DEGREE PROJECT

Motivating Cybersecurity Awareness within an Organisation

An explorative study from an awareness practitioner's perspective

Adedoyin Agbo-ola

Information Security, master's level (120 credits)
2022

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

LULEÅ UNIVERSITY OF TECHNOLOGY

Abstract

Security awareness has been a popular topic in the last few years for both information systems researchers and organisations. News broadcasts has brought attention to the increase in cyber-attacks, with these reports noting that a significant number of these breaches have been caused by human error, linked to employee's lack of engagement with their organisations security policies and awareness campaigns. Whilst there is existing research in human factors and the barriers of security behaviours effect on cybersecurity awareness; in practice we know very little about how employees can be motivated to engage in cybersecurity awareness programs.

This study aims to explore how information security practitioners motivate interest in cybersecurity awareness. It does this through an exploratory case study approach using qualitative data collected from in-depth interviews of four cybersecurity awareness practitioners that were conducted. From an application perspective, the findings suggest that these practitioners do use a variety of techniques to motivate employee interest in cybersecurity awareness. The study identified four factors used by practitioners to motivate cybersecurity awareness which are 1) using different engaging techniques, 2) making it personable & relatable, 3) utilising leadership commitment and 4) embracing technical controls. This paper discusses these factors and implications for practitioners.

Keywords: cybersecurity awareness, barriers, motivators.

Foreword

This study is the culmination of a two-year Master of Science (MSC) in Information Security program at Lulea University. This work was carried out under Martin Lundgren (PHD), my thesis supervisor whom I would like to thank for his comments, suggestions, and encouragement. I would also like to thank my fellow thesis group members who peer reviewed the paper and provided constructive feedback. It has been a pleasure working with you and I wish you all best of luck in future endeavours.

I would like to thank the cybersecurity practitioners that agreed to be interviewed, their insights have made this thesis possible. I am also grateful to my employer and line manager who over the last two years gave me time off for exam commitments.

Finally, I would like to thank my husband and daughters who have been patient with me over these last two years, giving me the space and encouragement to meet course work and exam timelines.

To God be the Glory.

Adedoyin Agbo-ola

June 2022

Table of Contents

1. Introduction

Organisations are fighting information and cybersecurity battles on two fronts; they have to deal with both outside threats and insider threats (Raddatz et al., 2020; Li, et al., 2019). These organisations have increased their efforts in using security awareness and training programs to equip their employees with the ability to mitigate cybersecurity threats (Reeves et al., 2021). As information security have shifted towards organisation and individual perspectives (Bulgurcu et al., 2010), this has seen organisations carry out and design cybersecurity awareness programs to improve employees' cybersecurity behaviours (Reeves et al., 2021, Ergen et al., 2021).

Most breaches are the result of employee's failure to comply with the organisation's security policies (Nifakos et al., 2021). Whilst cybersecurity awareness is growing amongst senior executives, there is a need for organisations to rethink their cybersecurity awareness strategy as cyber threats become even more sophisticated. Ergen et al (2021) noted that cyber threats that organisations must deal with are usually difficult to detect.

There is a growing need for organisations to understand why employees seem to disregard organisational security policies, particularly when there is a security awareness program in place within those organisations. With the increase in the number of security breaches caused by employees' noncompliance to security policies, this is becoming a major concern for organisations (Alshaihk et al., 2018).

Research has focused on cyber awareness, and many of which agree that an effective awareness program improves the security behaviours of employees (Li, et al., 2019; de Bruijn & Janssen, 2017). The usual consensus within information security community is that people are the weakest link within a security infrastructure (Gratian et al., 2018; Calvin, 2018; Donalds & Osei-Bryson, 2020), one of the reasons for this is that people usually behave in ways that are at odds with what they intend to do (Shappie et al., 2020), another reason is they often fail to comply with security policies (Donalds & Osei-Bryson, 2020). There is several research on the role of human factors, where these articles have researched associations between human factors and cybersecurity and exploring the role of human factors as a variable to be considered within cybersecurity (Shappie et al., 2020; Nifakos et al., 2021; Calvin, 2018; Gratian et al., 2018). Nonetheless, there is no detailed finding that seems to inform security awareness practitioners on how they can motivate positive security behaviours and what factors to consider when developing an awareness campaign. Security awareness practitioners are security professionals who create and deliver cyber awareness programs as part of their job, to promote, educate and motivate adoption of security best practices and technologies (Haney & Lutters, 2018).

Blythe et al (2015) suggested as future research a move away from information security policies as a yard stick for compliance but to focus on targeting specific security behaviours, so there is a need to understand what cyber security behaviours are considered when developing a security awareness campaign.

The ability in Identifying key human behaviours or organisational motivators will be a starting block in understanding how to resolve or manage the barriers that stop the effectiveness of security awareness with employees. Once these barriers are understood, then the quality of the training given to employees will be a key factor to changing their risky cybersecurity behaviours into adopting a corrective behaviour (Ergen et al., 2021).

1.1 Research Question

Cybersecurity awareness program, for the purpose of this study is defined as courses, instructions or guidelines that reinforce the company's acceptable usage policies (Reeves et al., 2021). To avoid a security awareness program from being poorly received (Reeves et al., 2021) there must be an understanding of what deterrent factors and user perception exist. Reeves et al (2021) identified that employees' perceptions of security awareness programs correlate with previous experiences, the behaviours of others and the structure of the organisation.

Prior research has concentrated on barriers and security behaviours. Haney & Lutters (2018), as an example, have tried to address negative perceptions of cybersecurity using cybersecurity advocates. They define advocates as security professionals who attempt to encourage and facilitate good security behaviours in parallel with their main jobs. In their paper the authors attempted to answer how to overcome the negative perceptions of employees that security 'is scary, confusing and dull' (Haney & Lutters 2018, p. 411). However, less attention seems to have been given to exploring how to motivate cybersecurity awareness from the perspective of those who create and deliver these cyber awareness programs.

To address this gap, the purpose of this study is to explore from a security awareness practitioner's point of view the motivative factors used when creating and delivering their cybersecurity awareness and training programs.

Therefore, this study aims to address the following research question*:*

(Q1) What factors do security awareness practitioners use to motivate cybersecurity awareness.

1.2 Delimitation

The purpose of this study is exploring the perspective and the view of the security awareness practitioner, with the aim of addressing the research question identified in section 1.1 above.

The types of Information security policies or how they are formulated will not be investigated. It is seen as part of the guidelines that make up cybersecurity awareness.

The contents of a cybersecurity awareness program will also not be investigated.

The focus will be on how security awareness practitioners motivate.

1.3 Disposition

The rest of this thesis study is structured as follow. In the next chapter existing literature on cybersecurity awareness is reviewed and concepts identified. Chapter 3 will outline the research methods, the rationale for choosing an explorative case study, description of the case study and the data collection and analysis methods. Chapter 4 details the findings of the data analysis with Chapter 5 discussing the findings in terms of theoretical comparison with implications of the findings and directions for further research. Lastly, the study is concluded in Chapter 6.

2. Theoretical Background

This chapter explores existing literature and presents a discussion in terms of the concepts for the research topic and set the scene for the reader in understanding the topic. The chapter will also discuss the motivation theoretical framework which will be drawn on to guide the data collection, data analysis and interpretation of the collected data.

2.1 Related research

Previous literature has widely discussed human factors and cybersecurity behaviours influences on cybersecurity awareness, or the effects that cybersecurity awareness over behaviours (Alghamdi, 2021). Employees main objective is to complete a task, if security controls in place impede or slow down this objective, then the employee will see this as a barrier and circumvent the process. This phenomenon is perceived barrier which is what an employee deems inconvenient and the cost of them carrying out cybersecurity tasks (Alghamdi, 2021). This is in line with Calvin (2018) who noted that if employees are frustrated to the extent that they believe that performing a behaviour is negative then there would be a disagreeable attitude from that employee. Blythe et al (2015), called this a response cost in which employee's security behaviour is determined by the degree to which it impacts on their job productivity.

Human factor are human errors that cause a security incident error (Gratian et al., 2018). Calvin, (2018) describes human factors as human interactions and practices within an information system environment. Behaviours in terms of security compliance continues to be a challenge as identified by Donalds and Osei-Bryson (2020) that individuals' malicious, negligent, or unintentional actions is listed as the top cause of security incident. The explanation of behaviours within the research papers have been grounded on the theory of planned behaviour (TPB) and protection motivation theory (PMT) (Ergen et al., 2021; Blythe et al., 2015; Alghamdi, 2021; Calvin, 2018). Carelessness or negligence rather than malicious intent is the main cause of human enabled data breaches (Nifakos et al., 2021). Employees' resist compliance due to human factors such as time pressure, high workload and finding quicker way of completing a task (Calvin, 2018).

In Alghamdi (2021) case study, he noted that 51% of the respondents regarded the threat associated with cybersecurity awareness as significant. Restrictive organisational policies would be viewed by some as unnecessarily constraining (Donalds & Osei-Bryson, 2020), this is not helped by existing cybersecurity awareness training that are restrictive in scope as they fail to modify employee security behaviours (Calvin, 2018). In organisations where security resources are usually under resourced, engaging in a detailed cyber security awareness program with employees might prove to be a wish list, rather, what it ends up being is a compliance tick box exercise where computer-based training is an annual exercise.

Companies need to move away from the traditional security training and awareness initiatives in the form of an annual computer-based training and move towards implementing a more transformative based training (Alshaikh, 2020).

2.2 Cybersecurity awareness programs

Cybersecurity is an interdisciplinary multidimensional global phenomenon (de Bruijn & Janssen, 2017). A cybersecurity breach can range from low to limited impact, the stealing and manipulation of data, or even taking over control of systems and causing harm to the physical world (de Bruijn & Janssen, 2017).

Whitman and Mattford (2019, p. 689) define cybersecurity as the "protection of computerised information, processing systems and the data they contain and process". This is similar to UK's National Cyber Security Centre (2021, para. 16), which defines cybersecurity as "the protection from theft or damage of devices, services and networks including the information contained within them".

Cybersecurity concerns both humans and systems as the concept of cybersecurity refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values of people regarding cybersecurity and how they manifest themselves in people's behaviour with information technologies (Georgiadou et al., 2020). Despite the fact, that almost everybody has heard of cybersecurity, the urgency and behaviour of people do not reflect high level of awareness (de Bruijn & Janssen, 2017). The need for effective cybersecurity awareness is even now more important with the introduction of Internet of things (IoT) interwoven into everyday life and our continued dependencies on information and communication technologies.

Cybersecurity Awareness as noted by Ergen et al (2021) is the starting point to fight against cyber-attacks and can be defined as the level of knowledge employees have on the cyber threats facing their organisation, their systems and themselves. Awareness as described by Alshaikh et al (2018) involves the provision of informal training to employees to raise their awareness about risk and security.

Most breaches are the result of employee's failure to comply with the organisation's security policies (Nifakos et al., 2021). Whilst cybersecurity awareness is growing amongst senior executives, there is a need for organisations need to rethink their cybersecurity awareness strategy as cyber threats become even more sophisticated. Ergen et al., (2021) noted that cyber threats that organisations must deal with are usually difficult to detect.

It has been identified that many employees lack basic understanding of organisations information security policies and even if they do have some understanding of their organisation's policies there is no guarantee that they will comply with them (Hadlington et al., 2020). Awareness is elementary to behavioural change (Ergen et al., 2021). Organisations must invest in changing employees' behaviours to be consistent with their information security policies in a way that it becomes natural (Alshaikh, 2020) in both their corporate and personal activities. By being proactive in preparing cybersecurity awareness programs and measuring

the results, there is an opportunity to reduce existing gaps with security behaviours (Ergen et al., 2021).

The consensus in the security research field is that security and awareness should be in place to not only raise employees' awareness but also equip them with the necessary knowledge to comply with the organisation's security policies (Alshaikh et al., 2018).

Cybersecurity awareness campaign must convey a sense of importance and urgency to their audience, one way of doing this is to be open about the risks and what is at stake (Haney & Lutters, 2018) as well as advocating empowerment of people to foster the belief in one's ability to manage or control a situation. Context within cybersecurity awareness is important, one size fit all approach must not be taken. Whoever is responsible for the awareness program must ensure that the operational environment of their audience is considered ensuring that technology, roles, constraints, and goals are taken into consideration (Haney & Lutters, 2018). Having context awareness is critical to selling the security message in a manner that the audience understands and cares about (Haney & Lutters, 2018).

Cybersecurity awareness programs should not just concentrate on the organisation but should also touch on personal environment, it is important that security awareness programs should include reasons for why people should follow security guidelines and rouse feelings of wellbeing, rationality, and logic (Haney & Lutters, 2018).

Understanding what motivates people to effect good security behaviours is paramount as this will give security awareness practitioners an understanding to evaluate if their current approach to their awareness campaign needs to be changed.

2.3 Motivation theory

Motivation is related to psychology and as noted by Ryan and Deci (2020), it is through understanding the basic psychological needs, that practitioners are better able to understand what factors alienate or encourage engagement.

Motivation is concerned about the act of intention (Ryan & Deci, 2000) and may influence a user to comply with security policy and take action to protect information assets (Menard et al., 2017) People are moved to act by different circumstances, they can be motivated because they have a vested interest in that activity (intrinsic motivation) or because they have been influenced by an external factor (extrinsic motivation), (Ryan & Deci, 2000). Motivation is an action influencer as it arouses, sustains, and directs activity (Menard et al., 2017).

Kieinginna and Kleinginna (1981) in their paper categorised a list of definitions for motivation. The description chosen for this paper is the definition by Herbert L. Petri (1981, p. 281) which defines motivation as the "concept used to describe the forces acting on or within an individual to initiate and direct behaviour".

To understand the underpinning security behaviours within information systems field, theoretical models are used to facilitate the identification of factors (Blythe et al., 2015). The

two most used theories within information systems are the Theory of Planned Behaviour (TPB) that identifies links between attitudes and behaviours and Protection Motivation Theory (PMT) a risk perception theory that explores individuals' threat, their response behaviour, and their motivation to protect themselves (Blythe et al., 2015).

2.3.1 Protection motivation theory

Protection motivation theory (PMT) is one of the most applied theories in behavioural information systems (IS) security research and has been used as a foundation for information security research (Haag et al., 2021; Posey et al., 2015). It is considered a general theory of motivation that can be used to explain individuals' actions regarding any threat (Posey et al., 2015) and can be used and applied to situations involving threats (Haag et al., 2021). PMT postulates that an individual assesses a threat when confronted with one and looks to find possible solutions (Menard et al., 2017). The most discussed components for PMT model include perceived severity, perceived vulnerability, self-efficacy, response efficacy and response cost (Posey et al., 2015; Blythe et al., 2015; Haag et al., 2021). These components have been identified by prior research as having a direct effect on behaviour (Menard et al., 2017)

Central to the PMT model is the threat appraisal and coping appraisal processes (Posey et al., 2015). Threat appraisal consists of perceived severity and perceived vulnerability and is about how individuals assess and evaluates the danger level that is presented by a cybersecurity threat (Li et al., 2019; Posey et al., 2015).

Coping appraisal, which includes self-efficacy, response costs and response efficacy, on the other hand, refers to how individuals assess their abilities to deal or cope with the threat, it is about the individual's confidence in coping with the security situation (Li et al., 2019).

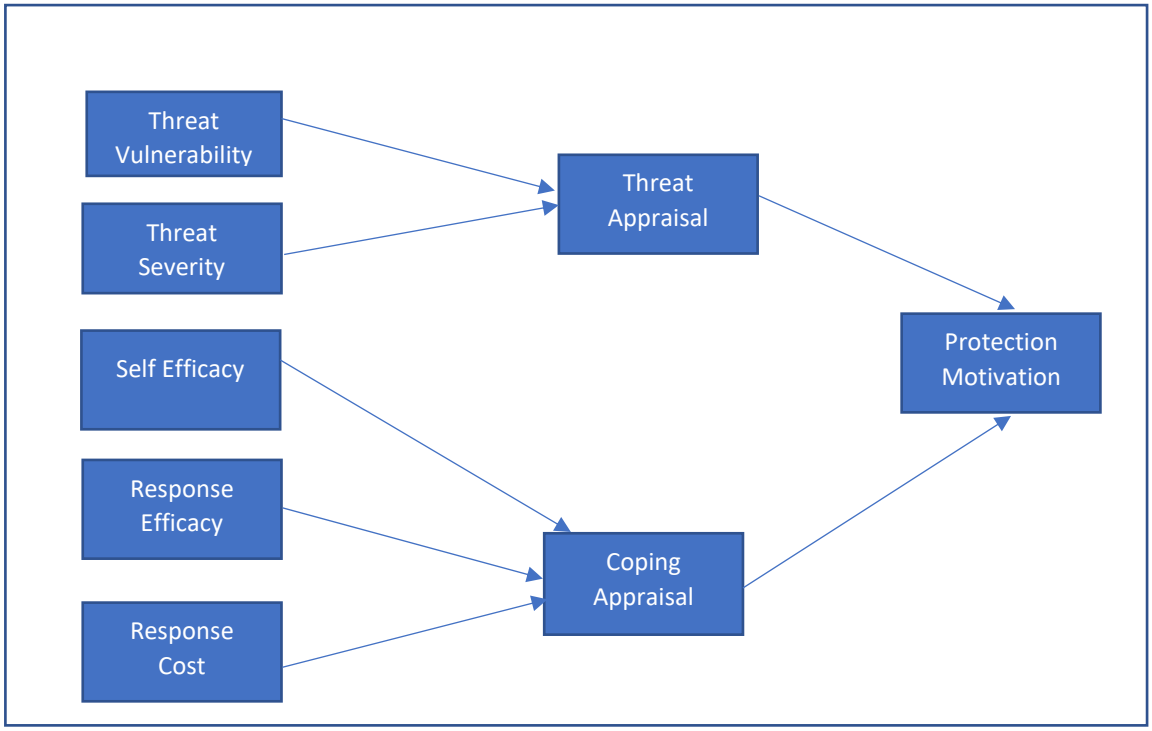


Figure 1. *Components of Protection Motivation Model (adapted from Posey et al., 2015)*

Protection motivation is made up of threat appraisal and coping appraisal. The components that make up the threat and coping appraisals are explained below.

Threat vulnerability is the degree to which individuals feel that they or their organisation is easily open to certain security threats (Posey et al., 2015).

Habits has a significant influence on whether an individual feel subjected to a particular threat (Vance et al., 2012), as the combination of unavoidable events that exacts discomfort often causes individuals to become nervous, scared, and upset (Posey et al., 2015). If individuals feel that security attacks are unlikely to happen to them then they may not engage in security awareness campaigns or good security behaviours (Blythe et al., 2015) on the other hand It is possible that when an individual feels vulnerable to security attacks this may result in displaying protective behaviour (Blythe et al., 2015). This is supported by Haag et al (2021) in their paper who identified significant impact on threat vulnerabilities on users who have had a personal experience or knew someone who had been exposed to a threat or the likelihood of them.

Threat severity is the level of seriousness of a security threat and its related consequences (Blythe et al., 2015). It is the extent to which organizational threats are perceived to be damaging and to cause harm (Posey et al., 2015). In simple terms it is the perception that an employee has on the seriousness of the threat (Menard et al., 2017).

Vance et al (2012) have found that the severity of the threat does have a positive impact on an individual's intention to comply with their organisations IS security policies. Although security breaches may or may not a have direct consequences for the individual, the breach itself may lack personal relevance (Menard et al., 2017), thereby using appeals that are individually focused is much more effective in reinforcing security behaviours rather than fear or threat focused communications.

Self-efficacy is an individual's belief that they can alleviate cybersecurity threat (Shappie et al., 2020), it is basically the belief in one's ability to make appropriate decisions when faced with a cybersecurity situation. Self- efficacy a dimension within cybersecurity (Shappie et al., 2020), has been identified by Alghamdi, (2021) and Shappie et al., (2020) as an important factor of cybersecurity awareness. It has consistently been shown within research to influence security compliance (Blythe et al., 2015). This is because it relates to personal belief in one's ability in being able to make appropriate decisions in the event of a cybersecurity event. Alghamdi, (2021) study identified that individuals with high levels of self-efficacy have positive impact on cybersecurity behaviours. This is in support of Blythe et al (2015) paper that identifies self-efficacy as an individual's belief in their ability to cope with a task, the higher the self-efficacy, the more likely to follow cybersecurity policies. This indicates that self-efficacy is a dimension of cybersecurity. Donalds and Osei-Bryson (2020), state that security self-efficacy influences an individual's cybersecurity compliance behaviours. As self-efficacy is about self-belief, this can be positively influenced into improvement through the targeting of an individual's knowledge of the organisational security behaviour as well as their belief that the knowledge will help improve cybersecurity within the organisation (Shappie et al., 2020).

Response efficacy is the perception of how well the recommended response or coping strategy addresses the threat at hand *(*Menard et al., 2017*;* Posey et al., 2015). It is the belief that a specific security behaviour will reduce a security event (Blythe et al., 2015). Employees who are committed to their organisation are more likely to engage in security awareness programs as they are willing to equip themselves with the knowledge of how to protect the company information (Posey et al., 2015).

Some researchers claim that response efficacy is the most important predictor of protection motivation, this is supported by Posey et al (2015), who in their paper were able to demonstrate that response efficacy exhibited a stronger relationship with protection motivation than the other components. Menard et al (2017) also identified in their study that response efficacy is a more important factor than self-efficacy in terms of protection motivation and that by reinforcing an individual's computer-based competence increases the individual's confidence in their ability to carry out the recommended response.

Response cost refers to the belief on the costs of performing the expected security behaviour (Blythe et al., 2015). An individual may interpret response cost in a number of forms, including

time, money, effort, inconveniences, difficulties, and potential side effects (Menard et al., 2017; Posey et al., (2015). One of the difficulties identified by Posey et al (2015) is that response costs often conflict with an individual or organizational goals, such as trying to get one's own assignment completed on time. If the individual perceives that the cost of following a security behaviour is too high, then they are unlikely to follow through with it (Blythe et al., 2015).

Individuals and organisations have a different perspective of costs for certain security compliance behaviours (Blythe et al., 2015), an individual might have multiple effective responses and evaluate the costs associated with each of the responses to select the appropriate response based on minimizing cost of performance (Menard et al., 2017).

As response cost is seen to negatively affect the adoption of security behaviours (Menard et al., 2017), as individuals consider the inconvenience of adhering to IS security policies a legitimate reason for not complying with those policies (Vance et al., 2012). It is important that individuals within the organisation are made to understand the need to perform good security behaviours despite any perceived response cost to them (Posey et al., 2015).

Posey et al (2015) identified that coping appraisal process (self-efficacy, response efficacy) is more vital to increasing protection motivation and protective actions than the threat appraisal process. Behaviour responses should be identified to design distinct IS security threat messages that are able to change perceptions of the targeted individuals.

Security awareness practitioners whilst ensuring that their awareness campaigns do cover the threats vulnerabilities and severity, should really concentrate on how they can motivate and empower the employees in identifying and dealing with a security event.

In turn, creating a culture where individuals within the organisation comply with IS security policies as part of their habit will have a positive influence on threat severity, self-efficacy, response efficacy (Vance et al., 2012).

2.4 Understanding the barriers

The Cambridge online dictionary defines a barrier as "something that prevents something else from happening or makes it more difficult".

Applying these definitions to cybersecurity awareness, implies there is a need to understand what is 'that thing' that is preventing or encouraging a certain behaviour. What factors cause these barriers need to be understood, to counter them using different motivating factors.

People have the tendency to select only those parts of a message that they want to hear (de Bruijn & Janssen, 2017), there is a belief of their ability in engaging in a particular way and are not usually worried about cybersecurity unless they have been previously affected. This self-interest is both a barrier and motivator. Haney and Lutters (2018) identified that when a threat was personally relatable the security behaviours were better, this shows that individuals who

develop feelings of ownership for their work-related data are more likely to engage in positive behaviours (Raddatz et al., 2020).

The perceptions of cybersecurity that people have is also another factor, people choose to accept security advice based on trustworthiness (Haney & Lutters, 2018). Unfortunately, sensationalised media portrayals of cyber incidents of big corporations, has a hand in giving a false sense of security that they or their organisations will not be targeted as in their opinion only a certain type of organisation is targeted. It has not helped that within the cybersecurity realm, security professionals are seen as negative, due to the history of security professionals having regularly expressed the belief that users are unable to comprehend and practice good security behaviours (Haney & Lutters, 2018). There is also a weariness towards security when it becomes too burdensome (Haney and Lutters, 2018). Employees view rigid security measures as counterproductive as they believe it hinders their ability to be flexible in their day-to-day operations (Haney & Lutters, 2018).

Another barrier is communication, as cybersecurity has been the domain of specialists and experts who are not trained to communicate about the issues (de Bruijn & Janssen, 2017), these specialists often use technical terms which in turn fails to get the right message across. De Bruijn and Janssen (2017) identified that management techniques are used to over dramatize and oversimplify cybersecurity risks, these techniques are applied when security policies are written. A consequence of this approach is that employees within an organisation see security policies as inefficient or counter-productive to them attaining their business objectives thereby making them a barrier.

Mandating or forcing users to complete organisational annual security awareness program is another reason that drives user lack of interest in adopting good security behaviours (Haney & Lutters, 2018). These annual computer-based training do not encourage good security behaviours but rather reinforces lack of apathy as the aim of the training is not to change behaviour but rather to meet a regulatory obligation.

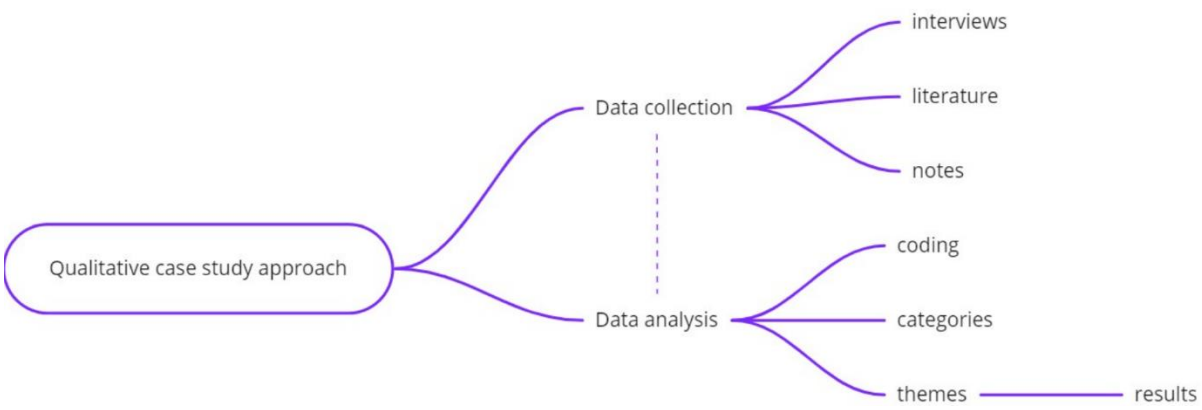
A real challenge within the current environment is that cybersecurity comes at a price and complete protection is never possible (de Bruijn & Janssen, 2017). If a complex topic such as cybersecurity is made relevant to people's immediate living environment, then they will readily recognize the urgent need to address cybersecurity (de Bruijn & Janssen, 2017), within their own personal and professional space.

3. Research Method

The purpose of this study was to explore from a security awareness practitioner's point of view of what factors they use to motivate cybersecurity awareness when creating and delivering their cybersecurity awareness and training programs. An exploratory qualitative research approach was adopted within this study to gain an in depth understanding of the research question.

Research is about collecting, analysing, and interpreting data to expand or increase our understanding of a particular subject (Leedy & Ormrod, 2015, p.2-3.). It is not just about gathering information but a systematic process of information collation and dissemination. This systematic approach must have an order to it.

Figure 2. Overview of research method.



The choices of the research method have been guided by the research question and access to data set. The criteria for conducting and evaluating the study is presented through the research methodology, research design, data collection and analysis methods and the justifications for using them. Firstly, qualitative research and the rationale for using this research method is presented, followed by the case study description and introduction to case participants. Then the study plan and design are introduced with the remaining sections detailing the data collection and the data analysis methods. A diagrammatic overview is presented in Figure 2.

3.1 Research methodology

There are several research methodologies available to researchers to help them in the research of their chosen topic, the most common two research approaches used is the quantitative and

qualitative research methods. Qualitative research has been steadily becoming used more within information systems (IS) community and now more acceptable within the mainstream IS literature (Sarker et al., 2013). Qualitative research provides researchers unique ways in investigating unknown or complicated phenomenon (Hill et al., 1997).

Quantitative research methods are usually likely to be confirmatory, objective, deductive and predictive whilst qualitative research methods are usually exploratory, subjective, inductive, descriptive, and interpretive (Chenail, 2011). This study used the qualitative research exploratory method as it aimed to explore an unknown phenomenon and generate data relevant to the research question which will be interpreted using data analysis. This study falls under the exploratory approach and aimed to generate data relevant to the research question (Blythe et al., 2015) and is not based on testing an existing theory.

Whilst quantitative research deals with the notion of realist and qualitative is constructivist, both these paradigms must deal with real phenomena and must ascribe meaning to their data (Fielding & Schreier, 2001), this means that both quantitative and qualitative research must meet a set of criteria. For qualitative research these criteria include, clarification and justification of the research, what procedural rigour have been undertaken, what sampling techniques have been represented, and how the data collected been interpreted (Kitto et al., 2008). For quantitative research, these criteria include a numerical and reliable outcome, using a structured research method and standardised statistical methods.

Qualitative research helps to define what is important in terms of what needs to be studied (Leedy & Ormrod, 2015, p. 228) and can be defined as the systematic collection, ordering, description, and interpretation of data (Kitto et al., 2008) that has been generated from several sources such as interviews, observations, focus groups and documents. Qualitative research explores the behaviour, processes of interaction, and the meanings, values, and experiences of participants (Kitto et al., 2008).

Goldkuhl (2019) propose that when undertaking a qualitative inquiry, one should consider the possible data sources and to select and design a suitable method to capture the data. Whilst qualitative research is quite different from quantitative research, it presents some challenges as it does require significant preparation and planning, in terms of understanding previous research and reading through substantial amounts of data (Leedy & Ormrod, 2015, p. 229) to identify what will be suitable for one's research.

Hill et al (1997) suggests that qualitative approaches enable exploration of the phenomenon as it occurs and enables researchers to investigate in depth. For this research study, qualitative method was deemed most suitable as a deeper perspective is needed and allowed the participants experiences and perceptions to be drawn out through the interview process.

Another reason for using qualitative research, is the nature of the qualitative research design, which is iterative in nature, allowed for adjustments to be made during the research (Chenail, 2011). This gave the space within this study in expanding as there is the opportunity to move back and forth between the data collection and data analysis stages (Leedy & Ormrod, 2015, p. 229).

A summary of the research methodology is given in the below table.

Table 1. *Research methodology summary*

Function	*Description*
Aim of study	*The aim of the study is to understand how security awareness practitioners motivate cybersecurity awareness*
Methodology	*Explorative qualitative approach*
Research method	*Case study of individuals*
Phenomenon	*Motivating factors in cybersecurity awareness*
Unit of analysis	*Individual security awareness practitioners*
Participant's selection	*Based on defined criteria*
Data sources	*Existing literature review* *Semi-structured interviews* *Discussions* *Training documents*
Data analysis	*Interpretation through reading, transcribing interviews, highlighting identified concepts, and grouping of concepts*

3.2 Case study approach

Case study research is widely used for exploration and hypothesis generation (Dubé and Paré 2003). The 'case' in a case study is a key component and can be defined as the phenomenon that needs to be studied and could be individuals, groups, organisations, or projects (Yin, 2018, p. 29-31). Case study research can be defined as closely investigating in-depth, one or more contemporary real-world social settings situation (Goldkuhl, 2019). This is like Yin (2018, p. 15) who defines case study as an "empirical method that investigates within a real world a contemporary phenomenon in depth". Choosing a case study as the research method is dependent on three conditions. First is the form of the research question, the second is the researcher having no control over the phenomenon being studied and lastly the study should focus on current contemporary events rather than historical events (Yin, 2018, p. 9-11).

For the first condition, the research question for this study focused on "what question" which is exploratory in terms of identifying what factors are used to motivate cybersecurity awareness, another reason for it being exploratory is that it is currently unknown how motivation is carried out. Although Yin (2018, p. 10-11) suggests that case study research should generally be used for 'how' and 'why' questions, he also states that for an exploratory study any of the five research methods (experiment, survey, archival analysis, history, and case study) can be used. This is supported by Sarker et al (2013) where the authors identified that a significant proportion (26%) of papers they reviewed addressed 'what' questions in their

research paper. Dubé and Paré (2003) are also in support as they identified that 'what' questions were most frequently used in exploratory case research. Case study approach was therefore chosen as the method to use within this study.

For the second condition, case study is carried out to understand an issue, by studying a particular individual(s), program, or event over a period (Leedy & Ormrod, 2015, p. 231). It is used to give clarity when the boundaries between the phenomenon and context may not be clear (Yin, 2018, p. 15). Within this study, the aim was to understand the experiences of the cybersecurity practitioners who are responsible for the security awareness program, within their organisation in motivating their employee's cybersecurity awareness; through the investigating of the experiences, of each individual and the meaning they have associated to these experiences.

Lastly, Yin (2018, p. 12) states that case studies are used for flowing interpretation of events using a variety of evidence, this study is investigating the concept of motivation and cybersecurity awareness and involved data sources such as interviews, related literature, and discussions to collect, analyse and conclude based on the data.

The research question is key when determining the case study as how the problem has been created has a direct impact on how the case study is designed, how the data is collected and how it is analysed (Sarker et al., 2013).

It is also important that when using a case study, there is detailed preparation that has been undertaken and any bias is limited, Yin (2018, p. 20) states that methodical procedures undertaken must be highlighted, and there must be transparency in limiting or eliminating any biases.

3.3 Case study participants selection

The 'case' in this case study research will be individuals. The research question has been used as a tool used in identifying what type of access is required of the participant case study. As sampling strategies also apply to qualitative research (Sarker et al., 2013), purposive sampling has been used to ensure maximum information is extracted from the selected participants. Purposive sampling is choosing participants for a particular purpose (Leedy & Ormrod, 2015, p. 178), for the context of this study the participants will be security practitioners and the particular purpose is to understand from their perspective what motivating factors they use to motivate cybersecurity awareness. Yin (2018, p. 105) advocates the screening of candidates as a preparatory step for the case study selection but feels that the use of the term 'sample' can mislead the reader into thinking that the case is from a large population. For clarification purposes, the participants were chosen based on the following criteria, 1) can be in full or part time employment 2) must be involved in either creating content for cybersecurity awareness campaigns or responsible for an awareness campaign 3) have at least a minimum of 2 years level of experience within the information security and data protection area.

An In-depth interview with four security practitioners was solicited through LinkedIn contacts. The number of participants is in line with qualitative research approach followed by other researchers such as Alshaikh (2020) whose study was based on interviews with three participants and Alshaikh et al (2018) study that carried out interviews with six participants.

The in-depth interview was conducted through semi-structured open-ended questions such as that followed by (Blythe et al., 2015, Alshaikh et al., 2018, Haney & Lutters, 2018; Reeves et al 2021). In-depth open- ended questions reveals the participants perspective on the topic of research (Ergen et al.,2018). The open- ended questions designed for this study by the researcher, used the theory to formulate the questions ensuring that they are aligned to the research question. As an example, questions e- f were based on the concept of cybersecurity awareness programs to extract an understanding of the awareness program contents.

The interviews were carried out mainly through online session interviews. Any required follow-up questions were sought via email. The length of the interview was aimed between 45mins to an hour for each participant, but this was dependent on the availability of the participant.

3.4 Case study design

The research was based on an explorative case study approach on selected individuals, it is explorative because there is not one single set of outcomes, and an in-depth view is sought to capture the perspective of each individual participant. The aim is to answer the research question of "what factors security awareness practitioners use to motivate" cybersecurity awareness. The question helped to determine what data collection and data analysis approach used.

Research design is a blueprint of how the case study will be undertaken (Yin, 2018 p. 26) and the design of research methods within a research study is dependent on the purpose of the study (Goldkuhl, 2019). By following a systematic approach, this can make a case study design easier to undertake (Yin, 2018, p. 23). One way of mitigating the difficulties of a case study is to avoid the concern about the lack of rigour (Hill et al., 1997; Yin, 2018, p. 18), in addition to the lack of rigour concern, Yin (2018, p. 18-21) identified other concerns such as the amount of effort required and transparency of the research scope.

The scope of the research can be managed by using theory or existing literature as an initial guide for the design and data collection (Walsham, 2006), the theory related to motivation within information systems has been reviewed as part of the related literature research in chapter 2. This will act as a guide in developing the interview questionnaire for data collection.

The challenge of choosing an appropriate criterion for rigour is one that was experienced as it was difficult to identify which systematic approach was best to use. As this is an exploratory study, Yin's (2018, p. 43) criterion of validity and reliability was applied. A summary of how these criterions have been applied within this study has been listed in table 2.

Table 2. *Case study design criteria (adapted and adjusted from Yin, 2018, p. 43-47)*

Criteria	*Tactics*	*Application in study*
Construct validity	*Multiple sources of evidence* *Draft report review*	*Interviews, training document, discussions* *Get at least one participant to review interview transcript*
Internal validity	*Not applicable for exploratory studies*	*Not applicable*
External validity	*Using theory in single case studies*	*Using theory identified in related literature research to define concepts*
Reliability	*Develop case study database* *Develop interview protocol guide*	*Use researcher notes, documents, transcripts*

For this study, a single exploratory case study has been chosen because it fits the common rationale. The objective of the common case is to capture circumstances and conditions of an everyday situation (Yin, 2018, p. 50), security awareness is a common topic within information security and the objective of this study is to capture how security practitioners motivate cybersecurity awareness. The other single case rationales (Yin, 2018, p. 47-53) have not been deemed suitable as the study is not testing existing theory due to it being exploratory and will look at the data to aid in understanding motivating cybersecurity awareness. The topic of cybersecurity awareness is not an extreme or unusual case, additionally this study is also not revelatory as cybersecurity awareness is not an inaccessible phenomenon and lastly the case cannot be studied at two or more different points in time due to the time frame of the thesis completion date, so can't be classed as longitudinal.

3.5 Data collection

Case study research can include multiple methods for collecting data (Goldkuhl, 2019) and researchers need consider how to extract and capture the data. Yin (2018, p. 114) presents six ways to collect data in case study research: documentation, archival records, interviews, direct observation, participant observation, and physical artifacts. As a preparation technique, researchers should have some knowledge on how to collect data using these various sources as Goldkuhl (2019) suggests that how data is generated should be based on what the researchers know about the available data generation methods and the respective capacities.

Interviews were the primary data source. This follows the trend of some of the articles used for the related research section in this study, who have used interviews as their main data collection method (Reeves et al., 2021; Alshaikh, 2020; Alshaihk et al., 2018; Blythe et al., 2015).

This fits into the findings by Sarker et al (2013) who identified that Interviews were found to be the most common technique of qualitative data collection.

Supporting data sources that was used for this study included documentation from participants such as security policies and awareness contents which I was shown. Informal discussions, literature review and researcher notes, were also data sources that were used. These data sources have been chosen for their accessibility. Sarker et al (2013) encourage the use of multiple data sources and collection methods, which is in line with Yin (2018, p.113), who also endorses the use of more than one data collection method to meet the construct validity and reliability of the case study. Whilst direct observation and participant observations are also sources of data collection, these have been deemed unsuitable for this study as it is time consuming, and participants are in different location areas from the researcher which makes it difficult to meet and observe.

To ensure the reliability of the study, a case study database was also created to preserve all collected data. Information from participants, interview transcripts, analysed data have been stored in this database.

The aim of a data collection is for relevant data to be collected and used in answering the research question. The theory section in chapter 2 has been used as an initial guide for the design and data collection in the following ways. Section 2.2 (cybersecurity awareness programs) was used to create questions for theme 1 in the interview guide to determine the purpose of the awareness programs. Section 2.3.1 (protection motivation theory) and section 2.4 (understanding the barriers) were used to develop theme 2 questions to understand what components of the PMT are considered when developing an awareness program. And what barriers they face. The Interview protocol guide can be found in Appendix A.

3.5.1 Primary data source: Interviews

Dubé and Paré (2003) observed that a vast majority of research articles used interviews as the primary source of data collection method, this supports Sarker et al (2013) observations that found Interviews to be the most common technique used for qualitative data collection.

An interview helps the researcher through dialog, guide the participants to express their reflected knowledge and perspective (Goldkuhl, 2019). To get viable data from interviews, two things must happen; the researcher must pose relevant and intelligible questions and the participant must be willing and able to provide the answer (Goldkuhl, 2019).

To ensure viable data is received, an interview guide was created to ensure consistency based on the research question. In preparing the interview guide, ‘how’ or ‘what’ have been used to focus the questions.

To start the data collection process, the researcher identified practitioners who are involved in creating content for cybersecurity awareness campaigns from LinkedIn contacts. Invitations for interview was distributed using email and LinkedIn mail to the selected practitioners.

The invitation included a brief of the study which provided clear explanation of the study aim. Five participants from different business sectors responded with their interest but only four were available for interviews within the required time frame. See Table 3 for participants details. The dates, times and medium of interviews were agreed with the participants. This is in line with Goldkuhl (2019) who suggests that the situation in which the interview is to take place also needs to be arranged by the researcher and separated from the participants everyday work reality (Goldkuhl, 2019).

The interviews took place between the 18/03/22 to 31/03/22 and was conducted virtually using Zoom and Google meet.

The interviews consisted of semi-structured questions that were aimed at exploring how these practitioners motivate or have motivated cybersecurity awareness in their current or past organisations.

As the researcher can interpret and assess the given answers and decide on whether there is a need to ask a follow-on question or move to the next question (Goldkuhl, 2019). The interview guide ensured that the researcher did not go off track on the line of inquiry.

The questions were sent to the participants before the interviews, with the interviews lasting an average of 43 minutes (min:25, max:54). The participants consented to having the interviews recorded and to keep to GDPR rules, any personal identifiable data has been removed or anonymised within the transcripts. The names of the practitioners were replaced with a participant ID number.

The interview started with an introduction of the study and confirmation of consent of participants to record the interview. Then the interview guide was used in asking relevant probing questions. During the interviews, the researcher also took notes. Taking particular care not to repeat a question, that had already been answered in a previous non-related question.

Table 3. Study participant's background details

ID	*Role*	*Sector*	*Experience (years)*
Part1	*Information security officer*	*Charity*	*16+*
Part2	*Information security manager*	*Information security consultancy*	*10+*
Part3	*Cybersecurity programme manager*	*Government*	*6+*
Part4	*Data Protection Officer*	*Transport*	*8+*

The recorded responses were transcribed in preparation for analysing. Recording and transcribing of collected data is often seen as essential for ensuring rigor of the study as it can increase the credibility and auditability of the study (Sarker et al., 2013). For each recorded response, transcribing started 24hrs after the interview.

To meet the construct validity criteria, participants were given the option of having a copy of the transcript. None wanted a copy except participant 1 who requested a copy to be sent.

3.6 Data Analysis

Qualitative research is associated with different data analysis approaches (Sarker et al., 2013). Analysing data for case study research can be a challenge as it is the least developed area of carrying out case studies due to there being few guidelines (Yin, 2018, p. 165)

Sarker et al (2013) defines data analysis as the processing of empirical material collected to make contribution claims. Collected data were compared and analysed from the different interview transcripts and worked inductively through the data using content analysis method.

Content analysis method is described by Alahmari and Duncan (2021) as the analytical process of categorising qualitative textual data from interviews into categories or themes. This study used an inductive content analysis approach as the motivating factors for cybersecurity awareness is a less known phenomenon. The three stages of content analysis include 1) preparation, 2) organisation and 3) reporting (Alahmari & Duncan, 2021)

For the preparation stage, each recorded audio was downloaded from the recording tool and then labelled and stored. The interviews were transcribed from audio recording, this resulted in approximately forty-three pages in total. The recorded files were first downloaded to a textual file using the functionality within the recorder. Then the file was further worked on to ensure that the transcript match the audio recording. During this process, any personal or company information was redacted to meet confidentiality agreement.

Transcribing each recorded file averaged about four hours and totalled about seventeen hours overall. Once the files were fully transcribed, they were re-read a few times to get a general understanding of the participants view.

For the organisation stage, the transcript text was divided into units to develop descriptive codes that reflect the data in a different way (Erlingsson & Brysiewicz, 2017). Codes that had meaning to the research question were used to make it easier to break down the data. It also helped to link the connections between the different interview transcripts and lead to identifying themes that appear to deal with the same topic. Coding all the transcripts took a week to complete.

The first transcribed interview was the starting point in identifying codes, and this continued with the remaining interview data. The themes were identified after all the transcripts had been coded. Microsoft word was used as the tool with a two-column table created in which the transcribed data was pasted. After going through the transcribed documents looking for texts relevant to the research question, a code that will help identify the text later was put in the second column. This process was repeated for the remaining three transcribed document.

Table 4. Text units, coding scheme and categories

Text units	*Codes*	*Categories*
our internal pages where we share information, so we'll have it'll be like news feeds and stuff like that	*Forms of delivery*	*Types of engagement techniques*
you could get engagement that way by actually going to see the people	*Engagement*	
you engage in a group of champions to start selling the right message to the right people	*Champion*	
People have fed back really good stuff	*Feedback*	*Emotional and personal*
it's take it out of the work environment as well, make it personal	*Personal*	
there are also those emotional societal drivers that hooks and things that we use.	*Emotion*	
So, I need to have a chat with the exec to say, the exec that is responsible for that area and say. This is what I'm doing, this is how I need your help there to achieve that.	*Leadership*	*Leadership*
I think if the leadership of the functional area is brought into it and they are passing those messages down. it's proving to be far more powerful than if the CISO starts pushing out messaging	*Buy in*	
make the password long, and you then use technical controls to support and augment security around people	*Technical controls*	*Controlling factors*
So it's basically reducing the load on the people.	*Reducing load*	
It is difficult to know if there would have been more incidents without the campaigns	*Measures*	

For the reporting stage, the resulting codes from each file were then compared against each other using an excel spreadsheet. To ensure consistency, codes were aligned, duplicates were removed, and class of codes sorted into categories. An example of text units, coding and categorisation is given in Table 4.

The next chapter will present the findings of the data analysis.

4. Findings

The purpose of this study is to investigate the factors security awareness practitioners use to motivate cybersecurity awareness and this chapter present the findings of the analysis.

Four themes emerged from the data analysis which is presented in Table 5. All participants had similar perceptions, however there were some differences which will be discussed together in each section.

Table 5. Emerged themes

Theme	*Brief description*
Using different engaging techniques	*How the content and cyber awareness campaigns are delivered and communicated*
Making it personal and relatable	*Connecting the cyber awareness campaigns to personal circumstances*
Utilising leadership commitment	*The influence of senior executives and managers in supporting the awareness campaigns*
Embracing technical controls	*The use of technical controls to reduce the technical load on employees*

4.1 Theme 1: Using different engaging techniques

A common trend that all the participants agreed on, was how the cybersecurity awareness programs were delivered. The techniques used to engage people need to be much more than the normal computer-based training. And participants have used a variety of techniques to motivate. Whilst participants acknowledged that they must deliver mandatory training as part of compliance, they also try to make awareness more entertaining and funkier. For instance, one participant, stated *"We also try to make the cyber cultural awareness program quite fun and funky. It's got a sort of fun and funky feel to it. Which kind of makes it slightly less dry I guess for people" (Part3).* Another participant also agreed that the awareness programs should be more entertaining and more interesting for the users.

Content: on discussion on what context is used to form the awareness campaigns, the threats (threat vulnerability) that the organisation faces were mentioned as topics used to motivate awareness. All participants interviewed have based their awareness contents on the current threats such as phishing emails and social engineering. And they equip their users with the knowledge on how to identify these threats through the awareness content. As indicated by one participant "*knowledge is about actually arming ourselves against what the threats are for information security. So, knowledge, do you know how to spot a phishing email? Do you know what social engineering is? How do we report these sorts of things?". (Part1)*

Specific cybersecurity awareness content for different groups has been used as a motivating factor with some participants agreeing that it should be targeted.

"In terms of types of training, it takes place across different levels. So, we deliver techniques, sometimes it's even technical training to service desks to say, this is how you use removal requests, but it's also to the exec to say, right, we have these controls in place here, and this is what we're doing. This is how you could be targeted, and we create those same campaigns as well". (Part1)

From another participant's perspective, whilst they agree that a targeted approach model should be used in terms of the awareness, they use an all-style fit all as currently due to the organisation size they have not been able to understand the risk factors of certain department groups. *"I would say that the biggest barrier that we've had is that the cyber risks that we face are different depending on where you sit in the organisation and we have not been able to size and dice our contact data so that we can do the, you know, so that we can do sort of targeted campaigns according to the way, you sit in the organisation". (Part3)*

Communication: was a barrier identified in chapter 2, all participants saw communication as a key aspect in engaging motivation. *"You've got to communicate with the staff teams. Because if you don't communicate, if you just change something without communicating to them, why you've done it. They're just gonna go, I'm not doing that. That's dumb. So, you need to communicate". (Part2)*

Another participant manages communication through a raft of different sources *"We also have sort of cascading, communications that go out where the sort of particular brand to draw attention to it. Well, there'll be features around cyber and other people's newsletters will then link back to those pages". (Part3)*

Being able to sell the security message is important to get people on board, two participants were keen on using champions as a means of communicating the message at different levels. They feel that engaging in a group of champions, can help to start selling the right message to their audience. Champions are seen as people within the organisation who are willing to promote cybersecurity awareness. Using champions will help bridge the gap between technical and non-technical audiences.

Having used a variety of ways to motivate cybersecurity awareness one participant agrees that using champions can motivate engagement. *"I think we should go down the champion route because this can be the only way to get there. I think in this organisation…we seem to have tried everything else and I think we need to go down the champions route and start selling it at and doing a couple of events about the sites and just to start getting that message out there again. You know this is critical really for both the business and individuals". (Part4)*

The other participant is willing to work with another department to further motivate engagement *"in terms of champions, technology services or IT …., they are setting up their own IT champions. I'm hoping that security can piggyback on that (Part1)*

Platforms of delivery: there are several platforms that participants use as factors to pique interest and motivate engagement. Most participants use emails, internet articles and webinars. Road shows and events seem to be a method that will be reinstated as the pandemic restrictions are being lifted. As one participant said *"We're also doing road shows. We've got sites across the UK that we have never seen. So, we're also doing road shows, where we will turn up in locations or wherever and say right information security is here for the day. We've got some materials that we can present to you. If you do want that, if you do want to learn a bit more come and see us, we will add a 15-minute drop in sessions type of thing (Part1)*

Previous engagement techniques would have been things like posters at coffee machines and around office walls. This is seen as no longer relevant as there are less people in the office space. And the pandemic has seen a lot of the cybersecurity awareness programs shifting online. Participants have noted that previously, they have used events and road shows to motivate. For instance one participant noted *"In the past they've been like, for example, kind of road shows style, things have been done so like, you know, people would be standing in the reception areas with some freebies, giveaways, that kind of thing, raising awareness around cyber obviously the homeworking has sort of stopped that but that would have been one thing we would have done and they were always gone down very well with people and I guess, sort of videos, people quite like". (Part3)*

Other online forms such as social media type have been implemented by others to deliver cybersecurity awareness programs, such as one participant who uses a variety of mediums including social media. *"So, it's face to face, it's webinars, it's blogs, it's social media posts. It's over LME, computer-based training. We have a thing called workplace that we use here, which is like a social media, just for the organisation type people. And, and as part of workplace, then we can push out information security posts along the lines of and, you know, on this day type posts that are rather than to information security". (Part1)*

An interesting motivating factor that two participants discussed was the use of games to push the message. In one participant's company they've developed a character. This character occurs through all the threads of the cybersecurity awareness program. Thereby giving a sense of continuity to users. Using real life experiences seem to pique individuals' belief, in their ability to be able to make decisions (self-efficacy) when faced with security event such as a phishing email as an example.

"So the last training we had was using real life examples of emails that have been landed and then asking people to spot all the clues in each email that could have told you that this was a phishing attempt. So it's a kind of game. Although it was a mandatory training, if you like. People have fed back really good stuff on that one. They really liked it because it was quite challenging, and it was real. I mean it was based on real life". (Part3)

This was further collaborated by another participant who also held a similar exercise, where they broke their trainees into two teams and got them to think about how to create a phishing campaign, what they put in a phishing campaign why they would put that in there, what lures they would use to try and get the people they were attacking to click on the links. Having this type of competing game works as a motivating factor.

4.2 Theme 2: Making it personal and relatable

In chapter 2, it was noted that cybersecurity awareness programs should not just concentrate on the organisation but should also touch on personal environment. Most of the participants agreed with this. Staff need the awareness that they are also a security control that they have to consider themselves as guardians of the data that they are processing, guardians of the environment within which they work.

Personal and relatable: by making the awareness programs personal and relatable there is a higher chance of engagement and reduced chance of people switching off. One participant personally tries to always relate any cybersecurity awareness program to something everybody will be familiar with.

Another participant has made cybersecurity awareness relatable by recommending different tools and strategies that users can employ in their personal life. This participant has also used emotional drivers as a motivational factor "*We also have the emotions driver or the emotional hook for people in their personal life. Because our awareness material, isn't just about protecting the company, it's about protection, our clients, and our colleagues, as well. And so, we talk to them about how they report phishing emails outside of work as well and tools and tricks such as using password managers and setting up multifactor authentication and to the wider colleague base as well". (Part1)*

The participants' motivation is to get across the security message, to everyone why security is important. As noted by one participant "It's *trying to raise the awareness across the board, it's trying to get people to understand within a business that security is only as good as that person, at that point in time". (Part2)*

Security needs to become front and centre of what people do rather that it being seen as a barrier to doing business. As one participant stated *"Make them think about security in how it affects them in their personal life because, the principles of cybersecurity that we're trying to instil in everybody within a corporate environment are the same ones that they should instil in their personal lives to protect their personal environment. And their personal environment is their family. Their spouse. Their children, the bank account. It's the same principles". (Part2)*

Having informal sessions rather formal classroom settings seem to be advocated by one participant who thinks that it's easier to relate to people when interest is shown. He states, *"talk to people, engage with people, share stories with them about stuff and be interested in them and find out about them and ask them whether or not they are aware of all the accounts that their children are accessing". (Part2)*

In one participant's organisation whilst there have been discussions on bringing some personal perspective into the cybersecurity awareness program. They have been cautious as they are being mindful about giving out advice to people that may or not apply in their home environment. In the participant word's *"we don't make it relatable to their personal. We just stick to the purely professional. (Part3)*

Participants do feel that getting people to understand the consequences of getting security wrong can be used as a motivating factor. As one participant puts it *"I think it's more about what the consequences would be if you're shown to be negligent within the organisation is more important, I think it's one of the factors which does motivate people there". (Part3)*

Feedback: the participants also discussed how feedback can be used as a motivating factor and how they seek those negative feedback. To measure the effectiveness and build their security awareness program contents to be better for the following year.

Feedback can also be used to motivate users. Using a form of acknowledgment of the time they have spent, and their understanding of the content can also be used to motivate. One participant does this using digital certificates.

"With the data protection training a few weeks ago, it had three people in HQ on that day, come up to me. They printed off their certificates and showed me. They were happy. So, you know, we know it does work and it is positive". (Part4)

Using negative or positive feedback from users after a session has proved to be useful in measuring the effectiveness of the cybersecurity awareness content as noted by one participant *"we have those engagement surveys that help measure actually how good our awareness materials are. We typically send out our questionnaires once we've delivered specific training as well, depending on who the audience sent to that training". (Part1).* Another suggestion given for measuring effectiveness of an awareness content is to use Google analytics to track response on people's clicks on awareness courses they have completed or policies that they have read.

Celebrating success as a motivating factor was mentioned, making people feel that they are doing well by celebrating a good practice. One participant stated that *"one of the things we do is we call out good practice, good behaviour. So for example, an early reporting of a problem that can then be literally, you know, search and destroy can be conducted immediately. You know, if someone discovers a phishing attack and they happen to log on at 5am in the morning and report it, we can have that search and destroy done before anyone before the vast majority, people have logged in. Thus they saved the whole company a whole lot of problems. So if something like that happens, we tend to call that out. We try to at least". (Part3)*

Another participant wants to instigate celebrating events like cyber security day and data protection day.

4.3 Theme 3: Utilising leadership commitment

Participants discussed how leadership buy in is an important motivating factor and they have used this to their advantage in pushing engagement.

As noted by one participant, cybersecurity awareness within an organisation should be championed from the boardroom down. He further states that *"If you haven't got managerial, executive level buy in and sponsorship for security, you are wasting your time with all the rest. Because if they're not gonna drive it all through the organisation, if it's not gonna become a goal for the leadership team why on earth would the staff team bother". (Part2)*

Two participants have seen the positive impact of utilising leadership commitment to the organisation's cybersecurity awareness program. One participant state having a chat with the executive is usually sufficient *"So I need to have a chat with the exec to say, the exec that is responsible for that area and say, this is what I'm doing, this is how I need your help there to achieve that". (Part1)*

For another participant involving the functional managers have been more effective *"I think if the leadership of the functional area is brought into it, and they are passing those messages down. it's proving to be far more powerful than if the CISO starts pushing out messaging. So obviously that takes a hell of a lot of time if you're in a large organisation, but that in general, is the way to go is to get that buy in". (Part3)*

One participant gave a different view on how the lack of leadership buy in can have a negative effective to motivating cybersecurity. He identifies that little buy in from the executives and senior managers are blockers within the organisation. They do not champion cyber security or data protection in their day-to-day activities.

4.4 Theme 4: Embracing technical controls

Security technical controls are usually perceived as a complex and can be perceived as a barrier by the end user. But there is an argument on how technical controls can be used as enablers rather than as a barrier as seen by users. One example given was having single sign on for a number of applications, so users do not have to remember numerous passwords thereby mitigating the need for them to write passwords down.

Participants have looked at technical controls to reduce the security load on people to enhance security behaviours. As one participant states "*security requires you to just be a little bit more diligent and people are lazy by default. And that's why I say the make the password long, and you then use technical controls to support and augment security around people, so that they don't have to think about it. Because if they don't have to think about it, you've got better*

chance of being protected. If they're thinking about, then they might forget and then you're at risk. So, it's basically reducing the load on people". (Part2)

Another participant has in place rules that help reduce the load on people trying to identify if an email is real or not *"So we have an impersonation rule in place here, i.e. if somebody emails in trying to be the exec, I had to verify that this email address was not a member of our exec". (Part1)*

Forms of technical controls such as antivirus alerts are also factors used to monitor if users are reporting emails as Phishing emails or are clicking on them. As indicated by one participant *"are we seeing an increase in people reporting phishing emails or are we seeing an increase in antivirus alerts to say that people haven't actually spotted a phishing email, they clicked on the link, but our antivirus has protected us from that. (Part1)*

A similar approach has also been taken by another participant, who have also used incidents to monitor phishing click rates *"we also then, obviously monitor our incidents to see where the incidents are coming in, from what the sources are and phishing and social engineering is still a massive problem, and therefore, cyber culture and awareness programs training are vital". (Part3).*

A pragmatic view taken by one participant is that we should accept that there will be a proportion of individuals who are not interested in protecting the organisation. Putting technical controls as a managing factor removes the emphasis on the individual and protects the organisation from them.

"Maybe we accept the fact that 80% of the workforce are not interested in being secure, So isn't it our job as security professionals to put mitigating controls in place to allow them to be fluffy with their cyber security processes. So, for example, we block off all USB ports so they can't be used for storage USB drives, they can be used for keyboards and mouse. We ensure that those people have a good policy that shuts their computer after one minute of inactivity. So that if they're not, working on it for up to a minute, it shuts/locks screen, so they've got to log in. We take the technological controls we have got, and we put them around these people that don't want to partake of security so that they are partaking of security without being aware of it". (Part2)

Identifying metrics on how effective these technical controls in place have been noted as important. As one participant said*, "what metrics you're going to use to be able to determine the effectiveness of security controls that you deployed". (Part2)*.

One controversial suggestion was to take away some of the freedoms for people that are a little less security aware. If they wanted more access then they have to the cybersecurity awareness, course, and pass it.

5. Discussion

The research question for this study is what factors security awareness practitioners use to motivate cybersecurity awareness. The aim is to draw conclusions from the results of the interviews. While the barriers to cybersecurity awareness programs have been researched, few research have been taken on how to motivate employees to be engaged with their organisation's cybersecurity awareness program. To answer the research question, four practitioners were interviewed to understand their different perspectives and experiences.

This study explored and identified that there were similar approaches and activities taken by the practitioners in motivating their cybersecurity awareness programs. The four factors used to motivate cybersecurity awareness that this study has identified are 1) using different engaging techniques, 2) making it personable & relatable, 3) utilising leadership commitment and 4) embracing technical controls.

This chapter presents a deeper analysis of the results with the findings discussed in the context of the theoretical background as listed in chapter 2, the implications for practice and a discussion on the limitations of the study.

5.1 Discussion of findings

The data collected from the practitioners reveal that the role of cybersecurity awareness program's main purpose is to secure the organisation for which people are working. This is largely in line with literature and as noted by Ergen et al (2021), cybersecurity awareness is the starting point of the fight against cyber-attacks. For the cybersecurity awareness practitioners interviewed, they see their cybersecurity awareness programs as an important tool used to equip organisation employees. Of which, its purpose is not only to provide employees with an understanding of the threats to the company, but also how to protect the organisation from these threats that the organisation is vulnerable to. Rather than see employees as the weak link, the practitioners see them as guardians of the data they process. The practitioners work dynamically to instil this message through the cybersecurity awareness programs. It is used as a way of making the employees aware, that as guardians of the environment within which they work, they are also a level of security control as they act as defenders of their work environment.

Consequently, the method of delivery of the cybersecurity awareness programs is a major consideration for these practitioners. What message is conveyed and how it is delivered provides the opportunity for the practitioners to encourage behavioural change. Although several of these cybersecurity awareness programs are delivered to comply with regulatory standards and requirements. The collected data shows that effort has been made to ensure that the effectiveness of the awareness programs is a continuous flow of messaging through various mediums throughout the year and not just an ad-hoc computer-based training approach. Thereby taking it from a mere compliance requirement to establishing a

cybersecurity culture within the organisation. Existing restrictive forms of cybersecurity awareness training and delivery are being changed to motivate employee engagement as well as modify security behaviours. This finding supports Alshaikh (2020) suggestion of moving towards a more transformative based training, which is evident in the delivery methods of the cybersecurity awareness programs. Emphasis is on the engagement as practitioners are being inventive in the ways to motivate cybersecurity awareness. Traditional based methods such as classrooms-based training and posters on walls are being replaced with more innovative forms such as character-based avatars, road shows and social media.

Prior literature identified that employees do not usually comply with organisation's information security policy, and whilst this study took an explorative approach to understand how practitioners motivate cybersecurity awareness programs, there was however no intent within this study to investigate security policies. The data collected revealed an unexpected result, it showed that the practitioners struggle with finding a balance with security policies. This was evident in the practitioners' responses where one half felt that the security policies were cumbersome and needed to be scaled down. In comparison, the other half of the participants had several polices for a variety of topics. Like the literature suggests, employees lack basic understanding of their organisation's policies, and apart from the common 'acceptable use agreement' policy which is distributed to employees at induction. Other policies are not enforced and are dependent on employee's willingness or curiosity to be read. This means that employees can decide to either read or disregard these additional policies as they have not been made mandatory by the organisation. This makes it difficult for the practitioners to measure how these other policies are perused by the employees. For the practitioners there is work still to be done to embed security policies not just within the organisation but also within the cybersecurity awareness programs, so employees can be fully engaged in all aspects of the awareness campaigns.

The data collected from the practitioners revealed that cybersecurity awareness programs and its context in terms of its relatability to people and making it personable is an important consideration. This supports the literature that employees are likely to positively engage in better security behaviours when a threat was personally relatable (Haney and Lutters, 2018). Content of the cybersecurity awareness programs are created based on the different targeted audiences. And the practitioners use the feedback received from the employees, as a platform to understand employees personal understanding of organisational cybersecurity threats. Therefore, connecting the content of the cybersecurity awareness programs to both organisational and personal risks, has been shown to relate personally with the employee. This supports de Bruijn & Janssen (2017) who identified that making cybersecurity relevant to people's personal environment makes them receptive to the message.

Additionally, the collected data also shows that using supportive recommendations on how security can be applied within the personal environment is usually well received by employees. This supports the literature in that cybersecurity awareness programs should not just concentrate on the organisation but should also touch on personal environment, as noted by Ergen et al (2021) awareness is fundamental to behavioural change.

The collected data collaborates with the literature regarding threat vulnerability and self-efficacy, two components of the protection motivation theory. It identifies that threat vulnerability the organisation is exposed to, is a component considered by the practitioners when creating their cybersecurity awareness contents. This supports the literature that awareness programs give employees an understanding on how their organisation is easily open to security threats (Posey et al., 2015). Threat vulnerability for the practitioners is what security threats they feel the organisation is open to. They identify these threat vulnerabilities through monitoring and threat intelligence platforms they use to update themselves. The collected data shows that the practitioners work to manage these vulnerabilities through performing phishing simulation exercises and implementing security controls. These phishing simulations are used as the means to engage their users and equip them with the ability to identify the threat vulnerabilities. The outcomes of these phishing exercises then feed into the awareness content. There was some connection to threat severity which is defined in the literature as the perception that an employee has on the seriousness of the threat the organisation faces (Menard et al., 2017). It was shown that the participants included as part of the awareness content, the effects to the organisation if it does happen to suffer from a security event. An example one participant provided, was including as part of the awareness content; what the consequences to their clients would be and the organisation reputational damage in the event of a successful phishing email. By using different methods such as societal and emotional hooks to appeal to employees, they can become invested in the organisation's cybersecurity awareness campaign.

The collected data also supports the literature in terms of self-efficacy. The belief in one's ability to make decisions when faced with a security event can be influenced by the cybersecurity awareness programs using engaging techniques. The participants see the employees as a line of defence for the organisation data, and to improve the employee's ability in identifying and reporting suspicious activities, they ensure that they are equipped with the necessary knowledge. The cybersecurity awareness content is one way in which this is achieved. Such as using real life examples of phishing emails that have successfully delivered into the organisation environment and then asking employees to spot the clues within the email to identify the phish. By continually carrying out these types of exercises and relaying the messages, employees become able to question and report any suspicious activity they become aware of. This is in support of Shappie et al. (2020) who identified that self-efficacy can be positively improved through targeting of the individual's knowledge and belief.

The collected data identifies that the practitioners do have some predetermined ideas of some of the barriers that they might face and have tried to address this when putting together their programs. Careful and relevant communication plays a significant role in motivating cybersecurity awareness programs. De Bruijn and Janssen (2017) identified that the wrong type of communication technique can create a barrier. Based on the collected data, using different forms of communication mediums help to cascade the cybersecurity awareness message. From news feed features, newsletters, blogs and the intranet, these mediums help the practitioners deliver the cybersecurity awareness messages. Employees can be motivated to be engaged in a cybersecurity awareness program through effective communication on what the purpose of the awareness program and what it is about. Capitalising on a new approach has seen the shift towards using champions who are advocates that can help to spread cybersecurity awareness within the sections they are in. This is of particular use for those teams that have resource limitations or are siloed from an organisation headquarters. The main purpose of using champions is to use peer power to change the perceptions people have of cybersecurity and help push the cybersecurity awareness message. This was also identified by Alshaikh (2020), who noted that establishing a cybersecurity champion network plays an important part in building a cybersecurity culture within the organisation.

The collected data from the interviews also revealed that there was a collective agreement by the practitioners that employees should not be burdened with complex security requirements. Whilst the literature indicates that security control measures that are too stringent are perceived as barriers by the employees, this contrasts with the practitioners who have assessed security controls as a method to reduce the security responsibility load on employees. As an example, participants suggested the concept of single sign on, which is a form of grouping information applications to use the same password to reduce the number of times an employee must enter login details for a particular application. The use of a single login and password for different applications reduces the security load on the employee.

The discussion above has been a way to answer the research question using existing research to generalise the findings of the collected data, which in turn is proving the external validity of the study.

5.2 Implications for practice

This study demonstrates that there are factors that can be used to motivate cybersecurity awareness programs. While the result of this study is based on a small sample size of a group of cybersecurity awareness practitioners, there were similarities that were able to be grouped into themes. This study contributes to the existing knowledge by identifying the motivating factors that awareness practitioners can apply to help their cybersecurity awareness programs have better success with their target audiences. This includes ensuring that the content is relatable, personal, and clear on why the awareness campaign is being undertaken.

Alshaikh (2020) theory of establishing a cybersecurity champion has been shown to be possible. This is already being thought of by the practitioners interviewed as they see champions as a

tool that can be used to motivate cybersecurity awareness which leads to better security behaviours. This is an area that practitioners could invest in and push further within their organisation.

The participants noted that whilst all these motivating factors were being utilised, time resource was identified as their biggest barrier. Employees do need to be given time to complete these awareness programs and as there are only so many hours in the working day of an employee, there is competition for their time. Practitioners need to be aware of other training commitments that the employees have and should work with the human resource (HR) teams and managerial teams to ensure that employees are not fatigued by numerous awareness requirements. They should look to work with the other functions that also have training programs that take up the employee's time and possibly embed their security training with these other courses.

The practitioners interviewed for this study recognised the importance of measuring the effectiveness of the cybersecurity awareness programs. The usual approach used as a measuring tool is feedback questionnaires or surveys, that are delivered at the end of a cybersecurity campaign. Whilst feedback measures the effectiveness of the cybersecurity awareness programs, the tool used to measure behavioural change is through phishing simulation exercises. Using these two forms of measurements as a minimum can help organisations identify, areas of improvement of their awareness programs but also identify if further technical controls can be implemented to reduce the security load on employees.

Existing barriers need to be understood so adequate motivators can be considered, which can lead to stronger levels of awareness programs and training activities that are offered to the staff within the organisation.

The nature of cyber awareness training should be investigated further as it will particularly be useful to managers or security awareness practitioners who put together the awareness and training courses as well as companies that develop learning software modules. This study shows that motivation is piqued by the platforms used in delivering the cybersecurity training modules.

5.3 Limitations and future research

Whilst this study has been conducted using a systematic approach and Yin's (2018) guidelines for case study, there have been some limitations. This study used a "four-case" case study approach which is based on the number of participants that were interviewed. The study would have benefitted from a larger participant pool which would have significantly reduced any bias the participants might have presented during the interview. To ensure a diverse view can be explored, participants from different sectors were sought so unique perspectives can be gathered.

Another limitation is that the research can be said to be one-sided as it looks at just the cybersecurity awareness practitioner's perspective. Having the opinions of the employees

could give a more rounded overview on how they have been motivated to engage in a cybersecurity awareness program. This could then have been compared with the experiences of the cybersecurity awareness practitioners. Unfortunately, due to lack of access to resources and the limited time factor, it was not possible to include in this study.

The study concentrated on qualitative approach as the aim is to explore the perceptions and experiences of the cybersecurity awareness programs. There is a need for future research that will involve quantitative approach in which a questionnaire can be sent to both practitioners and employees to understand how cybersecurity awareness programs are motivated. This study also identified that further research is required in the use of security polices as part of a cybersecurity awareness program.

6. Conclusion

This study aim has been to address a research gap in identifying how security awareness practitioners motivate cybersecurity awareness. The research question "what factors do security awareness practitioners use to motivate cybersecurity awareness" set the direction in which the study progressed.

The main contribution of this study is that it has identified four common factors from the interviews that are used by the practitioners to motivate interest in cybersecurity awareness campaigns. These include, using different engaging techniques, making it personable & relatable, utilising leadership commitment, and embracing technical controls.

The findings of this study have revealed practical guidance for cybersecurity practitioners, such as using different forms of communication techniques to cascade the cybersecurity awareness message. It has also provided guidance on measuring the effectiveness of the awareness program.

The study has illustrated that for the research question, even though the practitioners work in different sectors, their perspectives on how they motivate align with each other and are quite similar. These findings provide a basis for future research. It is suggested that further empirical work, is to conduct several in-depth case studies from a large pool of cybersecurity practitioners and employees, to better understand how cybersecurity awareness programs are motivated from both perspectives. Furthermore, it is also suggested that future research investigate the use of security policies as part of a cybersecurity awareness program. This is important as it will enable practitioners to assess what security policies should be mandatory for their users and are therefore enforced through the cybersecurity awareness programs. Consequently, creating a culture where individuals within the organisation comply with IS security policies.

References

Alahmari, A. A., & Duncan, R. A. (Jul 1, 2021). Investigating potential barriers to cybersecurity risk management investment in SMEs. Paper presented at the 1-6. doi:10.1109/ECAI52376.2021.9515166 Retrieved from https://ieeexplore.ieee.org/document/9515166

Alghamdi, M. I. (2021). Determining the impact of cyber security awareness on employee behaviour: A case of saudi arabia. *Materials Today: Proceedings,* doi:https://doi.org/10.1016/j.matpr.2021.04.093

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations.

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. Paper presented at the *Eleventh Symposium on Usable Privacy and Security ({SOUPS} 2015),* 103-122.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-A7. doi:10.2307/25750690

Calvin, N. (2018). Botching human factors in cybersecurity in business organizations. *Holistica, 9*(3), 71-88. doi:10.2478/hjbpa-2018-0024

Cambridge dictionary (online). Retrieved from https://dictionary.cambridge.org/dictionary/english/barrier

Chenail, R. J. (2011). Ten steps for conceptualizing and conducting qualitative research studies in a pragmatically curious manner. *Qualitative Report, 16*(6), 1713-1730.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7. doi:https://doi.org/10.1016/j.giq.2017.02.007

Donalds, C., & Osei-Bryson, K. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management, 51*, 102056.

Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: Current practices, trends, and recommendations. *MIS Quarterly, 27*(4), 597-635.

Ergen, A., Naci Ünal, A., & Saygili, M. S. ı. (2021). Is it possible to change the cyber security behaviours of employees? barriers and promoters. *Academic Journal of Interdisciplinary Studies, 10*(4), 210. doi:10.36941/ajis-2021-0111

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine, 7*(3), 93-99. doi:https://doi.org/10.1016/j.afjem.2017.08.001

Fielding, N., & Schreier, M. (2001). Introduction: On the Compatibility between Qualitative and Quantitative Research Methods. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 2(1), Art. 4, http://nbn-resolving.de/urn:nbn:de:0114-fqs010146.

Galliers, R. D. (1), & Huang, J. C. (2). (2012). The teaching of qualitative research methods in information systems: An explorative study utilizing learning theory. *European Journal of Information Systems, 21*(2), 119-134. doi:10.1057/ejis.2011.44

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems,* , 1-11.

Goldkuhl, G. (2019). The generation of qualitative data in information systems research: The diversity of empirical research methods. *Communications of the Association for Information Systems, 44*, 572-599.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. doi:https://doi.org/10.1016/j.cose.2017.11.015

Hadlington, L., Binder, J., & Stanulewicz, N. (2021). Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. *Computers in Human Behavior, 114* doi:10.1016/j.chb.2020.106557

Haney, J. M., & Lutters, W. G. (2018). " It's scary... it's confusing... it's dull": How cybersecurity advocates overcome negative perceptions of security. Paper presented at the *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018),* 411-425.

Haven, T.,L., & Van Grootel, D. L. (2019). Preregistering qualitative research. *Null, 26*(3), 229-244. doi:10.1080/08989621.2019.1580147

Hill, C. E., Thompson, B. J., & Williams, E. N. (1997). A guide to conducting consensual qualitative research. *The Counseling Psychologist, 25*(4), 517-572. doi:10.1177/0011000097254001

Kitto, S. C., Chesters, J., & Grbich, C. (2008). Quality in qualitative research. *Medical Journal of Australia, 188*(4), 243-246.

Kleinginna Jr., P. R., & Kleinginna, A. M. (1981). A categorized list of motivation definitions, with a suggestion for a consensual definition. *Motivation and Emotion, 5*(3), 263-291. doi:10.1007/BF00993889

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* Pearson Education.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019a). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24. doi:https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019b). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24. doi:https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems, 34*(4), 1203-1230. doi:10.1080/07421222.2017.1394083

National cyber security centre glossary (2016). Retrieved from https://www.ncsc.gov.uk/information/ncsc-glossary

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors (14248220), 21*(15), 5119.

Nigel Fielding, & Margrit Schreier. (2001). Introduction: On the compatibility between qualitative and quantitative research methods. *Forum, Qualitative Social Research, 2*(1) Retrieved from https://search.proquest.com/docview/867758082

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214. doi:10.1080/07421222.2015.1138374

Raddatz, N. I., Coyne, J. G., & Trinkle, B. S. (2020). Internal motivators for the protection of organizational data. *Journal of Information Systems, 34*(3), 199-211. doi:10.2308/isys-18-067

Reeves, A., Calic, D., & Delfabbro, P. (2021). "Get a red-hot poker and open up my eyes, it's so boring"1: Employee perceptions of cybersecurity training. *Computers & Security, 106*, 102281. doi:https://doi.org/10.1016/j.cose.2021.102281

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *The American Psychologist, 55*(1), 68-78. doi:10.1037/0003-066X.55.1.68

Ryan, R. M., & Deci, E. L. (2020). Intrinsic and extrinsic motivation from a self-determination theory perspective: Definitions, theory, practices, and future directions. *Contemporary Educational Psychology, 61*, 101860. doi:10.1016/j.cedpsych.2020.101860

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Qualitative studies in information systems: A critical review and some guiding principles. *MIS Quarterly, 37*(4), iii-xviii.

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media, 9*(4), 475.

Shaw, R. L., Booth, A., Sutton, A. J., Miller, T., Smith, J. A., Young, B., . . . Dixon-Woods, M. (2004). Finding qualitative research: An evaluation of search strategies. *BMC Medical Research Methodology, 4*(1), 1-5.

Steffi Haag, Mikko Siponen, & Fufan Liu. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *Database for Advances in Information Systems, 52*(2), 25. doi:10.1145/3462766.3462770

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3), 190-198. doi: https://doi.org/10.1016/j.im.2012.04.002

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems, 15*(3), 320-330.

Watkins, D. C. (2012). Qualitative research: The importance of conducting research that doesn't "count". *Health Promotion Practice, 13*(2), 153-158.

Whitman, M. E., & Mattord, H. J. (2019). *Management of information security* (Sixth edition ed.). Boston, MA: Cengage.

Yin, R. K. (2018). *Case study research and applications* (Sixth Edition ed.). Los Angeles; London ; New Delhi ; Singapore ; Washington DC ; Melbourne: Sage.

Appendix A. Interview Protocol Guide

The interview questions have been adopted from Haney & Lutters 2018 and Reeves et al 2021. The aim of these questions is not to have a yes or no answer but a detailed answer which opens the researcher to probe further if required

Guiding research question: ***What factors do security awareness practitioners use to motivate cybersecurity awareness.***

Interview opening: Background

(1) Introduction of researcher and overview of study
(2) Participant background information
    a. What sector do you work in ?
    b. How long have you worked within information security?
    c. Can you describe what you do in your work?

Theme 1: Cybersecurity awareness programs

    d. How involved are you in creating or delivering cybersecurity awareness in your workplace?
    e. What sort of cybersecurity awareness training do you deliver at your workplace?

    f. What is the main purpose of your cybersecurity awareness programs/campaigns?
        i. What are you trying to change and why? Probe if no behaviour change is mentioned
        ii. What type of messaging do you use?
            1. Probing question – do you use the fear factor within the messages
        iii. What security policies as part of your cybersecurity awareness?
            1. How are these distributed to employees?
            2. What would you say is the compliance percentage of these policies?
    g. How are your awareness programs valued by others?
        i. What do you use to measure?
    h. What kind of feedback do you get?
        i. What do you think makes a good or bad cybersecurity awareness campaign?

(3) What would you say are the factors that help with motivating cybersecurity awareness
(4) What would you say has been your biggest obstacle in implementing a cybersecurity awareness program?

Theme 2: Motivation and barriers

a. What would you say are barriers to employees engaging in cybersecurity awareness?
    i. What type of behaviours (probe question)
b. What would you say is the most challenging in dealing with these barriers?
c. How do you motivate against these barriers?
    i. What do you do?
    ii. Is there anything in particular that works / or does not work?
d. How do you promote cybersecurity awareness within the organisation (For example, conferences, invited talks, blogs, social media, articles, client visits, face-to-face meetings, phone, email, security champions)?
    i. Which of these means are most effective? And Why?

(5) How do you identify if you are targeting the right people within the organisation?
    a. What prevents you from reaching the right people?
    b. How have you managed to overcome the barrier?

Closing questions

- Is there anything else that you'll like to add that to further what we have discussed today?