House of Cards: developing KPIs for monitoring cybersecurity awareness (CSA)

Author List

Mohammad Mulayh. Alshammari
Department of Management and Information Systems,
College of Business Administration,,
University of Hail, Saudi Arabia
M.Mulayh@uoh.edu.sa

Dionysios S. Demetis
Centre for Systems Studies,
Hull University Business School,
United Kingdom
D.Demetis@hull.ac.uk

[1]

[1] This paper was presented at the Annual Security Conference, May 9-10, 2023, Las Vegas, NV. www.security-conference.org

House of Cards:
developing KPIs for monitoring cybersecurity awareness (CSA)

ACKNOWLEDGMENTS

The authors would like to take this opportunity to thank University X and all participants of this study.

Mohammad Mulayh. Alshammari is an Assistant Professor in the department of Management Information Systems at the University of Hail Business School in Saudi Arabia. He holds a PhD in cybersecurity and Information Systems Security from Hull University. His primary research interests are around cybersecurity awareness and culture and Information Systems Security.

Dionysios S. Demetis is an Associate Professor (Reader) of management systems at Hull University Business School, UK and a Visiting Professor at Texas A&M University, USA. He holds a PhD in anti-money laundering and information systems from the London School of Economics and his research concentrates around systems theory, anti-money laundering and cybersecurity. He is the author of two books, one on the philosophy of science and the intrinsic paradoxes of knowledge creation.

House of Cards:
developing KPIs for monitoring cybersecurity awareness (CSA)

Abstract

Non-malicious insider threats continue to pose a significant concern to an organisation's cybersecurity defence strategy, yet organisations still struggle to contain such insider threats. A critical pillar for doing so rests on the development and monitoring of Cybersecurity Awareness (CSA) programmes. CSA programmes need to be both prioritised and acknowledged as an important and crucial approach to the reduction of such threats. Although CSA programmes are developed on an ad-hoc basis by many organisations, the effectiveness of such programmes and how their entire lifecycle needs to be reviewed, monitored and managed needs to be further explored. In order to do so, this paper extracts a number of key performance indicators (KPIs) for monitoring CSA programmes. The paper relies on empirical data from an in-depth case study of University X in Saudi Arabia and sensitises the research approach by using Kirkpatrick's four level model as a theoretical scaffold. Through the combined use of Kirkpatrick's model that is recognised as a comprehensive model for evaluating the results of training and learning programmes and the empirical data from the case study, we offer a customised CSA-oriented model for managing cybersecurity awareness programmes, reflect on its associated KPIs, and consider broader information security management considerations.

Keywords: cybersecurity awareness, Kirkpatrick, information security, Key Performance inductors (KPI)

House of Cards:
developing KPIs for monitoring cybersecurity awareness (CSA)

INTRODUCTION

Over the last few decades, the non-technical approaches to cybersecurity have gained ground and they are widely recognised as important as the technical ones. A key part of non-technical approaches deals with user education and training. Cybersecurity awareness (CSA) has become an integral part to handling information systems security and a key dimension to reducing security incidents. Due to the daily use of technology for work purposes, users need to be educated about information security in an effective manner and made aware of their roles and responsibilities in protecting their organisations' systems. CSA is a significant driver to reducing cybersecurity incidents caused by end-users (Dhillon, 2007; Safa et al., 2016; Monzelo and Nunes, 2021). According to Furnell and Vasileiou (2017), the main causes of data breaches are malicious activities, system glitches and human errors.

In information security, end-users are considered to be a security risk (Parsons et al., 2014). A number of studies have found that end-users are responsible for the majority of security incidents (Chan et al., 2005; Pathari and Sonar, 2012). Users' lack of cybersecurity awareness (CSA) causes the majority of incidents (Okenyi and Owens, 2007); thus, information security is affected by end-user awareness (Galba et al., 2015), while in turn, end-users' cybersecurity performance is influenced by the level of their awareness of cybersecurity (Stanton et al., 2005). Although end-users are seen as a weakness (Balozian and Leidner, 2017; Rezgui and Marks, 2008), in the broader information system that needs to be protected, they also have an essential role in protecting information and preventing security incidents (Spears and Barki, 2010; Dhillon et al., 2016). The duality of this role places CSA in a critical place within the broader spectrum of information security.

The significance of cybersecurity awareness (CSA) has been recognised by Rhee et al. (2009) who find that knowledgeable end-users are more likely to comply with information security policies and best practices than others with less knowledge. However, this requires that end-users are regularly exposed to CSA. Thus, it is necessary to conduct CSA as an ongoing project, since multiple exposures (e.g. face-to-face training seminars, phishing simulations, mentoring, intranet-based training and e-learning, etc) have been recognised as an effective way to influence end-users' CSA (Foltz et al., 2005). Previous studies have found that CSA can have poor results for many reasons, including lack of management support, lack of investment, lack of alignment with business goals and lack of proper management (Morrison, 2018). A project-oriented and project-management outlook to conducting CSA is seen as a key component for ensuring its success (Hitachi, 2018). This leads to the need to manage the progress of CSA, review its ongoing development, and frame CSA management carefully by considering broader project-management considerations, as well as evaluation and learning dynamics.

One of the mechanisms with which this can be achieved is the introduction of Key Performance Indicators (KPIs). Introducing KPIs has proven to be a highly efficient tool for evaluating multiple activities (Parmenter, 2007), particularly when not taken at face-value but interpreted within their broader context. KPIs are one of the most widely used tools for measurement (Chan and Chan, 2004; Paddeu, 2016; Tripathi and Jha, 2018), particularly for measuring the performance of projects (Radujkovic et al., 2010). Therefore, the construction of meaningful KPIs for measuring the progress of CSA requires the development of KPIs specific to cyber-awareness, which, in turn, can help to better manage CSA projects. Without measuring the progress of a CSA project, it becomes difficult to determine whether it is moving in the right direction. KPIs generally help organisations by providing significant information about the performance of each KPI (Parmenter, 2010), as well as about the entire CSA project. Despite the growth of the body of literature on CSA, there is a lack of research about the development of KPIs in this field. A closer look at cyber-awareness will allow us to gain a better understanding for a better execution of the CSA project and to improve its effectiveness by creating a number of KPIs.

The purpose of this research is to develop key performance indicators (KPIs) for managing CSA projects and to address the gap in the existing literature but also frame them in a context of interpretation. The findings of this study will help future scholars and security professionals to better manage their CSA projects and reflect on their contextual significance within their own organisations. We approach the development of KPIs critically and we argue that they can help improve an organisation's current state of CSA, as well as increase its benefits and impact. At a minimum, these KPIs necessitate that organisations treat CSA as an ongoing project and abandon the approach that cybersecurity is an once-a-year training exercise, typically rushed through the organisation's intranet portal so that employees can receive a passing score and the 'exercise' can be ticked off as completed.

The essay is structured as follows: first, we review related work on CSA. This is followed by the methodology, including the selection framework and the instruments used for the data collection. The other sections include the analysis of the case-study data, the discussion of the results and the conclusion of the study.

RELATED WORK

During the last two decades, numerous studies on information systems security have identified the importance of cybersecurity awareness (Parsons et al., 2014; Safa et al., 2016). Security scholars have emphasised the importance of cybersecurity awareness in various ways and associated it to the reduction of security incidents caused by end-users (Siponen, 2000; Foltz et al., 2005; Dhillon, 2007; Okenyi and Owens, 2007; Roy et al., 2011; Mejias, 2012; Parsons et al., 2014; Safa et al., 2016). Information security awareness is defined by Whitman and Mattord (2012) as "a control measure designed to reduce the incidences of accidental security breaches by employees" (p. 595). Cybersecurity awareness plays a powerful role in increasing user knowledge (Whitman and Mattord, 2012), it helps organisations avoid security threats (Furnell et al., 2023; Siponen, 2000), reduces the number of security incidents (Okenyi and Owens, 2007) and it also improves end-user information security performance (Stanton et al., 2005). Though human mistakes can always occur, the establishment of an effective cybersecurity awareness programme can minimise security threats. Several studies (Puhakainen and Siponen, 2010; Okenyi and Owens, 2007; Roy et al., 2011; Galba et al., 2015; Safa et al., 2016) show that reliance on technology solutions alone is inadequate to protect information systems. For example, spear phishing attacks that are highly customised phishing attempts are designed to trick users into clicking malicious links; however, the very personal targeting and the elevated level of crafting such e-mails means that it really is up to users to identify the ensuing risk. Quite often, the inadequacy of technological solutions, coupled with the lack of awareness from staff, has led some organisations to shift rapidly from relaxed to strict controls, change their security practices and not approach cyber-awareness in a developmental character. Users might be treated as scapegoats for security incidents, but the responsibility lies with management. Nevertheless, a fragmented and always-tactical tackling of CSA might lead to user dissatisfaction with security practices and this can put an organisation's information systems at an increased risk (Montesdioca and Maçada, 2015b). Security fatigue remains another concern and so even with an increased focus on cybersecurity and awareness, the number of the security incidents is growing (Dhillon and Torkzadeh, 2006; Ponemon and IBM, 2017). There is a consensus that cybersecurity awareness must be further explored (Furnell et al., 2007; Furnell and Vasileiou, 2017).

Some studies on cybersecurity awareness have been conducted from different viewpoints (Mani et al., 2014; Parsons et al., 2014; Hanus and Wu, 2016; McCormac et al., 2017; Pattinson et al., 2017; Wiley et al., 2020; Hart et al., 2020). This includes understanding human vulnerabilities and the characteristics that affect user (Bulgurcu et al., 2010; Farooq et al., 2015; McCormac et al., 2017). Other studies concentrate on assessing the level of cybersecurity awareness among various audiences (Rezgui and Marks, 2008; Korovessis, 2011; Mani et al., 2014; Parsons et al., 2014) or on considering factors that affect cybersecurity awareness (D'Arcy et al., 2009; Mejias, 2012; Hanus and Wu, 2016; Pattinson et al., 2017; Wiley et al., 2020). Meanwhile, some aim to improve cybersecurity awareness by suggesting the use of gamification, with the suggestion to keep updating the content of awareness programmes regularly to increase benefits and influence users' positivity (Slusky and Navid, 2012; Kim, 2013; Hart et al., 2020). The purpose of those studies is to find out which characteristics affect the users behaviour towards CSA.

Thus, cybersecurity awareness has been researched from different perspectives; even though the studies on awareness differ, they still aim to improve the cybersecurity awareness experiences of users by enhancing their knowledge, increasing their compliance with information security policies, reducing and preventing human errors and enhancing organisations' security cultures. To understand the different viewpoints, we classify the previous studies into four areas (see Table 1) and review them briefly right after.

Table 1: A few key Cybersecurity Awareness (CSA) studies

Areas	Article research
User characteristics that affect CSA	Rezgui and Marks (2008)
	Bulgurcu et al. (2010)
	Farooq et al. (2015)
	McCormac et al. (2017)
Assessing the level of CSA	Korovessis (2011)
	Mani et al. (2014)
	Parsons et al. (2014)
Factors affecting CSA	D'Arcy et al. (2009)
	Mejias (2012)
	Hanus and Wu (2016)
	Pattinson et al. (2017)
	Wiley et al. (2020)
CSA programme improvement	Slusky and Navid (2012)
	Kim (2013)
	Hart et al. (2020)

In the first area labelled as "users characteristics that affect CSA", the studies that were conducted aimed to research cybersecurity awareness by considering what user characteristics affect it (see table 1). The purpose of those studies are to find out which characteristics affecting the users behaviour compliance towards CSA (see table 2). Rezgui and Marks (2008) find a number of factors influencing users' behaviour towards the CSA, including conscientiousness, cultural assumptions, beliefs and social conditions. Bulgurcu et al. (2010) determine the attitudes, normative beliefs and self-efficacy that affect employees' compliance with the CSA. Furthermore, differences among knowledge, behaviour and general awareness level were identified between males and females (Farooq et al., 2015), though McCormac et al. (2017) determine that age and gender as variables do not have a significant effect, but conscientiousness did. The key scope of several CSA-oriented studies is summarised in the table below.

Table 2: Summary of publications in information security awareness

Authors	Purpose
Bulgurcu et al. (2010)	To study the impact of the CSA on the employee's compliance with information security policy (ISP)
Farooq et al. (2015)	To examine the gender wise difference
McCormac et al. (2017)	To study the relationship between the user's information security awareness and their different variables
Rezgui and Marks (2008)	Explore the levels of information systems security awareness
Korovessis (2011)	Assess the level of the information security awareness
Mani et al. (2014)	To gain a better understanding about the statues of CSA
Parsons et al. (2014)	To assess the employee's awareness and to gain an understanding of the level of the employees' awareness in term of knowledge, attitude and behaviour.
D'Arcy et al. (2009)	To find out the effect of security countermeasures on information security misuse
Mejias (2012)	To develop a model to help better underhanging of the information security awareness
Hanus and Wu (2016)	To examine the information security awareness of home users
Pattinson et al. (2017)	To find out what are the factors that improve the level of CSA of bank employees
Wiley et al. (2020)	To explore the relationship between CSA, organisational culture, and security culture
Slusky and Navid (2012)	To study the characteristic of the student's practices, student awareness of risk, and the countermeasure
Kim (2013)	To study the statues of CSA to develop effective information security awareness training.
Hart et al. (2020)	Proposed a card game to improve the cybersecurity awareness

The second area of exploration (as shown in Table 1) is the assessment of the level of CSA among various audiences. By using a student sample, Korovessis (2011) finds that there is a lack of knowledge such as the importance of making backups of the data and performing regular software updates. Korovessis (2011) makes a strong case for conducting the CSA programme with a certain frequency/regularity. Mani et al. (2014) further corroborate and support the need for conducting regular CSA training and they too underscore the importance of regularity within a CSA programme; in fact, even when a reasonable level of CSA is found among employees (Parsons et al., 2014), key weaknesses can be identified, making the case for regular training pressing, not only for updating staff on new vectors of attack but for reinforcing the state of awareness that is required. The research from these scholars indicates an importance of monitoring frequency of CSA training though they have not formalised it as a potential KPI, nor explored its effects.

The third area we can classify in our review of relevant CSA-work is the factors that affect CSA. Here, scholars aim to find factors that influence CSA. D'Arcy et al. (2009) for example, consider whether users' personal awareness deters computer misuse while additional factors are identified by Mejias (2012) including technical knowledge, organisational impact and attacker assessments, which contribute to creating strong CSA. But as Hanus and Wu (2016) conclude, CSA impacts home users' security behaviour positively, such as response efficacy and self-efficacy. Other factors are identified by Pattinson et al. (2017) such as that previous information security education affects users' level of awareness. Finally, the broader security culture of the organisation is an important factor that improves the CSA (Wiley et al., 2020).

The fourth area that remains important in reviewing the context around developing KPIs is reflected on CSA programme improvement, in which previous studies try to improve CSA through a variety of techniques, tools and methods. Slusky and Navid (2012) recommend including topics such as physical security while Kim (2013) supports a need for regular update of CSA content. Moreover, Hart et al. (2020) recommend using gamification in CSA to improve user involvement and cybersecurity awareness.

Even though a lot of scholarly work around information security concentrates around awareness, and as we can observe from the work reviewed above, several dimensions of cyberawareness, including assessment elements, are mentioned, a coherent set of key performance indicators (KPIs) that would allow organisations to adopt a closer monitoring of cyber-awareness is missing. Of course, not all of the indicators need to be depicted in a quantifiable form; the extraction of a coherent set of both quantitative and qualitative indicators from within the literature and the empirical data can allow us to build one more stepping stone towards the formalisation of cyber-awareness monitoring. Thus, in all four areas, a reflection on the development of key performance indicators (KPI) is clearly missing. In the context of cybersecurity awareness, developing KPIs while being conscious of the potential side-effects of KPI-recording in management (Parmenter, 2007) is vital for organisations. Monitoring the effectiveness of cybersecurity awareness through KPIs is important, precisely because CSA is not an one-time endeavour (Foltz et al., 2005, Pathari and Sonar, 2012) and continuous effort (and monitoring of such effort) is required to enhance user security awareness. An ongoing effort, and reflection on KPIs for CSA can also provide a better understanding and visibility of CSA within an organisation, not only as a way of measuring CSA project objectives and charting progress on an annual basis, but also as a reflection instrument on the qualitative characteristics applied in the course of a long-term CSA effort. A set of KPIs can also help assess the strengths and weakness of a CSA project, identifying areas of excellence and those which need improvement; in turn, this will help to achieve project goals and aid goal setting and planning. Overall, creating KPIs for CSA can contribute towards the success of managing CSA as an ongoing project.

A review of previous studies in the cybersecurity awareness domain reveals that it is important to approach CSA as a long-term project and there seems to be a lack of methods used to monitor CSA regularly. KPIs are one of the most common methods to provide ongoing performance measurement and an overall evaluation of CSA performance. Adopting the KPI method and creating specific KPIs for CSA can help to improve the effectiveness of CSA and can create a heuristic accepted guideline for properly monitoring CSA for continuous improvement. It also can become a platform on which to provide information about CSA performance ebbs and flows. In this case, in order to develop KPIs for monitoring CSA, individual interviews and focus group discussions were conducted at three different organisational levels with those who have been exposed to the ongoing CSA programme.

THEORETICAL BACKGROUND

Previous research on information security has shown that the protection of information systems requires both technology and human effort. Dhillon (2007) recommends that information systems be protected at three levels: technical, formal and informal. Organisations tend to reach a satisfactory level of technological solutions, however they struggle dealing with humans. Researchers have applied different theories to address human behaviour towards ISP compliance and CSA has been seen as a powerful tool for developing a security sensitivity and a mindset that can help users adjust their behaviour and reducing internal security incidents. A number of theoretical frameworks have been applied to study CSA. These include the General Deterrence Theory (GDT), Knowledge–Attitude–Behaviour (KAB) model, Theory of Planned Behaviour (TPB), Technology Acceptance Model (TAM) and Kirkpatrick's four-level evaluation model. We summarise those briefly below and then concentrate on our selection of Kirkpatrick's model.

General Deterrence Theory (GDT)

GDT is rooted in criminology and aims to prevent criminal behaviour. It uses fear of punishment to deter criminal behaviour. In information security awareness research, the theory has been adopted to study cybersecurity awareness and find ways to prevent user behaviour that violates ISP. Foltz et al. (2005) adopted the GDT to assess the impact of ISP on users before and after they been exposed to ISP. The study shows that user awareness of ISP can affect their behaviour towards compliance with it. However, the study confirms that a single exposure to CSA is not enough. Another study applying GDT was conducted by D'Arcy et al. (2009), who found that ISP and computer monitoring affect the intention behind security misuse.

Knowledge–Attitude–Behaviour (KAB) model

The KAB model has been adopted to study the relationship between the variables of knowledge, attitude and behaviour. It was proposed by Bettinghaus (1986) to assess the influence of information campaigns on health behaviours and attitudes. The KAB model has also been applied to CSA studies. Sheng et al. (2010) conducted a study of user behaviour in regards to phishing e-mails; they found that user awareness and knowledge affected their behaviour. The result of the post-test scam e-mail shows a reduction in the number of employees interacting with scam e-mails. In addition, Pattinson et al. (2017) found that user personality such as "social desirability bias" has to be considered in designing the ISA programme.

Theory of Planned Behaviour (TPB)

The TPB is frequently adopted to predict human behaviour. The theory has been applied and used in many research fields, including information security. For example, in information security, Bulgurcu et al. (2010) applied the TPB to identify factors that prevent users from following ISP. They found that normative beliefs and self-efficacy influenced compliance; they also found that information security awareness plays a significant role in determining employee ISP compliance.

Technology Acceptance Model (TAM)

The TAM was proposed by Davis et al. (1989) to address the users predicament of accepting a new technology. The model's primary goal is to determine user behaviour towards accepting a new technology. The TAM has been widely applied in the information systems security (ISS) field. Despite the similarities between the TAM and TPB, TAM is based on two main factors: perceived usefulness (PU) and perceived ease of use (PEOU) (Davis et al., 1989). In information security awareness studies, the model is applied to study the impact of PU and PEOU on employees' intentions to comply with ISP (Lebek et al., 2014).

Kirkpatrick's Four-Level Evaluation Model

Kirkpatrick's model was proposed in 1959 to provide a comprehensive technique with which to evaluate any training programme (Kirkpatrick and Kirkpatrick, 2006). The model consists of four levels: reaction, learning, behaviour and results. An organisation's training programme effectiveness is evaluated based on these levels in order to identify its strengths and weaknesses. This model has been adopted by many fields for evaluation purposes. It has been recommended for use in studying the cybersecurity awareness programme (Abawajy et al., 2008; Rahim et al., 2015). Rahim et al. (2015) mentions that there is a lack of programme evaluation techniques used to evaluate cybersecurity awareness.

This study adopted Kirkpatrick's four-level evaluation model to examine the CSA programme within a case study. There are multiple reasons for this selection: a) the model accounts for the changes that can result from the CSA programme, b) the model is abstract enough to combine technical and non-technical perspectives of the CSA programme, c) it can be operationalised and customised to provide a comprehensive view of any CSA programme, and d) as a model, it includes critical dimensions that can be deployed in any organisation in order to capture the employees' reaction to the CSA programme, the programme's impact on their learning progress, behavioural changes which remain important, particularly in the context of behavioural IS security research, and the results of the CSA programme, the interpretation of which can assist management in considering the overall impact of CSA to the organisation. Collecting feedback about the programme from employees at different levels is important because the CSA programme targets all employees. Naturally, the views of top management and the technical team that provide the CSA programme are equally important. Involvement of top management has been shown to be an important factor in employee compliance with the ISP (Power, 2007). Therefore, when evaluating the CSA programme, the Kirkpatrick Model involves three different levels of employees: top management, technical team and end-users. Considering different subjects will help extract appropriate and corresponding KPIs according to each level of the model. Furthermore, the application of the model will help to organise the KPIs based on the four levels of Kirkpatrick model. The complete and comprehensive views that this model provides will help in the development of several KPIs that cover the important areas that need to be considered when monitoring the CSA programme. The adoption of the Kirkpatrick model to assess the awareness programme can help further improve the organisation (Abawajy et al., 2008).

REVIEW OF THE SELECTED MODEL

The First Level of the Kirkpatrick Model: Reaction

The aim of the first level of the Kirkpatrick model is to obtain CSA participants' feedback about the programme. Kirkpatrick (1983) argued that user satisfaction is vital as it largely reflects the effectiveness of the programme. User dissatisfaction with a security practice could result in putting information systems at risk (Montesdioca and Maçada, 2015a). Therefore, this level will help to extract KPIs that reflect the end-users' and top management's views about the CSA, and these will be used to monitor employees' positive and negative feedback about the CSA. The evaluation of this level will help to place emphasis on areas of excellence and areas that need improvement according to the employee's reactions, as they are a main customer of the CSA programme, thus motioning their reaction is vital. Thus, this will help to monitor the CSA project.

The Second Level of the Kirkpatrick Model: Learning

The second level aims to find out whether the CSA programme influences the participants' knowledge, that is, if user knowledge improves as a result of the CSA programme. Kirkpatrick and Kirkpatrick (2006) emphasised the importance of this level. According to Kirkpatrick and Kirkpatrick (2006), there is no behavioural improvement without learning. Thus, in security awareness, learning is an important step towards a reduction in ISP violations and security incidents. Knowledge of information security has a significant influence on employees' security performance (Pérez-González et al., 2019). Therefore, recognising the importance of the learning level draws attention to the need for a closer monitoring of learning. The evaluation of this level can help to develop several KPIs for learning that will contribute to better monitoring and the success of the CSA project.

The Third Level of the Kirkpatrick Model: Behaviour

The aim of the third level of the Kirkpatrick model is to find out whether the CSA programme contributes to changing the participants' behaviour. According to Kirkpatrick and Kirkpatrick (2005), the third level is the most significant, because if there is no behavioural change, the training programme is ineffective. Slusky and Navid (2012) argued that employees do not necessarily apply what they are aware of or what they learn. In cybersecurity awareness, the existing research literature shows a heavy focus on changing employee behaviour towards compliance with ISP. Many studies (D'Arcy et al., 2009; Bulgurcu et al., 2010) have adopted different theories and models to influence user behaviour. Therefore, this level will help to develop several KPIs that reflect the employee's behaviours that contribute to monitoring the CSA project.

The Fourth Level of the Kirkpatrick Model: Result

The aim of the fourth level is to find out the overall impact of the CSA programme on an organisation. For example, there may be a reduction in security incidents or an enhancement in the security culture. Each organisation needs to decide what combination of result-oriented elements should be considered in their evaluation at the fourth level. According to Kirkpatrick (1996), for any training programme, there must be a return on investment, such as a cost reduction or moral improvement. Thus, any given CSA project, like any other programme, has aims that should be accomplished, such as enhancing the security culture and reducing security incidents. Pathari and Sonar (2012) argued that a security awareness programme is not a one-time event. Therefore, the evaluation of the programme results will be diversified and reflected on various KPIs that need to be considered; these need to be continually monitored to ensure the success of the CSA programme.

Overall, the selection of the Kirkpatrick model was useful from a methodology standpoint as it abstracted both technical and non-technical elements through its four levels. The model also helped us to organise data collection around the categories and study CSA through a project- or programme-lens. Both perspectives are essential for the successful implementation of the CSA project. Thus, the development of KPIs requires accommodating both technical and non-technical approaches. In information security awareness, employees' behavioural and learning attributes are important factors to be enhanced positively through CSA. Because the CSA project targets all employees, their views need to be considered when generating KPIs. The results of each KPI and overall project are essential to understanding whether a given project is working. Thus, the Kirkpatrick model is organised into four levels that can help us to construct KPIs which cater to both perspectives. The structure of the Kirkpatrick levels makes it easier to generate KPIs in a more organised way by linking them to each of four subjects (levels). Also, the model supports the application of the KPIs in a more efficient way. Therefore, the model offers a foundation upon which to start constructing, deconstructing and organising the KPIs.

METHODOLOGY

The research design follows an interpretivist case study (Walsham, 2006) at University X. The data were collected using two methods. The first was in-depth individual interviews, which were conducted with 15 individuals at three different organisational levels, including top management, IT personnel and cybersecurity awareness (CSA) providers, and end-users. In this part, the focus was to extract a number of KPIs that are relating to each level of Kirkpatrick's model by obtaining the interviewees' feedback about the CSA programme at University X, as well as to determine whether CSA has contributed to increasing participants' knowledge. In addition, the interviews aimed to explore whether interviewees (from top management, the technical team and CSA providers) had observed behavioural changes. Finally, the interviews were meant to discuss the results of the CSA programme and its impact on University X. The second method was a focus group discussion; three focus groups were conducted, where the first and second groups included four people and the third group three people. In this part, the aim was to obtain the overall end-users' perspective of the CSA programme.

The output of the CSA data collection process has led to the extraction of KPIs (both from the interviews and focus group discussions). More importantly, the comprehensive views that have been gained throughout the empirical data collection approach have helped us create the richer context around which the KPIs can be framed. In this study, the Kirkpatrick's four-level model (see Figure 1) was also adopted as a theoretical scaffold in order to explore the CSA at University X. The analysis of this research is organised based on the four-level Kirkpatrick model. Data from individual interviews and focus group discussions were organised according to how they related to each level. The transcribed data were imported and analysed using NVivo software, coding the reaction level, learning level, behaviour level and result level.

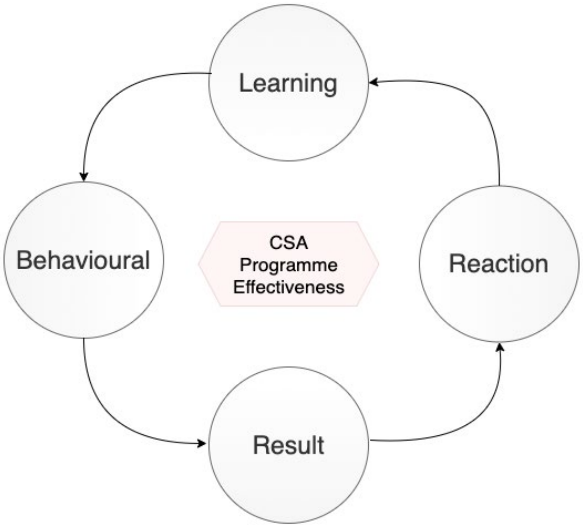

Figure 1: Kirkpatrick's four-level model

THE CASE OF UNIVERSITY X

University X is a public university in Saudi Arabia. The university has more than 12 different colleges including Applied Medical Sciences, Art and Sciences, Business Administration, Community college, Computer Sciences and Engineering, Education, Nursing, Public Health, Sciences, Pharmacy, etc. The university has more than 30,000 students divided into undergraduate and graduate studies. Also, it has more than 4,000 employees, including faculty and administrative staff. As a large institution that engages with CSA at a more strategic and longitudinal level, it is a fascinating context for this study.

To ensure the successful of the CSA programme, the University decided to set up a long-term CSA project to ensure that the implementation is successful. Four different channels are being used to create awareness about the project, including e-mail, electronic posters, face-to-face session and online sessions. The frequency of each channel is different; however, it is sustained. All the channels were established to improve University X's level of awareness. Therefore, the longitudinal character of the CSA project taking place at University X, makes it a suitable case for studying the project-oriented elements of CSA, their ongoing challenges, and also in extracting the relevant KPIs for the broader project.

DISCUSSION

Framing a CSA Start-up Checklist

The empirical data discussed above, evidences the need to have a number of items which are established in order to advance the benefits of CSA and to improve users' experiences with CSA. Kirkpatrick's 4-level conceptual scaffold also allows us to organise these CSA-oriented elements. The first item is the feedback mechanism. During the data collection processes, a number of interviewees (end-users) discussed difficulties in their experiences with CSA. Unfortunately, those issues were ignored at University X due to the absence of a feedback mechanism. On the other hand, some employees offered valuable suggestions about CSA; for instance, information on preferential methods of delivering CSA. Unfortunately, employee data was overlooked as well. Therefore, the establishment of a feedback mechanism would help in establishing a central platform for employee's issues, challenges, feedback, and suggestions.

On the bright side, the University X has established a solution for behavioural monitoring (software). According to CSA providers and IT department representatives, this software is a helpful tool for monitoring employees' behaviour and spotting suspicious activities. Although behavioural monitoring software is not a new solution, it is a necessary step. Furthermore, this solution would provide an indicator about employees' behavioural changes, which aligns with CSA goals for positive changes in users' behaviour.

Another factor mentioned was the availability of manpower and resources. One of the interviewees, an IT manager, revealed that the lack of manpower and resources was a major problem and limitation of the former CSA. Relatively, the availability of those two items has helped the University X to achieve a better CSA condition. Of course, the availability of manpower and resources is a key factor in the success of any project.

This underlines the need to run and consider CSA as a project. The information security discipline keeps changing along with the cyberattacks; while regular updating and upgrading of CSA is required, a more comprehensive project management of CSA is needed. Furthermore, according to previous studies (Foltz et al., 2005; Pathari and Sonar, 2012), CSA is not a single event. This factor aligns with the need for top management support and willingness to invest in CSA projects over time. As echoed by Rhee et al. (2012), management engagement and support is a significant factor in the success of CSA.

Finally, Table 3 presents four points as a checklist. These points should be established before commencing an CSA project or during CSA project, as again, CSA is not a one-time event. All of those points are driven from the empirical data at the University X, and a number of them were also supported by previous scholarly works.

Table 3: Checklist of CSA

	Checklist
1	Establishing a feedback mechanism
2	Establishing a behavioural monitoring mechanism
3	Evaluating the availability of manpower/resources for an ongoing CSA programme
4	Establishing top management support and willingness to invest on CSA

The Development of KPIs

The analysis based on the Kirkpatrick model shows that there is a need to develop KPIs for monitoring the CSA programme over time. Monitoring the CSA is clearly needed to examine the real condition of the CSA and to provide better visibility of its status, such as increases in learning and changes in behaviour. Despite all the improvements to which the CSA contributes, there remain some issues that need to be tackled. A development of KPIs is therefore needed to measure the progress and effectiveness of the CSA and to determine what needs to be added, updated or changed in order to improve its status. Table 4 presents all extracted KPIs (total of 11 KPIs) from the empirical data at University X.

Table 4 presents all extracted KPIs (total of 11 KPIs) from the empirical data at University X. Each group of extracted KPIs in the table below is assigned to one of the four main subjects as per the Kirkpatrick four-level model (reaction, learning, behaviour, and results). Next, a discussion will be held on each of the extracted KPIs. In addition to those four main subjects, an addition subject emerged from the data analysis which is self-reference as well as the assessment strategies for each KPI.

Table 4: Extracted KPIs

Subject	KPIs	KPIs Description	Assessment Strategies
Reaction	Satisfaction of beneficiaries with the CSA resources	This KPI pertains to the usability, effectiveness, and availability of the CSA resources (the CSA materials, awareness messages, e-learning platforms, and other pertinent resources as well)	Quantitative
	Employees' reaction towards the quality of learning experience in the programme	This KPI can assist in obtaining the viewpoint of all employees and their evaluation of the quality of the learning experience they have received. This includes *all employees* (even Senior Managers that complete CSA training as employees of the institution).	Quantitative

	Senior Management reaction towards the *perceived quality* of learning experience in the programme.	Once training of all employees is completed and the results of that training cycle are evaluated, this KPI captures the Senior Management reaction on the perceived quality and effectiveness of the programme.	Quantitative
	Average employee satisfaction with the presence and the quality of the CSA channels	In this KPI, the employees should be questioned about the effectiveness of the distinct delivery channels used in order to deliver CSA-content (e.g. face-to-face, online sessions, e-posts) and their associated perceived effectiveness (e.g. convenience of channel, etc)	Quantitative
	The overall satisfaction with the CSA programme	Overall, this KPI captures the overall satisfaction of all employees with the CSA programme when considering all related aspects (e.g. channels, content, etc)	Quantitative
Learning	Average learning performance (learning gain) of employees on the CSA programme across all objectives.	Prior to delivering the CSA programme, a set of objectives should be developed (e.g. employees should be taught on how to report a spearphishing attempt). Following the completion of the programme, a test distributed either through a survey or through the e-learning platform, needs to contain a number of questions targeting each of those aims. Some of these may change over time in future CSA cycles, while others would remain constant. The goal is to ensure that the employees are vigilant and aware and they have assimilated the knowledge required to protect the organisation's assets as well as reduce human errors. More significantly, for both newly launched CSA programmes and/or those that have been in operation for some time, there should be an external benchmark that might be used as a target (e.g. through industry forums, partner institutions that have more experience, etc).	Quantitative
	The awareness of the employees of the mission/goal of the programme	This KPI is concerned about the CSA programme's goal and vision and whether these are communicated to all staff, and more significantly, whether they are aware of the purpose/rationale for having such programme.	Quantitative
Behaviour	Average number of participants in the CSA sessions	The average number of employees participating in the CSA session, whether it is provided online or in person and measured against baseline (example). In this KPI, the average participation rate from the prior years might serve as a baseline.	Quantitative
	Behavioural progress in all CSA activities	This KPI helps to assess employee performance and behaviours when *masked* security threats are posed to them for interaction (e.g. phishing simulation, USB drops, etc). This can involve observation of employee behaviours when specific security scenarios/threats/challenges are presented to them. It is	Qualitative

		important to both monitor behavioural changes and actually shift employee perspectives from security ignorance or security apathy to security awareness.	
Result	The evaluation of the CSA programme effectiveness (e.g. reduction in the number of security incidents)	The security team alongside senior management are in charge of these indicators. By averaging the results, this KPI may be used to benchmark against an international/industrial average. It is crucial to identify gaps and include them in the operating plan of the next run of the CSA programme.	Quantitative and Qualitative
Self-reference	Percentage of achieved indicators of the CSA programme	Since the CSA programme is supposed to be carried out on a regular basis, the KPI results can identify the areas of excellence (which need to be maintained) and those that require development. These should be taken into account and included into the operational plan objectives for the next year, where those areas should be addressed.	Quantitative and Qualitative

Reaction KPI:

The analysis of subject reactions showed that five KPIs need to be considered for monitoring at this level. The analysis confirmed that employee satisfaction is vital to keeping the CSA alive and effective, since its goal is to improve cybersecurity awareness, change certain behaviours and build a solid security culture within the organisation. This aligned with Kirkpatrick (1983) claim about the significance of the reaction level; collecting their feedback lets the employees know that their feedback is valuable for further improvement.

After analysing the data with regard to the reaction subject, the first KPI that emerges is how satisfied the subject is with the resources offered by the CSA programme. CSA materials, such as an e-learning platform, are critical to a successful CSA programme, as they impart essential information to employees and increase their level of awareness about data privacy and other security issues. In addition to being available, these materials must also be accessible. The "satisfaction" KPI would therefore help provide insight into the effectiveness of the CSA programme in terms of employees' overall satisfaction with the availability of CSA resources.

This is the first dimension of the success and effectiveness of the CSA programme.

The second KPI is employees' opinions regarding the quality of the learning experience offered by the programme. Analysis of the empirical data reveals that employees' perception (self-conception) of the quality of learning offered by the CSA programme, as well as how that learning affects them, is a significant factor in improving the effectiveness of the programme. While the outcome of the learning evaluation is an important element in learning improvement, adding the element of self-conception provides deeper insight into the value of the CSA programme. The knowledge conveyed by the CSA programme is considered a key positive driver in employee performance with regard to information security (Pérez-González et al., 2019). Therefore, it is important to capture employees' self-conception of the quality of the programme's content, because their perceptions can influence their actions. Their recognition of the importance and value of the CSA programme may prompt them to change their behaviour in positive ways (by complying with ISP, for example) and improve their engagement with the programme, which in turn can improve the CSA programme.

The third KPI that emerges from the empirical data is senior management's reaction to the perceived quality of the learning experience offered by the programme. A CSA programme is like any other programme in that it requires the commitment, funding, and support of management to be successful. Therefore, a related KPI is required to ensure that the programme remains viable on an ongoing basis. Our findings confirm that senior management is the key factor in determining the success of the CSA programme. Our study shows that management involvement clearly supports the success of the programme. The importance of this KPI is that the benefit of CSA programmes is usually intangible to management. Therefore, since senior management is involved in the CSA programme in a participatory as well as a supervisory capacity, this KPI is needed to capture management's self-conception regarding the quality of the programme.

Concerning the fourth KPI, analysis shows that University X is utilising multiple delivery channels to broadcast its CSA programme. The empirical findings also demonstrate that the adoption of multiple channels has a positive impact on employees. From the interviewees' responses, we have determined that delivery channels, as well as employee satisfaction with those channels, are key to the success of the programme. However, what works in one place doesn't necessarily work in another. Therefore, the fourth KPI that emerges from the empirical data is user satisfaction with CSA delivery channels. Channel-variety is significant as it amplifies both the distribution of the message as well as the possibility of its receptivity. Empirical data analysis shows employee satisfaction with delivery channels is important and should be considered when monitoring the CSA project. Channels may vary from one organisation to another, but the important factor is whether employees are satisfied with the availability of those channels. This KPI can inform decisions regarding whether existing channels should be maintained, replaced, or supplemented with new channels.

The last KPI gleaned from the reaction subject is overall satisfaction with the CSA programme. Increasingly, employees are unintentionally causing security incidents within their companies. Although the reduction of security incidents is one of the prime goals of the CSA, it is not enough. Employee satisfaction with the CSA programme itself is also extremely important for establishing trust and longevity, reduce security fatigue, and is a significant factor in improving the effectiveness and ensuring the continuity of the CSA programme. In fact, employee dissatisfaction with information security could be a reason for compromising information systems (Montesdioca and Maçada, 2015). Evidence from the present case study supports the idea that employee satisfaction with the CSA programme is integral to its success. Therefore, we believe the improvement of the employee's positive reaction toward the programme would positively influence their own learning and behaviour. In fact, a review of the literature indicates that although changing employee behaviours have been seen as a major component of the effectiveness of CSA programmes (Parsons et al., 2014), CSA programmes have not been completely successful in inducing positive behavioural change (Jaeger, 2018; Abawajy, 2014). Our interpretation of the findings is that delivering the programme is important, but not enough. Soliciting employees' feedback and their self-conception about certain aspects of the CSA programme, and incorporating that feedback into the next iteration of the programme, could improve employee behaviour.

Overall, the assessment of all KPIs in the reaction subject can be quantitively evaluated. Actually, the reaction subject helps to obtain the user perspective about the activities of the IT department, specifically in this study the CSA activities, which will definitely lead to better improvement of CSA. Employee satisfaction with the CSA is an important factor (Montesdioca and Maçada, 2015); employee recognition of the value of the information has a positive influence on compliance with security polices (Doherty and Tajuddin, 2018).

Learning KPIs:

At the learning subject, we extracted two KPIs. The analysis showed that the learning level is very important and it needs to be monitored because it indicates not only the progression of the employees' knowledge, but also whether there are gaps that remain to be filled.

The KPIs associated with learning a subject also show the level of awareness over time with regard to how the CSA is progressing. The literature review discussed the serious threats that are unintentionally caused by internal employees, and these threats are often the result of carelessness and a lack of knowledge. In addition, the literature review argued that increasing the level of employee awareness could be a significant factor in reducing such human errors. In fact, the level of employees' cybersecurity awareness is not a new phenomenon, and it has been researched previously (Furnell et al., 2007, Kim, 2013), but it remains important for the development and improvement of the CSA, and it provides an important indicator of the CSA's effectiveness.

From the empirical data, we extracted two KPIs, the first of which was the average learning performance (learning gain) of employees in the CSA programme across all objectives. As with any other programme, the CSA programme should have well-defined objectives to ensure that employees are working toward achieving those objectives. For example, one of the potential objectives could be educating employees on how to report a spear phishing attempt. Therefore, following the completion of the CSA programme, a test should be distributed to capture the average employee awareness of the defined objectives. The overall goal of this KPI is to ensure that employees become vigilant and that they have accumulated the knowledge required to reduce potential human errors.

The second KPI is the awareness of employees of the missions and goals of the programme. Since the CSA programme at University X is approached as a longitudinal programme, it is important to ensure that employees are well aware of the programme's goals and mission. With regard to information security policy, it has been found that employee perceptions about the importance and value of information have a very positive impact in terms of complying with ISP (Doherty and Tajuddin, 2018). Sharing knowledge about information security has also been recognised to have a positive impact on employee performance (Pérez-González et al., 2019). Therefore, taking the literature review, the present empirical data, and the criticality of the CSA programme together, we noticed that delivering the programme message and discussing its goals and missions alone are not enough. It is important to ensure that the message gets across, meaning that we must ensure that the message is fully understood. We have come to the conclusion that this approach would help to get employees on board to improve their information security performance.

Learning is a key factor in cybersecurity awareness, and it requires regular monitoring. Creating KPIs for learning is vital to the success of the CSA project. This is because knowledge significantly influences users' behaviour.

Behavioural KPIs:

Regarding the third subject (behaviour), the data analysis showed a need for two KPIs. The first KPI is the average number of participants in CSA sessions. Usually, the CSA programme utilises multiple channels to deliver its message. Therefore, it is important to monitor employee participation in the CSA programme, such as the average number of employees attending security awareness sessions either online or in person. This KPI can be used as an indicator of employee behaviour and can serve as a method of monitoring employee engagement, which is important since these sessions seem to have a significant impact on learning improvement. Also, a stable or increasing participation rate could be interpreted as an indication of positive behavioural change. Moreover, because cybersecurity threats are continually changing, it is important to ensure employee participation in cybersecurity sessions in order to confirm they have the most current information. More importantly, increasing the rate of participation can help employees recognise and understand the importance of attending those session, the value of the CSA programme in general, and how the programme contributes to their behavioural change. Without employee participation, CSA programmes will most likely fail to fulfil their desired objectives. This KPI is essential for the entire CSA project. The analysis showed that University X, for example, ensured a high level of employee participation in the CSA programme by offering awareness sessions both face-to-face and online. Overall, this KPI can help assess the effectiveness of the CSA programme. The second KPI that emerges from the empirical data is behavioural progress in all CSA activities. Those activities could include, for example, phishing simulations. It is important to both monitor behavioural changes and shift employee attitudes from security ignorance or security apathy to security awareness. Accomplishing that shift can be a major step toward achieving the programme goal and reducing human error. Changing employees' behaviour is challenging, but necessary. Therefore, it is important to observe and monitor employee behaviour in specific security scenarios. This important indicator demonstrates increases in awareness as well as positive behavioural changes. Thus, the monitoring of the CSA requires monitoring the progress of this KPI, as it reflects a positive behavioural change. If this KPI declines, it could indicate that employees are not following the policy, or that the programme is failing to increase security awareness among employees. In fact, the empirical data shows that there was an increase in the number of employees reporting suspicious e-mails, which is one example of a positive change. While this KPI indicates how employees handle a real cyberattack, it can also show how they behave when faced with a fake one. For instance, in the case of University X, the university sends simulated phishing emails in order to test its employees' preparedness and vigilance. Thus, monitoring employee behaviour is key to ensuring the project's effectiveness.

On the behavioural subject, monitoring employees' behaviour is critical for the CSA project, as employees generally had higher scores in learning than in behaviour (Parsons et al., 2014). Many factors can affect employee behaviour, such as background knowledge and past experience. Reducing human error to zero is unrealistic; a more attainable goal is to minimise human error to the lowest possible level. The empirical data reveals a reduction in human error at University X since the staring of the CSA programme. Therefore, those two KPIs are vital, as data demonstrated that monitoring employee behaviour is essential to enhancing the project's effectiveness. Concerning the third subject, without behavioural change, the CSA programme is more likely to fail to deliver its potential benefits. As one of the CSA project goals is to reduce ISP violations by users, monitoring employees' behaviour is a necessary part of the CSA project.

Result KPIs:

The fourth subject is the result, in which we extracted one KPI which is the evaluation of CSA programme effectiveness (e.g., reduction in the number of security incidents). This KPI generates a better understanding of the overall CSA progress, strengths, and weaknesses. For example, the reduction of security incidents is a sign of CSA effectiveness. On the contrary, an increase in security incidents is a warning sign that improvement is required. In addition, this KPI can generate a benchmark, which can serve as an internal benchmark that maintains the progress of the programme and reveals the areas of excellence and those that need improvement. It is worth noting that the CSA is not a one-time programme. Therefore, regular monitoring is essential, as the CSA programme is cumulative work. This subject provides a better understanding of the progress of the CSA over time, thus helping decision makers make plans for the programme. It also generates benchmarks for the higher education sector.

Self-reference:

The KPIs in all four Kirkpatrick domains (i.e., reaction, learning, behavioural, and result) are necessary to determine the effectiveness of the CSA programme. Hence, the analysis brings additional insight into the literature by showing how to adjust Kirkpatrick's four-level model for application to the CSA programme. In our work, we incorporated an additional dimension, self-reference. In order to consider the effectiveness of CSA programmes, self-reference demarcates the continuous re-entry of KPI-evaluation and re-evaluation. This is more than selfbenchmarking and one extracted KPI here can be the percentage of achieved indicators of the CSA programme. Since the CSA programme is critical and must be run regularly over time as a project with a coherent project management, this KPI is necessary. Generally, the CSA programme should have a set number of objectives at the beginning of the programme (e.g., reducing the number of security incidents). If these objectives are not met, they should be pushed forward into the operational plan for the next year. The team would then attempt to achieve the objectives during the next programme run. As such, this KPI can help to produce a better view of the CSA team's effectiveness.

A depiction of the key indicators is shown in the figure below (Figure 2). We note that the self-reference level we propose is portrayed at the very centre of the model. The indicative KPI we have proposed for that relates to the percentage of achieved indicators, so in a sense, it is like a meta-KPI; this raises the interesting question of what other KPIs can be considered here for evaluating the whole programme. Such KPIs act as unifying threads that bring together an evaluation of the total CSA programme.

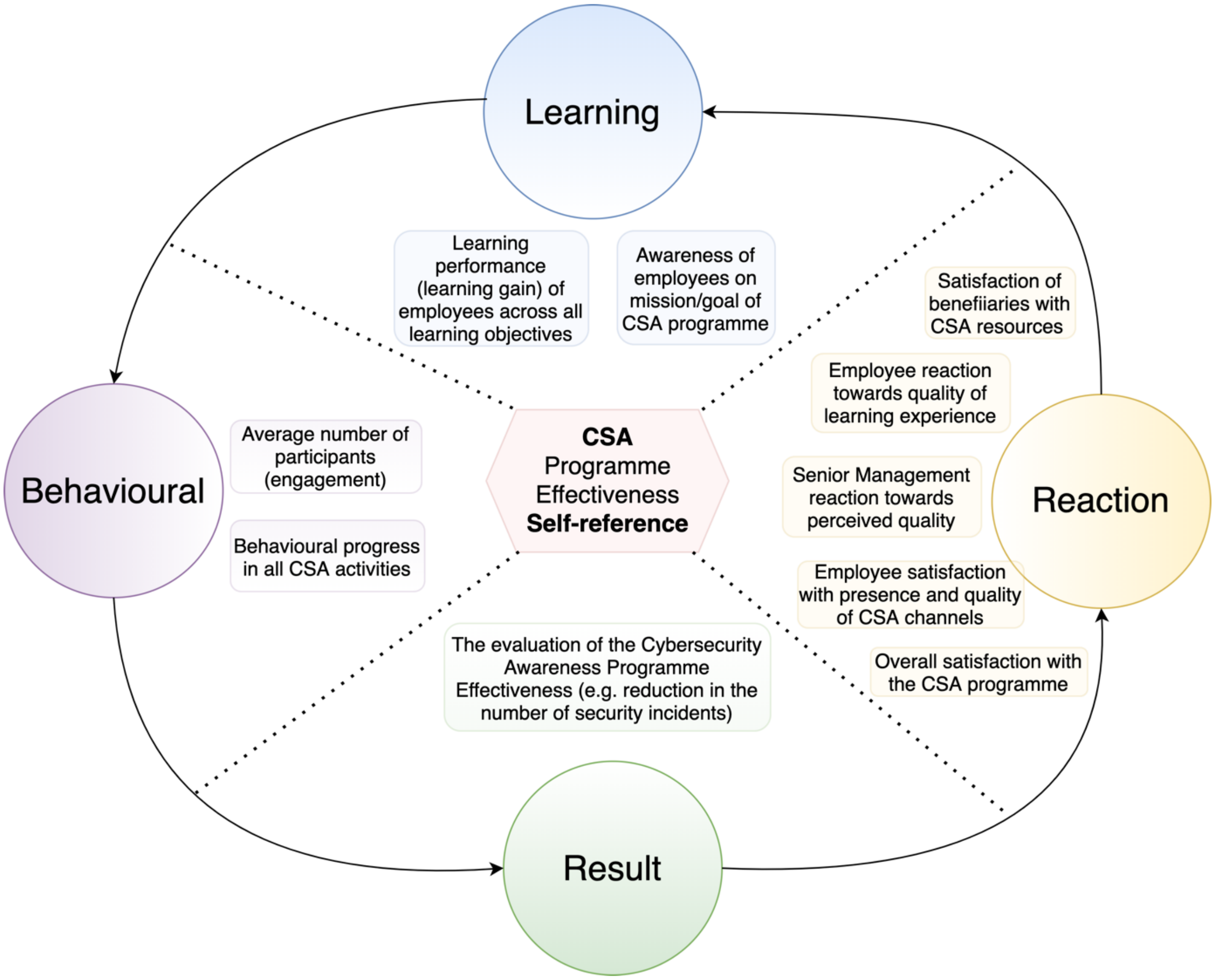
Learning
Learning performance (learning gain) of employees across all learning objectives
Awareness of employees on mission/goal of CSA programme
Satisfaction of benefiiaries with CSA resources
Employee reaction towards quality of learning experience
Senior Management reaction towards perceived quality
Reaction
Employee satisfaction with presence and quality of CSA channels
Overall satisfaction with the CSA programme
CSA Programme Effectiveness Self-reference
Behavioural
Average number of participants (engagement)
Behavioural progress in all CSA activities
The evaluation of the Cybersecurity Awareness Programme Effectiveness (e.g. reduction in the number of security incidents)
Result

Figure 2: A Kirkpatrick-oriented model for CSA-based KPIs

The measurement and consideration of those KPIs in all four domains (reaction, learning, behavioural and result) is necessary to determine the effectiveness of the CSA project. Hence, the analysis brings an additional insight to the literature by showing how to adjust the Kirkpatrick four level model in order to be applied for the CSA programme. We incorporate an additional domain of self-reference as it helps generate a better image about the effectiveness of the CSA project team and its self-monitoring, self-determination and self-actualization.

CONCLUSION

From the case study and data analysis, we devised a number of KPIs (see Table 4) that can be used to monitor CSA from a project perspective based on Kirkpatrick's model and its levels-reaction, learning, behaviour, and results and that of self-reference. Doing so can help establish a significant continuity in managing CSA and in elevating its role as an ongoing necessity rather than as an one-off training event. Each level has KPIs that need to be satisfied in order to ensure the effectiveness of the CSA, and the KPIs of each level can help to generate better visibility regarding the strength and weakness of the level and of the CSA overall. This list is neither exhaustive nor restrictive but provides a link between Kirkpatrick's model and CSA. We encourage others to implement and customize/adjust/extend/condense the KPIs based on the organisational needs and priorities they would like to achieve. Our framework is meant to provide a guiding architecture for evaluating CSA and indicative KPIs and it also stresses the need for considering monitoring the progress of the CSA programme over time and to work further towards exploring CSA-effectiveness from a programme perspective.

Practical Contribution

The present study offers a significant practical contribution that would help to better manage the progression of the CSA programme by providing 11 KPIs that can assist to improve the effectiveness of the CSA programme.

Research Limitations

Although the authors have developed an important method for managing the CSA programme, it has not been tested yet due to the nature of this study (qualitative research). However, the study still offers an important practice and theoretical implications.

References

Abawajy J (2014) User Preference of Cyber Security Awareness Delivery Methods. Behaviour and Information Technology 33(3), 237–248.

Abawajy J, et al. (2008) Investigation of Stakeholders Commitment to Information Security Awareness Programs. In 2008 International Conference on Information Security and Assurance, pp 472-476, IEEE, Busan, 2008.

Balozian P and Leidner D (2017) The Assumptions and Profiles Behind It Security Behavior. In International Conference on System Sciences, pp 4987-4996, Hawaii, USA.

Bettinghaus E (1986) Health Promotion and the Knowledge-Attitude-Behavior Continuum. Preventive Medicine 15, 475-491.

Bulgurcu B, et al. (2010) Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness1. MIS Quarterly 34(3), 523-548.

Chan A and Chan A (2004) Key Performance Indicators for Measuring Construction Success. Benchmarking: An International Journal 11(2), 203-221.

Chan M, et al. (2005) Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. Journal of Information Privacy and Security 1(3), 18-41.

D’Arcy J, et al. (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20, 79-98.

Davis FD, et al. (1989) User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science 35(8), 982-1003.

Dhillon G (2007) Principles of Information Systems Security: Texts and Cases. Wiley, Hoboken, NJ.

Dhillon G, et al. (2016) Interpreting Information Security Culture: An Organizational Transformation Case Study. Computers and Security 56, 63-69.

Dhillon G and Torkzadeh G (2006) Value-Focused Assessment of Information System Security in Organizations. Information Systems Journal 16(3), 293-314.

Doherty NF and Tajuddin ST (2018) Towards a User-Centric Theory of Value-Driven Information Security Compliance. Information Technology and People 31(2), 348-367.

Farooq A, et al. (2015) Observations on Genderwise Differences among University Students in Information Security Awareness. International Journal of Information Security and Privacy 9(2), 60-74.

Foltz CB, et al. (2005) Have You Met Your Organization’s Computer Usage Policy? Industrial Management and Data Systems 105(2), 137-146.

Furnell S, et al. (2023) Assessing Organizational Awareness and Acceptance of Digital Security by Design. Journal of Information Systems Security 19(1), 3-18.

Furnell S and Vasileiou I (2017) Security Education and Awareness: Just Let Them Burn? Network Security 5(9),

Furnell SM, et al. (2007) Assessing the Security Perceptions of Personal Internet Users. Computers and Security 26(5), 410-417.

Galba T, et al. (2015) An Information Security and Privacy Self-Assessment (Ispsa) Tool for Internet Users. Acta Polytechnica Hungarica 12(3), 149-162.

Hanus B and Wu Y (2016) Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. Information Systems Management 33(1), 2-16.

Hart S, et al. (2020) Riskio: A Serious Game for Cyber Security Awareness and Education. Computers and Security 95,

Hitachi S (2018) 5 Benefits of Project Management for Cybersecurity. Hitachi Systems Security.

Jaeger L (2018) Information Security Awareness: Literature Review and Integrative Framework. In 51st Hawaii International Conference on System Sciences, Hawaii.

Kim E (2013) Recommendations for Information Security Awareness Training for College Students. Information Management and Computer Security 22(1), 115-126.

Kirkpatrick DL (1983) Four Steps to Measuring Training Effectiveness. Personal Administrator 28(11), 19-25.

Kirkpatrick DL (1996) Great Ideas Revisited. Training and Development 50(1), 54-57.

Kirkpatrick DL and Kirkpatrick JD (2005) Transferring Learning to Behavior: Using the Four Levels to Improve Performance. Berrett-Koehler Publishers.

Kirkpatrick DL and Kirkpatrick JD (2006) Evaluating Training Programs. Berrett-Koehler Publishers, Inc, San Francisco: CA.

Korovessis P (2011) Information Security Awareness in Academia. International Journal of Knowledge Society Research,

Lebek B, et al. (2014) Information Security Awareness and Behavior: A Theory-Based Literature Review. Management Research Review 37(12), 1049-1092.

Mani D, et al. (2014) Information Security in the South Australian Real Estate Industry. Information Management and Computer Security 22(1),

McCormac A, et al. (2017) Individual Differences and Information Security Awareness. Computers in Human Behavior 69, 151-156.

Mejias RJ (2012) An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk. 45th Hawaii International Conference on System Sciences, Maui, HI, pp 3258-3267.

Montesdioca GPZ and Maçada ACG (2015a) Measuring User Satisfaction with Information Security Practices. Computers and security 48, 267-280.

Montesdioca GPZ and Maçada ACG (2015b) Measuring User Satisfaction with Information Security Practices. Computers and security 48, 267-280.

Monzelo P and Nunes S (2021) Information Security Awareness and Its Impact on the Ciso's Responsibilities — a Study of the Portuguese Environment. Journal of Information System Security 17(2), 81–102.

Morrison D (2018) 5 Reasons Why Cyber Security Projects Fail., Loop.

Okenyi PO and Owens TJ (2007) On the Anatomy of Human Hacking. Information Systems Security 16(6), 302.

Paddeu D (2016) How Do You Evaluate Logistics and Supply Chain Performance? A Review of the Main Methods and Indicators. European Transport/Trasporti europei 61(4), 1-16.

Parmenter D (2007) Key Performance Indicators: Developing, Implementing,and Using Winning Kpis. John Wiley and Sons, New Jersey.

Parmenter D (2010) Key Performance Indicators (Kpi): Developing, Implementing, and Using Winning Kpis. John Wiley and Sons, Hoboken, New Jersey.

Parsons K, et al. (2014) A Study of Information Security Awareness in Australian Government Organisations. Information Management and Computer Security 22(4), 334-345.

Pathari V and Sonar R (2012) Identifying Linkages between Statements in Information Security Policy, Procedures and Controls. Information Management and Computer Security 20(4), 264-280.

Pattinson M, et al. (2017) Managing Information Security Awareness at an Australian Bank: A Comparative Study. Information and Computer Security 25(2), 181-189.

Pérez-González D, et al. (2019) Organizational Practices as Antecedents of the Information Security Management Performance: An Empirical Investigation. Information Technology and People 32(5), 1262-1275.

Ponemon and IBM (2017) Cost of Data Breach Study: Global Overview. Ponemon, North Traverse City, Michigan.

Puhakainen P and Siponen M (2010) Improving Employees' Compliance through Nformation Systems Security Training an Action Reseach Study. MIS Quarterly 34(4), 757-778.

Radujkovic M, and, et al. (2010) Application of Key Performance Indicators in South-Eastern European Construction. Journal of Civil Engineering and Management 16, 521-530.

Rahim NHA, et al. (2015) A Systematic Review of Approaches to Assessing Cybersecurity Awareness. Kybernetes 44(4), 606-622.

Rezgui Y and Marks A (2008) Information Security Awareness in Higher Education: An Exploratory Study. Computers and Security 27, 241-253.

Rhee H-S, et al. (2009) Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior. Computers and Security 28(8), 816-826.

Rhee H-S, et al. (2012) Unrealistic Optimism on Information Security Management. Computers and Security 31(2), 221-232.

Roy S, et al. (2011) Detecting and Defeating Sql Injection Attacks. International Journal of Information and Electronics Engineering 1(1),

Safa NS, et al. (2016) Information Security Policy Compliance Model in Organizations. Computers and Security 56(70), 70-82.

Sheng S, et al. (2010) {Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In SIGCHI Conference on Human Factors in Computing Systems, pp 373-382, ACM, New York, NY, USA.

Siponen MT (2000) Critical Analysis of Different Approaches to Minimizing User-Related Faults in Information Systems Security: Implications for Research and Practice. Information Management and Computer Security 8(5), 179-209.

Slusky L and Navid PP (2012) Students Information Security Practices and Awareness. Journal of Information Privacy and Security 8(4), 3-26.

Spears J and Barki H (2010) User Participation in Information Systems Security Risk Management. MIS Quarterly 34(3), 503-522.

Stanton JM, et al. (2005) Analysis of End User Security Behaviors. Computers and Security 24(2), 124-133.

Tripathi KK and Jha KN (2018) An Empirical Study on Performance Measurement Factors for Construction Organizations. KSCE J Civ Eng 22, 1052-1066.

Walsham G (2006) Doing Interpretive Research. European Journal of Information Systems 15, 320-330.

Whitman ME and Mattord HJ (2012) Principles of Information Security. Thomson Course Technology, Boston, MA, USA.

Wiley A, et al. (2020) More Than the Individual: Examining the Relationship between Culture and Information Security Awareness. Computers and Security 88,

Mohammad Mulayh. Alshammari is an Assistant Professor in the department of Management Information Systems at the University of Hail Business School in Saudi Arabia. He holds a PhD in cybersecurity and Information Systems Security from Hull University. His primary research interests are around cybersecurity awareness and culture and Information Systems Security.

Dionysios S. Demetis is an Associate Professor (Reader) of management systems at Hull University Business School, UK and a Visiting Professor at Texas A&M University, USA. He holds a PhD in anti-money laundering and information systems from the London School of Economics and his research concentrates around systems theory, anti-money laundering and cybersecurity. He is the author of two books, one on the philosophy of science and the intrinsic paradoxes of knowledge creation.