings *et al.* (2004) that games are a more sustainable approach than the use of fear-based communications of risks.

> I think employing games with prizes will motivate and engage employees more. By playing games, employees can more easily read and understand the policies. (Dang, financial specialist, financial firm 2)

Another factor to consider under the category of promotion is the frequency of communication. Some participants noted that they would ignore messages if they were communicated too frequently. For example, some of the participants specifically stated that they normally ignored daily IT update emails since they do not create any urgency to review their contents. Most participants raised concerns that multiple exposures to security warnings could increase awareness, but too many messages too often may counter the effects by adding unnecessary pressure, increasing boredom, negativity towards the organization's cybersecurity measures.

Finding a balance of sufficient, but not overloading, amounts of promotion poses a challenge to organizations. Determining the amount of security communication can benefit

from the findings of Schmidt and Eisend (2015), which found an inverted U-shaped curve as the net effect of the positive and negative effects of repetition on advertisement exposure. Positive affect refers to audience's favorable response to the advertisement, while negative affect reflects their unfavorable attitude and disregard of the content. Schmidt and Eisend also recommended that the maximum positive attitude is reached at approximately ten exposures, and negative response is recorded if there are any further exposures.

Place and security behavior

Some of the participants explained that they take different security precautions depending on which devices or locations they use, and that access to support varied substantially between locations and devices (place). Participants took different security precautions when using the internet at work compared to what they did at home. At work, participants generally felt the IT systems were well-protected and IT staff should be able to deal with it quickly and effectively if anything went wrong. Consequently, they did not worry too much about taking security precautions while at work. However, when using their own computer devices at home, many stated that they would carefully check for viruses or malicious links, or even back up their information regularly:

> If I use my computer in public places or at home where I feel like my computer might get infected with a virus or people may hack my information, I would be more cautious. But if I am at work, I leave the problems for the IT department to solve. Partly because I trust the organization to take care of it. (Jason, lecturer, university)

Most participants reported the 'place' of security (non) compliance behavior occurred mainly through digital channels, including accessing emails and websites, and downloading software. Although online channels were identified by those participants as high-risk, the level of skepticism varied. For example, while the majority of participants were well aware of the security risks with opening email attachments and links, the risks associated with social media use were often not clearly understood or even covered in organizations' policies. Most participants from the financial organizations reported the use of several social media applications such as *Skype* and *Zalo* (a texting software commonly used in Vietnam) as an unofficial group information sharing channel. Some of these social professional groups comprised more than fifty people, from both inside and outside an organization. They often shared market information, investment advice, and other related information through these applications. Participants reported that the applications are popular because they facilitate group discussion well, they have interactive content, and they assist to build a community:

> Most people in my company use and check notifications on the mobile Zalo application, therefore, it is easier to get their responses by using this application than through formal emails. (Lan, auditor, financial firm 1)

> I use Skype daily in sharing and updating inquiries and trading information. It is very useful, convenient because every staff can join and discuss about the problem easily. (Dinh, finance specialist, financial firm 1)

However, we found that the participants from financial organizations did not consider the online security risks of using social media for information sharing. Furthermore, they were not aware of consequences that may occur from disclosing financial information on potentially open and unsecure channels, which may end up with people outside the organization. Furthermore, they did not consider the location of either themselves or the device to be pertinent to ensuring security.

Another aspect of computer usage that relates to place is in the use of personal or company-owned mobile devices such as tablets and smartphones when accessing corporate information from home or at work. According to Kaspersky Internet Security, data leakage due to unauthorized and unsecure mobile applications, accessing unsecured Wi-Fi sources, and network spoofing through fake access points, are the three most common mobile security threats to corporate networks (Kaspersky, 2018). However, very few participants were aware neither of the security threats from using unsecure mobile devices nor if the organizations provided guidance for their proper use.

Physical evidence of security measures

IT support and security staff and artifacts were mentioned consistently as a key factor for security behavior:

> At my company, IT communication with the staff is not very good. Maybe nobody cares about security, or possibly somebody does care but they don't know where to find the information when they need it. (Binh, university, professional staff)

This quote is indicative of the connected nature of the 7Ps – promotion (communication with staff), processes (capacity to search for information), people (no one cares), physical evidence (manuals and guides) and place (e.g. accessibility of information) all encompassed within the complaint.

Very few participants identified that physical office design could promote or hinder appropriate security behaviors. Functional design of the work place can affect people's view of the organization and whether or not there is organization-wide concern about security risks. Security concerns can magnify in modern open-plan offices. Open-plan offices allow employees to share ideas and improve team performance, but the safety of information assets can be affected; for example, if people leave computers open while undertaking tasks away from their desk or sharing hot desk passwords. In such offices, because people can easily see others' computer screens, private information (such as passwords) can be stolen. As one university lecturer mentioned, more traditional cubical offices seemed more private and secure for protecting information:

> I prefer to work in the open office with a private cubical design because I feel more private. In my office, everything is shared, and I don't have any privacy even when I want to login to my personal emails. For example, I have two other colleagues, one is beside me, and one is behind me, they can see everything on computer screen easily. In many cases you don't have much privacy. (John, lecturer, university)

Physical evidence such as office design plays an important role in developing and maintaining security awareness, which may positively impact on employees' attitudes on perceiving and evaluating cyber-threats and its consequences (Kokolakis, 2017; Sommestad *et al.*, 2015).

Process of implementing security measures

The participants offered mixed responses towards their organization's cybersecurity processes, from simple and straightforward to confusing and unclear, which led to various impacts on productivity and workflows:

> Security tasks are simple and straightforward with the help from IT and automated security settings. My only concern is that it is time-consuming performing these security tasks (Cuong, marketing assistant, marketing firm)

Most participants wanted to reduce the burden of configuring appropriate security settings for their devices:

> Personally, I think the IT department should set the desired security settings for all the tasks that we execute. As a result, it will save us time from configuring them ourselves and reducing user errors. (Dong, financial specialist, financial firm 2)

However, standardized security settings normally restrict many rights that users can have with their computers including the ability to install new software and customize settings. Hence, some of the participants complained about what they believed to be unreasonable restrictions on their computer use:

> I feel annoyed when I have to ask IT staff to come and authorize me to fix and install any software. I think it needs to have room for the users to do it by themselves. There is only limited software you can install by yourself. (Jason, lecturer, university)

A few participants stressed that if organizations viewed managing the processes and sub-processes associated with cybersecurity as a *shared* responsibility between organization and employees, employees needed to be empowered and enabled in solving certain problems themselves. That is, 'don't ask me to fix IT problems, if you won't even let me install my own software':

> Organizations need to consider user control levels to balance security restrictions and work productivity. If IT systems need to be secure at the cost of restricting users' permissions, then the users should still have some discretion in that process. If they find out that they don't have any options, the users will try to bypass security measures [e.g. to find a way to bypass blocked or restricted websites]. (John, lecturer, university)

To support users' active participation in security processes, companies could provide online training, handbooks, IT support, online systems, and virtual helpdesks, to help competent users navigate cybersecurity processes by themselves:

> For a company I worked at previously, [the cybersecurity processes] was very clear. From one online self-help portal, whenever we want to find out whether a policy exists or not, we can easily search for it. At my current company I don't know who to ask so I would ignore security risks even if I find them dangerous. (Jason, lecturer, university)

People in cybersecurity

Most participants agreed that timely and effective IT support from well trained personnel was required to reduce the impact of IT security systems on employees' work, by ensuring compliance time and effort were minimal. Effective IT support processes should provide a responsive and effective personal help desk to reduce work interruption, offset the effects of decreased productivity, and increase employee satisfaction (Salanova *et al.*, 2013). The pace of compliance behavior depends heavily on how the employees react to the people aspects of the ISM marketing mix:

> Our IT staff's competence is very important. They should be friendly, listening, and willing to help, and give advice beyond what people ask. Sometimes I have limited knowledge in IT or security even when I ask them, I'm not sure if it's right or not. IT staff should explain why I should do some tasks, not just what to do. (Jason, lecturer, university)

IT personnel are ideally equipped with technical skills, enthusiasm, and engagement skills. They can play an important role in the success of cybersecurity, since it enhances the engagement of other employees in technology activities. However, some participants stated

that IT staff did not fully address the IT needs of employees, which might lead to weaker support and control of the information security throughout all levels of organizations. Some of these participants recommended that IT staff should more actively focus on helping people:

> I will take IT advice if the IT people demonstrate competence and show that they are capable of managing the security risks. They have to demonstrate that they can do something to protect my computer first. (Canh, advertising designer, marketing firm)

Most participants highly regarded the roles of a colleague, either a supervisor or peer, who possessed expert domain knowledge and technology competence in promoting security behavior. This so-called "departmental champion" could provide instant and work-related advice that a traditional (usually virtual) IT support channel cannot. The champion could provide better advice than IT staff for employees' security needs, based on their thorough understanding of the job requirements:

> I think each team should have a designated champion so that we can come to them at times when the IT helpdesk people are busy. The champion also has work-related knowledge, so he or she can understand the implications of security compliance when performing certain tasks. (Luong, auditor, financial firm 1)

Citing the specific nature of each department's security requirements and also building trust between colleagues in the same department, having a departmental security champion was praised as enabling better compliance:

> Because each department has a different policy – for example the finance department cares more about personal trading policy than the marketing department – having a champion who has experience and knowledge about cybersecurity in the department is good idea. They know what problems we usually deal with during work and we can trust them to ask." (Phung, compliance officer, financial firm 3)

Finally, having the required security knowledge and skills is critical for employees to develop and maintain security compliance and effectively use existing organizational security resources (Pham *et al.*, 2016b; Rhee *et al.*, 2009). Users' lacking knowledge and skills can be a major threat to security programs (Posey *et al.*, 2014). A few participants admitted that they did not know what skills they were lacking until they were asked to do complex security tasks, such as verifying potential spoofing attacks in emails, or blocking malicious websites. Some participants argued that security knowledge for regular end-users should be easy to understand and apply, whereas acquiring more advanced security skills should be for IT professionals only:

> I like simple tasks and simple instructions such as a short security slogan – clearly indicating what I should do. Give me the control how I should do the security tasks. (John, lecturer, university)

Conversely, many participants appeared to not recognize the importance of acquiring knowledge, to better protect the organization's information and believed that the task should be the responsibility of the IT department:

> We hardly update our security knowledge. This task is for IT professionals and it is not one of our concerns. (Dong, financial specialist, financial firm 2)

It is clear that participants like John and Dong have quite different views on the need to acquire security skills and knowledge and may pose a challenge to any organization to effectively educate their employees. As discussed in the Process element, automated and universal security settings restrict users' computer permissions to make any changes by

themselves, including restricting external resources can be accessed. Hence users may have little chance to apply their new skills, which may result in them lacking any motivation to update their security knowledge.

Overall, the People element of the 7Ps is essential in facilitating safe security practice. From competent IT professionals, departmental champions, who clearly understand cybersecurity practice, to lesser-experienced employees, who need assistance in acquiring relevant security knowledge, can all be parts of the behavioral infrastructure. Those stakeholders should interact and complement each other in a quest for better cybersecurity environment. It is a challenge to convince users that protecting security is everyone's business, not just for IT professionals. Summary of the key findings is shown in Table II.

Marketing concept	IMS definition	Findings
Product	The desired behavior change or a shift in attitude. (e.g. not engaging in risky activities)	The product is the idea that users have to comply with security policies and procedures to create a safe and secure cyber environment for all. (e.g. cybersecurity is the idea being "sold" to users)
Price	The costs and benefits tradeoff associated with the required behavior	In cyber security, the price is the time and effort required by the user in implementing cybersecurity. (e.g. work productivity and performance can be depleted when security tasks are onerous)
Promotion	The use of communication tools and techniques to foster positive social behaviors	Promotion in cyber security is currently largely ineffective because it is not targeted towards the needs and wants of the target users. (e.g. policies and procedures are not easy to engage with; assistance is not easily accessed; not delivered in a timely manner; promotion is too distant from cybersecurity events to be helpful)
Place	A channel of distribution or the necessity of the message reaching the audience in the right place at the right time	Place is where and when people used virtual and physical resources to address cyber security issues. Users were more likely to behave securely at home than at work because the workplace "should" be protected by the organization. Social media is widely used for (unsecure) information sharing. Mobile security is a risk
Physical Evidence	The visible elements of a service delivery system (e.g. the physical aspects of the work environment), the 'front stage' of service delivery	Physical evidence was connected as a support for the other Ps in the marketing mix. (e.g. signs and the presence of IT staff as an indication that there is a security system active and in place)
Process	The methods that create services and deliver benefits and value to 'customers' (e.g. users). Processes are 'backstage' activities that ensure a service is delivered	Users largely did not see cyber security processes as being relevant to their work. They felt that IT should set security tasks to be invisible if possible, so as to lower the impact on workflows. However, users also wanted active participation in solving workplace problems that arise as a result of cyber security concerns
People	The management of human interactions within the system	Users wanted to see people at the core of IT security activities. Local champions who were not IT specialist staff were also an asset to the delivery of cybersecurity. There was a divergence of participants' views about the role of users in resolving security issues: some saying that the organization 'should' take care of everything and others saying that they would like to be involved

Table II. Summary of study findings

Discussions

By using ISM techniques, managers can develop a shared commitment between employees and organizations towards desired behaviors, through the co-creation of shared visions and values (Brennan *et al.*, 2015). Bansal (2003) emphasized the importance of aligning organizations' and employees' objectives as an essential element for successful behavioral changes. Inherent in successful alignment activities are considerations of perceived co-created costs and benefits (value propositions) for both organization and employee (Brennan *et al.*, 2015). Employees' recognition of their roles in security compliance brings positive impacts on the organization's compliance climate (Herath and Rao, 2009). Moreover, this may lead to employees' enhanced self-motivation, which is an important factor of the employees' willingness to follow security compliance requirements for their organizations (Safa and Von Solms, 2016).

A key contribution of the 7Ps framework is to provide a comprehensive tool for organizations to cover critical aspects in the whole process of initiating and maintaining security behavior. Our results indicate that there is disagreement between organizational ideas of what constitutes a safe and secure environment and users' perspectives. Thus, what is or is not a *Product* for the purposes of ISM in cybersecurity compliance is contested. Whether or not agreement can be reached, and therefore campaigns created to 'sell' the product, is as yet unknown.

It is clear that there are both costs and benefits for users participating in cybersecurity activities. Hence, the concept of *Price* is established as being a useful one for ISM campaigns involving cybersecurity. Users easily voiced that costs are time and effort, as well as loss of productivity. But other potentially more extreme costs to the organization are not well articulated by and indeed are probably unknown to users. This represents another opportunity to explore whether users can be engaged in cybersecurity issues sufficiently to become motivated to act, either by learning more about managing cybersecurity.

The *Promotion* element affirms the importance of Security Education, Training and Awareness programs (SETA) with better communicating methods (Willison *et al.*, 2018). More creative promotion such as the use of visual and interactive content, and potentially using social media on both PC and mobile platforms could be used to reinforce policy requirements. The impact of short and regular communications over that of annual SETA training effectiveness has been highlighted in Barlow *et al.* (2018), who studied how various types of short communications influenced policy violations. Another strategy to engage users is to make communication accessible and enjoyable (or at least palatable). Hence, gamifying security training could engage and interest users through more authentic and collaborative activities, which may in turn lead to better learning outcomes (Burke, 2016). This might also build on the social (people) aspects of compliance.

Managing the *Place* elements of security behavior can help security practitioners to consider different usage contexts that users can be exposed to security risks and develop necessary counter measures and awareness training. Further, compliance behavior often takes place in an uncontrolled environment and ensuring that support is available when and where it is needed, as well as in the form that is most useful at the time, was found to be a critical element in enhancing a cybersecurity system.

The *Physical evidence* of security measures reminds users of the reality of cyber-attacks and their consequences. It does so without the need for personal experience and risk taking. Many participants underestimated the impacts of cyber-attacks, as they thought such attacks did not relate to their jobs and might never happen to them. Understanding the difference between front (visible) and backstage (invisible) elements can be helpful in developing interventions that are user friendly (or merely invisible) and where the user has

the 'script' to enable them to participate in securing the environment. IT staff visibility, solutions readily visible, available and accessible, as well as physical in nature (so that people are not lost in the ether while they try to resolve an issue): all these physical factors can assist in co-creating cybersecurity.

Strongly linked to physical evidence are the *Process* elements of the ISM marketing mix. Processes can be invisible and therefore the user does not participate in the solution to the security issue. Processes can also be both a barrier and a facilitator to effective cybersecurity. If processes are too complicated and the user is not motivated or able to improve their knowledge to comply, then security will be at risk. Additionally, if processes are too simple, security may also be seen as ineffective. Co-creation of processes is one way of ensuring the balance between organizational and user needs.

Finally, the *People* element emphasizes that key stakeholders including managers, IT staff, peers and users need to view and exercise security practice with a good understanding of each other's perspectives. For an example, organizations can try to improve self-efficacy of employees to enhance their confidence and motivation to comply (Rhee *et al.*, 2009), but they also need to have a chance to use those skills or they may get bored and find something new to do that may damage the security of the environment (Johnston *et al.*, 2019).

Potential for future research

ISM as a mechanism for decreasing cyber security risks has yet to be explored in any depth. Due to the small sample size of the study and the hypothetical scenarios used to elicit opinions and perceptions from participants, the study's key findings need to be further explored with more employees, and in organizations where an ISM marketing campaign has recently been implemented. Particular elements in the 7Ps framework – namely promotion, place and physical evidence – need to be examined more thoroughly, particularly given that most participants requested changes in the ways security processes are communicated to employees (i.e. methods and frequencies), together with timely advice of proper security practices on social media through mobile devices. Future research could look at which forms of promotion would be most effective for different types of security communication including policy updates, security incidents, and skill training. Studies might also examine how employees' security practice varies across "place", such as when employees use various technology devices and platforms. Since cloud-based computing is more popular, unsafe use in one device can still affect the whole organizational system. More research is required to explore how organizations view and measure the costs and benefits of ISM initiatives for cybersecurity campaigns.

This qualitative research could be extended a number of ways. Researchers could undertake co-creation of a social marketing solution within an organizational context to ascertain the most effective mechanisms for a specific setting. Additionally, given the synergistic nature of marketing, quantitative studies into the effectiveness of specific strategies and combinations of elements would be useful in informing program design. Further, the impact of new technologies for communication and education such as games, animation and virtual reality has yet to be explored and it is well known in other social marketing contexts that gamification has significant effects on engagement and subsequent behaviors, especially when it comes to negative messaging spaces. Finally, the use of unsecure mobile and social environments remains problematic for ensuring cybersecurity. More research is required into how best to develop strategies that permit 'daily life' while ensuring a safe environment.

Conclusion

To date, most studies on security compliance have focused on identifying initiating factors of the expected behavior, and lack focus on understanding organizational factors enabling it. Despite being aware of the importance of safe cybersecurity practices, there is a significant gap between the attitudes and behaviors among employees (Cox, 2012). Such gaps have resulted from either internal factors, such as the level of user knowledge, technical skills or personal experience (Cox, 2012; Sommestad *et al.*, 2014), or external factors, such as organizational culture (Van Niekerk and Von Solms, 2010) and complexity of the security process (Pham *et al.*, 2016b). For individuals to behave in a maintainable manner, barriers to the intended behavior must be removed from the environment, and there must be a system that empowers people to behave in the expected way (Brennan *et al.*, 2015). Successful behavior change requires people be not only motivated and capable of initiating a change in their behavior, but also able to sustain that change over time (i.e. to be self-motivated to undertake the behavior).

Using the 7Ps framework from ISM, this study identified that expected security behavior can be affected by a range of factors, including internal and external communication, costs of complying (in terms of time and cognitive load), contexts and locations of use (places), physical artifacts of supporting environments, streamlined security process, and people elements, including IT staff, supervisors and peers. Any of these factors can motivate and engage people to overcome tangible and intangible barriers and adopt required cybersecurity behavior. The study also demonstrates clear evidence of the importance of considering the interaction between 7Ps' elements within the ISM system. Any element removed from the behavioral infrastructure or not done properly can negatively affect security behavior. For example, processes, people and product interact to create behavior. Increasing knowledge may counteract perceptions of complexity, but simpler processes might counteract the need for more knowledge. This also suggests people can be overwhelmed by efforts to educate them about the behavior. Thus, the dual barriers of knowledge and technical skills are magnified in circumstances where a user-supportive (customer-centric) infrastructure is not established for a cybersecurity system.

References

Anitsal, I., Girard, T. and Anitsal, M.M. (2012), "An application of services marketing mix framework: how do retailers communicate information on their sales receipts?", *Business Studies Journal*, Vol. 4 No. 2, pp. 77-90.

Bada, M., Sasse, A. and Nurse, J.R.C. (2015), "Cyber security awareness campaigns: why do they fail to change behaviour?", *International Conference on Cyber Security for Sustainable Society*, The Sustainable Society Network, Coventry.

Bansal, P. (2003), "From issues to actions: the importance of individual concerns and organizational values in responding to natural environmental issues", *Organization Science* , Vol. 14 No. 5, pp. 510-527.

Bardhan, I.R., Demirkan, H., Kannan, P., Kauffman, R.J. and Sougstad, R. (2010), "An interdisciplinary perspective on IT services management and service science", *Journal of Management Information Systems*, Vol. 26 No. 4, pp. 13-64.

Barlow, J.B., Warkentin, M., Ormond, D. and Dennis, A.R. (2018), "Don't even think about IT! the effects of anti neutralization, informational, and normative communication on information security compliance", *Journal of the Association for Information Systems*, Vol. 19 No. 8, pp. 689-715.

Barton, K.A., Tejay, G., Lane, M. and Terrell, S. (2016), "Information system security commitment: a study of external influences on senior management", *Computers and Security*, Vol. 59, pp. 9-25.

Bate, S. and Cannon, M. (2011), "A social marketing approach to building a behavioral intervention for congenital cytomegalovirus", *Health Promotion Practice*, Vol. 12 No. 3, pp. 349-360.

Belk, R.W. (2007), *Handbook of Qualitative Research Methods in Marketing*, Edward Elgar Publishing Limited, Cheltenham.

Binney, W., Hall, J. and Oppenheim, P. (2006), "The nature and influence of motivation within the moa framework: implications for social marketing", *International Journal of Nonprofit and Voluntary Sector Marketing*, Vol. 11 No. 4, pp. 289-301.

Bitner, M. (1992), "Servicescapes: the impact of physical surroundings on customers and employees", *Journal of Marketing*, Vol. 56 No. 2, pp. 57-71.

Booms, B. and Bitner, M.J. (1981), "Marketing strategies and organizational structures for service firms", in Donnelly, J.H. and George, W.R. (Eds). *Marketing of Services*, American Marketing Association, Chicago, pp. 47-51.

Borden, N.H. (1964), "The concept of the marketing mix", *Journal of Advertising Research*, Vol. 4 No. 2, pp. 2-7.

Brennan, L., Binney, W. and Hall, J. (2015), "Internal social marketing, servicescapes and sustainability: a behavioural infrastructure approach", in Wymer, W. (Ed.), *Innovations in Social Marketing and Public Health Communication*, Springer, New York, NY, pp. 87-105.

Brennan, L., Binney, W., Parker, L. and Nguyen, D., A., T. (2014), "Theories and their uses in social marketing", in *Social Marketing and Behaviour Change: Models, Theory and Applications*, Glos GL50 2JA, Edward Elgar Publishing, Cheltenham, pp. 7-14.

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*, Vol. 34 No. 3, pp. 523-548.

Burke, B. (2016), *Gamify: How Gamification Motivates People to Do Extraordinary Things*, Wharton Digital Press, Routledge.

Christmas, S., Young, D., Skates, A., Millward, L., Duman, M. and Dawe, I. (2009), "*Nine Big Questions about Behaviour Change*", Department for Transport, London pp. 87-105.

Coventry, L. Briggs, P. Blythe, J. and Tran, M. (2014), "Using behavioural insights to improve the public's use of cyber security best practices", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf

Cox, J. (2012), "Information systems user security: a structured model of the knowing–doing gap", *Computers in Human Behavior*, Vol. 28 No. 5, pp. 1849-1858.

Denzin, N.K. and Lincoln, Y.S. (2018), *The Sage Handbook of Qualitative Research*, 5th ed., Sage, Los Angeles.

Fischer, D., Stanszus, L., Geiger, S., Grossman, P. and Schrader, U. (2017), "Mindfulness and sustainable consumption: a systematic literature review of research approaches and findings", *Journal of Cleaner Production* , Vol. 162, pp. 544-558.

Furnell, S. and Rajendran, A. (2012), "Understanding the influences on information security behaviour", *Computer Fraud and Security*, Vol. 2012 No. 3, pp. 12-15.

Gordon, R. (2013), "Unlocking the potential of upstream social marketing", *European Journal of Marketing*, Vol. 47 No. 9, pp. 1525-1547.

Grönroos, C. (1984), "A service quality model and its marketing implications", *European Journal of Marketing*, Vol. 18 No. 4, pp. 36-44.

Grönroos, C. (2004), "The relationship marketing process: communication, interaction, dialogue, value", *Journal of Business and Industrial Marketing*, Vol. 19 No. 2, pp. 99-113.

Hastings, G., Stead, M. and Webb, J. (2004), "Fear appeals in social marketing: strategic and ethical reasons for concern", *Psychology and Marketing* , Vol. 21 No. 11, pp. 961-986.

Herath, T. and Rao, H.R. (2009), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Hopwood, T. and Merritt, R. (2011), "*Big Pocket Guide to Using Social Marketing for Behaviour Change*", Centre, N.S.M. (Ed.).

Ismail, N. (2018), "10 Cyber security trends to look out for in 2019", available at:, www.information-age.com/10-cyber-security-trends-look-2019-123463680 (accessed 20 January 2019).

Ivy, J. (2008), "A new higher education marketing mix: the 7ps for MBA marketing", *International Journal of Educational Management*, Vol. 22 No. 4, pp. 288-299.

Johnston, T.M., Brezina, T. and Crank, B.R. (2019), "Agency, self-efficacy, and desistance from crime: an application of social cognitive theory", *Journal of Developmental and Life-Course Criminology*, Vol. 5 No. 1, pp. 60-85.

Kaspersky (2018), "Top 7 mobile security threats: smart phones, tablets, and mobile internet devices – what the future has in store", available at: www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store (accessed 22 November 2018).

Kokolakis, S. (2017), "Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon", *Computers and Security*, Vol. 64, pp. 122-134.

Liljander, V., Gillberg, F., Gummerus, J. and Van Riel, A. (2006), "Technology readiness and the evaluation and adoption of self-service technologies", *Journal of Retailing and Consumer Services*, Vol. 13 No. 3, pp. 177-191.

Lockrey, S., Brennan, L., Verghese, K., Staples, W. and Binney, W. (2018), "Enabling employees and breaking down barriers to sustainability: internal social marketing and pro-environmental behaviour", *Research Handbook on Employee Pro-Environmental Behaviour*, Edward Elgar, Cheltenham.

McDermott, L., Stead, M. and Hastings, G. (2005), "What is and what is not social marketing: the challenge of reviewing the evidence", *Journal of Marketing Management*, Vol. 21 Nos 5/6, pp. 545-553.

Marshall, C. and Rossman, G.B. (2014), *Designing Qualitative Research*, Sage, Thousand Oaks, CA.

Mazlina, Z. and Rozilawati, R. (2016), "An empirical study of information security management success factors", *International Journal on Advanced Science*, Vol. 6 No. 6, pp. 904-913.

Pham, C.H., Brennan, L. and Furnell, S. (2019), "Information security burnout: identification of sources and mitigating factors from security demands and resources", *Journal of Information Security and Applications*, Vol. 46, pp. 96-107.

Pham, C.H., Brennan, L. and Nkhoma, M. (2016a), "Intrinsic motivators and security compliance: an internal social marketing approach", *ANZMAC: Marketing in a Post-Disciplinary Era*, University of Canterbury, pp. 872-879.

Pham, C.H., Dang-Pham, D., Brennan, L. and Richardson, J. (2017), "Information security and people: a conundrum for compliance", *Australasian Journal of Information System*, Vol. 21, pp. 1-16.

Pham, C.H., El-den, J. and Richardson, J. (2016b), "Stress-based security compliance model-an exploratory study", *Information and Computer Security*, Vol. 24 No. 4, pp. 326-347.

Posey, C., Roberts, T.L., Lowry, P.B. and Hightower, R.T. (2014), "Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders", *Information and Management*, Vol. 51 No. 5, pp. 551-567.

Previte, J. and Russell-Bennett, R. (2013), "The need for internal social marketing (ism): extending the people focus to service employees", in Hastings, G.and Domegan, C. (Eds). *Social Marketing: From Tunes to Symphonies*, Routledge, Milton Park, Abingdon, Oxon, pp. 326-334.

Rafiq, M. and Ahmed, P.K. (2000), "Advances in the internal marketing concept: definition, synthesis and extension", *Journal of Services Marketing*, Vol. 14 No. 6, pp. 449-462.

Raineri, N. and Paillé, P. (2016), "Linking corporate policy and supervisory support with environmental citizenship behaviors: the role of employee environmental beliefs and commitment", *Journal of Business Ethics*, Vol. 137 No. 1, pp. 129-148.

Rhee, H.S., Kim, C. and Ryu, Y.U. (2009), "Self-efficacy in information security: its influence on end users' information security practice behavior", *Computer and Security*, Vol. 28 No. 8, pp. 816-826.

Ruiz, J.F., Arjona, M., Maña, A. and Rudolph, C. (2017), "Security knowledge representation artifacts for creating secure it systems", *Computers and Security*, Vol. 64, pp. 69-91.

Russell-Bennett, R., Wood, M. and Previte, J. (2013), "Fresh ideas: services thinking for social marketing", *Journal of Social Marketing*, Vol. 3 No. 3, pp. 223-238.

Ryan, R.M. and Deci, E.L. (2000), "Self-determination theory and the facilitation of intrinsic motivation, social development, and Well-Being", *American Psychologist*, Vol. 55 No. 1, pp. 68-78.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015), "Information security conscious care behaviour formation in organizations", *Computers and Security*, Vol. 53, pp. 65-78.

Safa, N.S. and Von Solms, R. (2016), "An information security knowledge sharing model in organizations", *Computers in Human Behavior*, Vol. 57, pp. 442-451.

Salanova, M., Llorens, S. and Cifre, E. (2013), "The dark side of technologies: technostress among users of information and communication technologies", *International Journal of Psychology*, Vol. 48 No. 3, pp. 422-436.

Saunders, M., Lewis, P. and Thornhill, A. (2012), *Research Methods for Business Students*, 6th ed., Pearson Education.

Schmidt, S. and Eisend, M. (2015), "Advertising repetition: a meta-analysis on effective frequency in advertising", *Journal of Advertising*, Vol. 44 No. 4, pp. 415-428.

Shafiq, M., Zia-Ur-Rehman, D.M. and Rashid, M. (2013), "Impact of compensation, training and development and supervisory support on organizational commitment", *Compensation and Benefits Review*, Vol. 45 No. 5, pp. 278-285.

Smith, A.M. and O'Sullivan, T. (2012), "Environmentally responsible behaviour in the workplace: an internal social marketing approach", *Journal of Marketing Management*, Vol. 28 Nos 3/4, pp. 469-493.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: a systematic review of quantitative studies", *Information Management and Computer Security*, Vol. 22 No. 1, pp. 42-75.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015), "The sufficiency of the theory of planned behavior for explaining information security policy compliance", *Information and Computer Security*, Vol. 23 No. 2, pp. 200-217.

Spotswood, F., French, J., Tapp, A. and Stead, M. (2012), "Some reasonable but uncomfortable questions about social marketing", *Journal of Social Marketing*, Vol. 2 No. 3, pp. 163-175.

Stead, M., Gordon, R., Angus, K. and McDermott, L. (2007), "A systematic review of social marketing effectiveness", *Health Education*, Vol. 107 No. 2, pp. 126-191.

Thackeray, R., Neiger, B.L. and Hanson, C.L. (2007), "Developing a promotional strategy: important questions for social marketing", *Health Promotion Practice*, Vol. 8 No. 4, pp. 332-336.

Truong, V.D. (2012), "Social marketing: a systematic review of research 1998-2012", *Social Marketing Quarterly*, Vol. 20 No. 1, pp. 15-34.

Tsohou, A., Karyda, M. and Kokolakis, S. (2015), "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs", *Computers and Security*, Vol. 52, pp. 128-141.

van Doorn, J., Lemon, K.N., Mittal, V., Nass, S., Pick, D., Pirner, P. and Verhoef, P.C. (2010), "Customer engagement behavior: theoretical foundations and research directions", *Journal of Service Research*, Vol. 13 No. 3, pp. 253-266.

Van Niekerk, J.F. and Von Solms, R. (2010), "Information security culture: a management perspective", *Computers and Security*, Vol. 29 No. 4, pp. 476-486.

Warkentin, M., Shropshire, J. and Johnston, A. (2007), "The it security adoption conundrum: an initial step towards validation of applicable measures", *Proceedings of the 13th Americas Conference on Information Systems*, Keystone, CO.

Wasan, P.G. and Tripathi, G. (2014), "Revisiting social marketing mix: a socio-cultural perspective", *Journal of Services Research*, Vol. 14 No. 2, pp. 127-144.

Weinreich, N.K. (2006), "What is social marketing", *Weinreich Communications, 2018*, available at: www.researchgate.net/publication/240412155_What_is_Social_Marketing

Willison, R., Warkentin, M. and Johnston, A. (2018), "Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives", *Information Systems Journal*, Vol. 28 No. 2, pp. 266-293.

Zeithaml, V.A. (2000), "Service quality, profitability, and the economic worth of customers: what we know and what we need to learn", *Journal of the Academy of Marketing Science*, Vol. 28 No. 1, pp. 67-85.

Corresponding author
Hiep Pham can be contacted at: hiep.pham@rmit.edu.vn

Appendix

Source: Based on the social marketing primer from https://www.socialmarketingservice.com/

Figure A1. Steps to Develop Social Marketing Plan