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

Mohammad Mulayh. Alshammari
Department of Management and Information Systems, Business School, University of Hail, Saudi Arabia
Dionysios S. Demetis
Centre for Systems Studies, Hull University Business School, United Kingdom

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.

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). 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, endusers' 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 in order to review its ongoing development.

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 the CSA project and reflect on their contextual significance within their own organisations. The development of KPIs can help to improve the current state of CSA and increase its benefits and impact.

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, Parsons et al., 2014, Safa et al., 2016, Mejias, 2012). 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 (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. User dissatisfaction with security practices could put organisation's information systems at risk (Montesdioca and Maçada, 2015). Despite 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 behaviours (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). 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 are to find out which characteristics affecting the users behaviour compliance towards CSA.

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 take a step towards 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

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: the model has the ability to display the change resulting from the CSA programme, and the model is abstract enough to combine technical and non-technical perspectives of the CSA programme. It also provides a comprehensive view of the CSA programme and its impact on university X, including the employees' reaction to the CSA programme and the CSA programme's impact on learning progress, behavioural changes and the overall impact on the organisation. Collecting feedback about the programme from employees at different levels is important because the CSA programme targets all employees. However, the views of the top management and technical team that provide the ISA programme are equally important. Involvement of the top management has been shown to be an important factor in employee compliance with the ISP (Power, 2007). Therefore, when evaluating the ISA programme, the Kirkpatrick Model involves three different levels of employees: top management, technical team and end-user. Moreover, the model considers different subjects for evaluation: reaction, learning, behaviour and outcome. Considering different subjects will help to extract more 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).

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 (see Table 1). 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 (see Table 2), 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 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.

Table 1. List of Interviewees

No. of the Interview	Gender	Years of employment	Position classification
1	M	4	External organisation
2	M	4	External organisation
3	M	3	Information security supervisor
4	M	5	Department manager
5	F	3	Faculty member
6	F	2	Faculty/ department chair
7	M	9	Top Management
8	M	5	Top Management
9	M	4	Top Management
10	M	2	Faculty member
11	M	8	Top Management
12	M	5	University IT Manager
13	M	6	Department Manager
14	F	2	Faculty member
15	M	4	Top Management

Table 2. List of Focus Group Interviewees

	Gender	Years of employment	Position classification
Focus Group 1.	M	5	Faculty
	M	8	Staff
	M	10	Staff
	M	6	Staff
Focus Group 2.	F	4	Faculty
	M	3	Faculty
	M	3	Staff
	M	1	Staff
Focus Group 3.	F	1	Faculty
	F	4	Staff
	M	5	Staff

DISCUSSION 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 3 presents all extracted KPIs (total of 11 KPIs) from the empirical data at University X.

Table 3: Extracted KPIs

Subject	KPIs	KPIs Description
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)
	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).

	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.
	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)
	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)
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).
	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.
Behaviours	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.
	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 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.
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.

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 (selfconception) 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 (Abawajy, 2014, Jaeger, 2018). 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 e-mails 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.

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 3) 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. 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.

References

ABAWAJY, J. 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology,* 33**,** 237–248.

ABAWAJY, J., THATCHER, K. & KIM, T.-H. Investigation of Stakeholders Commitment to Information Security Awareness Programs. 2008 International Conference on Information Security and Assurance, 2008 Busan, 2008. IEEE, 472-476.

BALOZIAN, P. & LEIDNER, D. The Assumptions and Profiles Behind IT Security Behavior. International Conference on System Sciences, 2017 Hawaii, USA. 4987-4996.

BULGURCU, B., CAVUSOGLU, H. & BENBASAT, I. 2010. INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS1. *MIS Quarterly,* 34**,** 523-548.

CHAN, A. & CHAN, A. 2004. Key performance indicators for measuring construction success. *Benchmarking: An International Journal,* 11**,** 203-221.

CHAN, M., WOON, I. & KANKANHALLI, A. 2005. perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy & Security,* 1**,** 18-41.

D'ARCY, J., HOVAV, A. & GALLETTA, D. 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research,* 20**,** 79-98.

DHILLON, G. 2007. *Principles of information systems security: Texts and Cases,* Hoboken, NJ, Wiley.

DHILLON, G., SYED, R. & PEDRON, C. 2016. Interpreting information security culture. *Computers & Security* 56**,** 63-69.

DHILLON, G. & TORKZADEH, G. 2006. Value-focused assessment of information system security in organizations. *Information Systems Journal,* 16**,** 293-314.

DOHERTY, N. F. & TAJUDDIN, S. T. 2018. Towards a user-centric theory of value-driven information security compliance. *Information Technology & People,* 31**,** 348-367.

FAROOQ, A., ISOAHO, J., VIRTANEN, S. & ISOAHO, J. 2015. Observations on Genderwise Differences among University Students in Information Security Awareness. *International Journal of Information Security and Privacy,* 9**,** 60-74.

FOLTZ, C. B., CRONAN, T. P. & JONES, T. W. 2005. Have you met your organization's computer usage policy? *Industrial Management & Data Systems,* 105**,** 137-146.

FURNELL, S., . & VASILEIOU, I. 2017. Security education and awareness: just let them burn? *Network Security,* 5.

FURNELL, S. M., BRYANT, P. & PHIPPEN, A. D. 2007. Assessing the security perceptions of personal Internet users. *Computers & Security,* 26**,** 410-417.

GALBA, T., SOLIC, K. & LUKIC, I. 2015. An information security and privacy selfassessment (ISPSA) tool for internet users. *Acta Polytechnica Hungarica,* 12**,** 149162.

HANUS, B. & WU, Y. 2016. Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management,* 33**,** 2-16.

HART, S., MARGHERIA , A., PACIB, F. & SASSONE, V. 2020. Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security,* 95.

HITACHI, S. 2018. 5 Benefits of Project Management for Cybersecurity. Available from: https://hitachi-systems-security.com/5-benefits-of-project-managementforcybersecurity/ [Accessed 10/01 2021].

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

KIM, E. 2013. Recommendations for information security awareness training for college students. *Information Management & Computer Security,* 22**,** 115-126.

KIRKPATRICK, D. L. 1983. Four steps to measuring training effectiveness. *Personal Administrator,* 28**,** 19-25.

KOROVESSIS, P. 2011. Information Security Awareness in Academia. *International Journal of Knowledge Society Research*.

MANI, D., CHOO, K.-K. R. & MUBARAK, S. 2014. Information security in the South Australian real estate industry. *Information Management & Computer Security,* 22.

MCCORMAC, A., ZWAANS, T., PARSONS, K., CALIC, D., BUTAVICIUS, M. & PATTINSON, M. 2017. Individual differences and Information Security Awareness. *Computers in Human Behavior,* 69**,** 151-156.

MEJIAS, R. J. 2012. An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk. *45th Hawaii International Conference on System Sciences.* Maui, HI.

MONTESDIOCA, G. P. Z. & MAÇADA, A. C. G. 2015a. Measuring user satisfaction with information security practices. *Computers & security* 48**,** 267-280.

MORRISON, D. 2018. 5 reasons why cyber security projects fail. Available from: https://www.loopsec.com.au/blog-events/blog/5-reasons-why-cyber-security-projectsfail [Accessed 8/1 2021].
OKENYI, P. O. & OWENS, T. J. 2007. On the Anatomy of Human Hacking. *Information Systems Security,* 16**,** 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**,** 1-16.
PARMENTER, D. 2007. *Key Performance Indicators: Developing, Implementing,and Using Winning KPIs,* New Jersey, John Wiley & Sons.
PARMENTER, D. 2010. *Key Performance Indicators (KPI): Developing, Implementing, and Using Winning KPIs,* Hoboken, New Jersey, John Wiley & Sons.
PARSONS, K., MCCORMAC, A., PATTINSON, M., BUTAVICIUS, M. & JERRAM, C. 2014. A study of information security awareness in Australian government organisations. *Information Management & Computer Security,* 22**,** 334-345.
PATHARI, V. & SONAR, R. 2012. Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security,* 20**,** 264-280.
PATTINSON, M., BUTAVICIUS, M., PARSONS, K., MCCORMAC, A. & CALIC, D. 2017. Managing information security awareness at an Australian bank: a comparative study. *Information and Computer Security,* 25**,** 181-189.
PÉREZ-GONZÁLEZ, D., PRECIADO, S. T. & SOLANA-GONZALEZ, P. 2019. Organizational practices as antecedents of the information security management performance: An empirical investigation. *Information Technology & People,* 32**,** 12621275.
PONEMON & IBM 2017. Cost of Data Breach Study: Global Overview. North Traverse City, Michigan: Ponemon.
POWER, E. M. 2007. Developing a Culture of Privacy: A Case Study.
PUHAKAINEN, P. & SIPONEN, M. 2010. IMPROVING EMPLOYEES' COMPLIANCE THROUGH NFORMATION SYSTEMS SECURITY TRAINING AN ACTION RESEACH STUDY. *MIS Quarterly,* 34**,** 757-778.
RADUJKOVIC, M., &, VUKOMANOVIĆ, M., & & BURCAR DUNOVIC, I. 2010. Application of Key Performance Indicators in South-Eastern European construction. *Journal of Civil Engineering and Management,* 16**,** 521-530.
REZGUI, Y. & MARKS, A. 2008. Information security awareness in higher education: An exploratory study. *Computers & Security,* 27**,** 241-253.
RHEE, H.-S., KIMB, C. & RYUC, Y. U. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security,* 28**,** 816-826.
ROY, S., SINGH, A. K. & SAIRAM, A. S. 2011. Detecting and Defeating SQL Injection Attacks. *International Journal of Information and Electronics Engineering,* 1.
SAFA, N. S., VON, R. & FURNELL, S. S. 2016. Information security policy compliance model in organizations. *Computers & Security,* 56**,** 70-82.
SIPONEN, M. T. 2000. Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management & Computer Security,* 8**,** 179-209.
SLUSKY, L. & NAVID, P. P. 2012. Students Information Security Practices and Awareness. *Journal of Information Privacy & Security,* 8**,** 3-26.
SPEARS, J. L. & BARKI, H. 2010. User participation in information systems security risk management. *MIS quarterly,* 34**,** 503.
STANTON, J. M., STAM, K. R., MASTRANGELO, P. & JOLTON, J. 2005. Analysis of end user security behaviors. *Computers & Security,* 24**,** 124-133.
TRIPATHI, K. K. & JHA, K. N. 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, M. E. & MATTORD, H. J. 2012. *Principles of Information Security,* Boston, MA, USA, Thomson Course Technology.
WILEY, A., MCCORMACB, A. & CALIC, D. 2020. More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security,* 88.