Cyber Security Training in Small to Medium-sized Enterprises (SMEs): Exploring Organisation Culture and Employee Training Needs

Omolola Fagbule

A thesis submitted in partial fulfilment of the requirements of the degree of Doctor of Philosophy in

Bournemouth University

Copyright Statement

Abstract

Research shows that large businesses routinely provide cyber security training, to educate and train staff in readiness for a cyber threat. Contrary to this, small to medium enterprises (SMEs), are either unaware of risks and/or lack the financial resources for training and education. As a result, SMEs frequently fall victim to security breaches, and this can affect business reputation, access to private details, finance, and potential future business with clients.

Although investments are sometimes made to train staff, there are still shortcomings with the design and delivery of cyber security training, that may impact learners' perceptions and attitudes towards learning. Rather than applying learning theories, adult learning principles, and fundamentals for developing business objectives, training approaches are typically technical and knowledge-based. Past research has primarily looked at this problem from a computing perspective, instead of a psychological lens, that explores the nature of human beings and what affects learning and transfer of knowledge in the workplace. The design of cyber training incorporates knowledge-based questions to address learning objectives, however, there is a lack of interrogation into the effectiveness of training, and this raises the question, how effective is cyber training?

This thesis aims to evaluate learning theories and training evaluation methods by comparing them to the literature. The thesis will investigate the selection, development, and delivery of cyber security training and identify how, and if, these address employee training needs. The results will demonstrate the methods to derive cyber security training content compared to what the literature proposes, what training evaluation methods are used and how they address employees and the organisation’s needs.

The thesis adopts a qualitative approach with one exception. Studies 1a and 1b are part of a larger project, study 1a collected quantitative data, through a knowledge survey, which provided background insight into participant knowledge. Study 1b involves a follow-up interview about the Study 1a survey. The interviews involved 14 SME business owners in Dorset and focused on perceptions, peer influence, and motivation. The results from Study 1b highlight that organisational culture influenced attitudes and perceptions from other colleagues and managers towards cyber security. The results showed that employees showed little to no attention to cyber security due to work priorities. Participants associated their poor

learning and lack of behaviour change with limitations and style of the delivery and content of the training.

The results acquired in Study 1b prompted reason to further investigate training development and organisational culture in a second study. The second study (Study 2) also adopted a qualitative approach and investigates the process of how cyber security training is selected, devised, and delivered to businesses. The interview participants are content developers, awareness professionals, and employees. In addition, one of the aims of Study 2 is to investigate how much employee training needs are evaluated in the process of training selection. There was a total of 27 interviews with content developers, employees, and awareness professionals. The results from Study 2 showed that employee training needs are not evaluated in the selection process. Employees discussed factors that influence their attitudes towards cyber security, such as internal and external motivation, training material and time constraints.

The key conclusions from the studies demonstrate that content developers create arbitrary training because they neglect to investigate the needs of employees. In addition, awareness professionals neglect to support staff and outline training objectives, which leads to training that does not address employee challenges and, as a result, causes employees to feel disengaged, lose interest, and fail to apply what they have learned in training in the workplace. The findings from this research contribute to the cyber training and education community, as the thesis produced research-based guidance for developing training for SMEs. The current landscape fails to address security training from a psychological lens or established domains, like Education and Training. Key findings from this research demonstrate that consideration of employee training needs is vital for learning and transferring knowledge in the workplace.

Tables of Contents

List of figures

Acknowledgements

First of all, I would like to thank the Almighty God, it's only by His grace and mercy.

I dedicate the success of the PhD to my parents, my main source of motivation, support and sustainance. Thank you to my resilient God-sent phenomenal mother, Ms Kuburatu Bosede Alo, who refused to give up even when I gave up. A special and honourable thank you and reverence to my education enthusiast dad Mr Kolawole Francis Fagbule who sadly passed to glory, 10 months into my first year of the PhD. It brings me joy and peace to know I made you both incredibly proud.

I would like to thank, my supervisors Professor John McAlaney, Dr Jacqui Taylor, Dr Shamal Faily and Dr Sarah Hodge for their unwavering support and input over the years of the project.

I am extremely grateful to the Dorset Cyber Alliance (DCA) and Bournemouth Christchurch and Poole (BCP) council, namely Adrian Trevett and John Dale for match-funding the project and supporting the research.

I thank Bournemouth University for accommodating and providing me with the necessary resources during my journey. I also thank the participants that took part in studies.

I would like to thank my amazing friends: Esther Adeusi, Derrick Feehi and Munachiso Arthur for their kindness and support during my PhD journey. I also thank Dr Shane Shook, a true inspiration and source of encouragement throughout my PhD. I also thank Dr Gernot Liebchen for his push in the right direction right, from my undergraduate years to PhD level.

I would like to thank Pastor (Dr) Toyin Fakorede for advising me to start this journey and for supporting me through prayers. I would like to thank Pastor (Dr) Olu Baptist who has played an integral role in my PhD journey. Lastly, a huge thank you to Deacon Efe Ohwafasa who also supported me through this journey.

I could not have done this without you, thank you all.

Author’s declaration

I hereby declare that the work presented in this thesis has not been and will not be submitted in whole or in part to another University for the award of any other degree.

Signed: Omolola Fagbule

Chapter 1 Introduction

Online criminal activities exploit vulnerabilities in the use of the internet and other electronic systems to illicitly access or attack information and services used by citizens, businesses, and the Government (Anderson, 2013). A study conducted in 2015 to gain a general overview of the cyber-attacks from all over the world, revealed that regardless of the business sector, private sector, or size, organisations are targeted by cyber-attacks (Bendovschi, 2015). For example, Zoom, the video communication company experienced a breach in April 2020, with reports of more than 500,000 stolen Zoom passwords available for sale in dark web crime markets (Cubukcu, 2020). Bendovschi (2015) study presented a relative correlation between the business sector and the types of attacks; thus, cyber espionage is most likely aiming at Media, Government and Law Enforcement sectors, and quite unlikely to target other business sectors (Retail, Online services). Similarly, Marriott International suffered a breach where 5.2 million guests, used the business's loyalty application scheme. Cybercriminals stole login credentials of two Marriott employee accounts which had access to customer details about Marriott’s loyalty application (Daswani, 2021). These are examples that depict the diverse risks to businesses; any business is a potential victim, hotel or a communications business-like Zoom.

Cybercriminals take advantage of means, motives, and opportunity, which has further been made easy by the interconnectivity of society (Pasculli, 2020). Specifically, post the Covid-19 global pandemic, there have been reports of scams impersonating public authorities. Cyber attackers have maliciously targeted the World Health Organisation (WHO) and organisations, supermarkets, and airlines (Threat Team, 2020), by offering Covid 19 cures (Gervais, 2020). These examples demonstrate the widespread vulnerability and cross sector susceptibility to cyber attacks.

Due to the sporadic nature of cyber-attacks, many businesses are beginning to realise the necessity for security (Tounsi and Raism 2018). In anticipation of coming under attack by cybercriminals, many UK businesses are investing in stronger physical security, for example, advanced intrusion detection hardware, security cameras, as well as training initiatives and user behaviour incentives (Brooks, 2022). Traditionally, physical security measures such as access control, security personnel, and surveillance are treated as standalone functions, with little regard for how data and IT systems are intrinsically connected to physical security (Pieters, 2011).

As a result of the threat landscape, some businesses have seen that raising awareness of cyber security best practices is also essential for their organisation, especially from an empowerment and accountability perspective (Alami et al., 2019). For example, Abawajy (2014) discussed that training is a powerful means of empowering people with knowledge on focused topics. Similarly, it has become apparent to businesses and government bodies to build cyber security skills and increase knowledge in the workforce (Adams, 2015). This is exemplified in a study that found that financial services spend on average 10% of their IT budgets on security (Crawley, 2020).

Large organisations typically employ a chief security officer or chief information security office who has formal training as an information security analyst to address legal and compliance issues (Allen et al., 2015). However, small businesses seem not to have the working capital to hire and maintain a diverse and technically proficient staff of full-time employees (Perez, 2020). Instead, some small businesses invest very little in security. They might implement a router, to establish information mapping to prevent outsiders from determining the address of key employee equipment (Fabro et al., 2016). However small businesses do not have the resources to train employees on safe and secure Internet browsing practices (De Crescenzo, 2016).

1.1 Rationale

Though the threat landscape appears to depict large businesses as aware and prepared for cyber risks, the reality is that there is still a heightened level of risk towards businesses that do not embark on cyber training as much, such as SMEs. Khan et al. (2021) researched why cyber security campaigns fail and they discover that users may be considered an ‘unintentional threat’. However, users also have underlying factors that affect learning, adopting what has been learned and transcribing this into everyday behaviour. Sasse et al. (2014) highlight various psychological factors e.g., personal factors, motivation and self-efficacy, environment and fear; they investigate how these factors attribute to behaviour change. Coupled with this, they also investigate the framing and delivery of cyber training itself. One of their arguments is that cyber training often takes a pick and mix approach where they adopt portions of the research perceived to be relevant and merge this into a behaviour change campaign, which ignores the complexity of the original theories and can lead to undesired behaviours.

For example, NIST (1998) provide a model for building training courses, and they note that individuals learn in several ways but each person, as part of their personality, has a preferred or primary learning style. They assert that matching or mismatching a student’s learning style can affect a student's performance (Pashler et al., 2008). According to them, students who do not learn best through listening will tune out and learn little, therefore being aware of learning style differences will help content developers (of cyber training) develop and use a variety of teaching approaches congruent to trainee understanding (Dantas and Cunha, 2020). For Kolb and Kolb (2013) learning should be viewed as a process rather than just for the outcomes. It is aided when students can evaluate their knowledge, beliefs, and ideas about a particular subject and add fresh, improved ones. Counter to intuition, several studies into matching learning styles to people through questionnaires and surveys suggest that categorising individuals can lead to the assumption of fixed learning styles, which can impair motivation to apply oneself or adapt (APS, 2009). Mayer (2011) similarly argues that learning styles research has persistently lacked rigour and that there has been no evidence that supports the application or practice of learning styles-based instruction. This shows that cyber security content developers take different aspects of the literature and make presumptions on what they think is suitable for trainees to consume, without fully delving into the factors (Sasse et al., 2014). This is problematic as there is an increase in cyber breaches across businesses. There is ambiguity as to what barometers are in place to measure training effectiveness (Koutsouris et al., 2021). For example, cyber security training is a one-off event that typically happens when a new employee is recruited (Čeleda, 2015). After they undergo training, there is no follow-up or conversations about the employees learning or what concerns they have with cyber security. This poses the question of how is training evaluated?

In this thesis, models of learning are investigated via an educational lens, and models of training assessment are investigated by examining the components of successful learning and information transfer as well as the models that are already in use. The literature study identifies the discrepancies between the psychological elements' involvement in the choice and creation of cyber training, how this affects successful learning and application in the workplace, and the effectiveness of evaluating the success rate of cyber training. The findings are presented and contrasted with what is currently being done in business. Does cyber security training effectively prepare people for cyber threats? is a topic that has been posed due to the dearth of comprehensive study on this issue.

The thesis recognises the complexity of the problem and so it is broken into multiple studies with separate research questions, aims, and objectives. There is a pilot study that contains 4 interviews, these serve as baseline results for the main studies of the thesis. The first study was part of a larger project, and some elements are not completely relevant to the thesis. The study was broken into Study 1a and 1b. Study 1a is a survey that provides a baseline introductory study into broadly how a trainee's social environment could impact productivity to cyber security and 1b investigates the process for selecting, devising, and delivering cyber training to businesses and whether the output of training content address needs on an individual level and organisational level. While Study 2 investigates the process for selecting, devising, and delivering cyber training to businesses and whether the output of training content addresses needs on an individual level and organisational level.

1.2 Thesis structure

The thesis starts with the literature review in Chapter 2. The review starts with an evaluation of barriers to cyber security, origins of training, models of training and preliminary psychological factors that affect learning and behaviour change in the workplace. In Chapter 3 the research challenges, pilot study and chosen methodology are presented. Chapter 4 details the methodology for study1a (BEIS survey) and study 1b (BEIS Interview), followed by study 1a's (BEIS survey) results. Chapter 5 presents study 1b's (BEIS interview) results. 5.4 is a brief discussion about study 1b (BEIS interview) and introduces rationale for study 2 (Training Selection). Chapter 6 presents the results from study 2, training selection, these entail content developers, awareness professionals and employees. In Chapter 7 there is a corresponding discussion for each interview group presented in Chapter 6. Chapter 8 proposes a solution for designing a training package, targeted at each interview group. Chapter 9 concludes the thesis by addressing the research questions, illustrating research contributions, project limitations and future work.

1.3 Chapter Summary

This Chapter outlined the recent climate of cyber-attacks that businesses fall victim to; from novice attacks to COVID-19-driven attacks. Disparities between SMEs and large businesses were identified. To illustrate, large businesses typically employ professionals to address compliance issues, whereas small businesses seem to not have the financial liberty to hire a cyber professional. This Chapter introduced that cyber training may not fulfil learning outcomes as intended, some of this resides in psychological factors and learning theories, however, this is rarely adopted in cyber security training. The posited argument is that cyber security often takes a pick-and-mix approach, meanwhile, if a security breach happened, employees are blamed. Typically, this has been the approach from the cyber security domain, where employees are seen as a risk to business. However, the literature review starts by presenting beliefs and barriers from the security domain, characterised by a plethora of factors including personal. This is followed by underlying theories and models of training. The next part of the literature review (Chapter 2) evaluates training evaluation models and the factors that affect the transfer of training, e.g., motivation, the influence of social environment and attention and principles of adult learning (Andragogy). The Chapter discusses cyber security content developers, before introducing the research questions, aims and objectives for each study.

Chapter 2 Literature Review

2.1 Chapter Introduction

In this chapter, barriers to cyber security training from an Information Security domain are explored, and the existing landscape is highlighted to present current ideologies businesses and security professionals have about learning cyber security. This is prefaced by highlighting gaps in the Information security domain, before exploring Psychology evaluation models, and components of a successful training campaign, for example, organisational culture, motivation, and andragogy.

The literature review was deduced from a compilation of various databases: Web of Science, EBSCO, Eric, IEEE Xplore and Google Scholar. As the literature developed, a range of terms was searched to identify the threat landscape. The terms 'behaviour change strategy, cyber security training and education, cyber psychology theory, attitudes and perceptions, and attention and memory limitation' were searched in the database.

2.2 Barriers to cyber security training

There have been attempts in previous security work to highlight challenges in cyber security training, some of which portray users as unintentional threats (Ismail et al., 2018). That is, acts performed without malicious intent, nevertheless represent a threat to information security. It has been argued that these unintentional threats derive from poor user behaviour (Khan, 2022). While Van Bavel et al. (2019) argue that users have a minimal understanding of cyber threats and therefore enforce counterproductive actions, which make them unintentional threats. In light of this, Bada (2014) researched what factors could influence change in online behaviour. Results from their study specifically highlighted 'personal factors, cultural and environmental factors, and persuasion techniques'.

2.3 Personal factors

Bada (2014) starts by building on previous work that recognises that an individual's knowledge, skills and understanding of cyber security as well as their experiences, perceptions, attitudes, and beliefs are the main influencers of their behaviour (Pusey, 2005). They discuss that people can get tired of security procedures and processes, especially if they perceive security as an obstacle, preventing them from their primary task. Remaining at a high level of vigilance and security awareness can be described as 'security fatigue' and this can be hazardous to the overall health of an organisation (Stanton et al., 2016). In a work context, employees who experience security fatigue and engage in non-compliant security behaviour, for this reason, are separate from those employees who consistently ignore or refuse to comply with security policies (Cram et al., 2021). Rather, security-fatigued employees may have at one time been inclined to comply with security policies, and may still be, but rigid compliance is less likely for these employees due to their fatigued state (Furnell & Thomson, 2009). A user with growing security fatigue may encounter a reduced security attitude (i.e., their views on compliance) and lower self-efficacy (i.e., confidence in their ability to perform in a compliant manner), while simultaneously being exposed to security education activities (Cram et al., 2021).

In addition to this, the security domain describes the 'Security, Functionality and Usability Triangle' as the situation of trying to create a balance between three, usually conflicting goals. If the triangle leans too far in either direction, this can lead to an insecure system that everyone can use, even intentional threats (Waite, 2010). Security fatigue becomes an issue when the triangle swings too far to the security side and the requirements are too intense for the users to handle. As a result, there should be a balance between system security and usability (Bada et al., 2014).

2.4 Protection Motivation Theory (PMT)

PMT seeks to clarify the cognitive processes which meditate behaviour in the face of a threat (Rogers, 1975). It posits that, when facing a threatening event, people conduct two appraisal processes: one focused on the threat itself and the second on their ability to act against that threat. This affects their intention to take precautionary action and results in adaptive or maladaptive behaviours in relation to the threat. In their threat appraisal, people will consider how negative the consequences of the threat are (perceived severity) and the likelihood of the threat happening in a way that will directly affect the, (perceived vulnerability). This threat appraisal may lead to maladaptive behaviours such as denial or avoidance (Witte and Allen, 2000).

PMT has been applied to cybersecurity, specifically to security behaviour among people who know how to protect their systems but fail to do so, security behavioural intentions of home computer users, convincing internet users to protect themselves, the role of personal responsibility in the protective behaviour of college students, teenagers' willingness to provide information online, security behaviour in response to fear appeals by employers, and employees' adherence to information security policies. There is, a significant and growing body of research in this area, however, most of the PMT studies have used behavioural intention as a proxy for cyber security behaviour. This is typical of many approaches that are derived from Azjen's (1985) theory of planned behaviour, which has behavioural intention as the primary driver of observed behaviour.

2.4.1 Self-Efficacy

Bandura (1986, p. 391) defines self-efficacy as "people's judgements of their capabilities to organise and execute courses of action required to attain designated types of performances. It is concerned not with the skills one has but with judgements of what one can do with whatever skills one possesses".

Self-efficacy, in the context of information security, refers to an employee's self-confidence in their skills or ability to comply with the controls taken by the organization (Kankanhalli and Xu, 2009). Rhee et al. (2009) demonstrated that people with high efficacy demonstrate a higher degree of belief about their ability to utilise motivation and cognitive resources needed to successfully execute the guidance of the organization's information security policies (Rhee et al., 2009). At the same time, habits and subjective norms were found to directly influence actual behaviour and reduce the impact of behavioural intentions to comply with organizational security policies (Limayem and Hirt, 2003).

2.4.2 Cultural and environmental factors

The concept of Cybersecurity Culture (CSC) refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people’s behaviour with information technologies. When considering factors that could influence change in online behaviour, Bada et al. (2014) discussed that culture is an important factor that can have a positive security influence on the persuasion process for users (Kreuter, 2004). Information security culture encompasses the thinking, feelings, and everyday activity of employees (Al Sabbagh et al., 2012).

The cultural structures of a society shape psychological processes, including cyber security. Intrinsically motivated behaviours originate from the self and enhance by the enjoyment and satisfaction of engaging in an activity. While extrinsic motivation refers to the motivation to engage in an activity to achieve a contributory result, i.e., earning a reward or avoiding a punishment (Reiss, 2012). Cyber security campaign messages tend to be more persuasive when there is a match between the user’s cognitive, affective, or motivational characteristics and the content of framing of the message (Uskul et al., 2009). In addition, messages are more persuasive if they match a user’s self-guide. They claim that, while people may be motivated to follow a security campaign's advice, if it causes certain limitations on the sites they can visit, then this can automatically result in emotional discomfort, thus leading to an ignorant state of a suggested ‘secure’ behaviour.

2.4.3 Persuasion techniques

Persuasion can be defined as an “attempt to change attitudes or behaviours or both (without coercion and deception)” (Fogg, 2002). Behavioural change can be segregated into two ways (Dolan, 2010). The first model is based on influencing what people consciously think about, the rational or cognitive model. This model suggests that citizens and consumers will analyse the various pieces of information from various sources, and the numerous incentives offered to them and act in their best interests. The second model of shaping behaviour focuses on the more automatic processes of judgment and influence. This shifts the focus of attention away from facts and information, and towards altering the context within which people act, the context model. The context model highlights that people are irrational and inconsistent in their choices, often attributed to the influence of surrounding factors. It focuses more on ‘changing behaviour without changing minds.

2.4.4 Fear appeal

On the other hand, the fear appeal approach has been adopted in the past to scare people into behaviour change. Fear is essentially an emotion; and emotions, both positive and negative, act on humans as follows (Dillard, 1994): emotions arise from the individual's assessment of a situation, have a biological basis, are informed by learning, and unfold over time, while individuals continuously attempt to regulate their emotions. A fear appeal usually packages some fear "trigger", together with an action that the fear appeal designer wants the recipient to take (Dupuis & Renaud, 2021). They are delivered via a variety of channels including, for example, on cigarette packets, in health practitioners' waiting rooms and via a computer's user interface. It has been argued that the inclusion of fear in an appeal will improve the persuasiveness of messages, increase engagement, enhance information processing and render the message memorable (Dupuis & Renaud, 2021). On the contrary, Ruiter et al. (2014) argued that while fear does impact attitude and intention, this does not necessarily convert into actual behaviour. They argue that fear could arouse defensive reactions, including, denial of health threats (Ruiter & Kok, 2005).

In a cyber security context, fear messages are used to scare people into taking a particular recommended action to secure their information and devices. Phishing campaigns have been used to elicit fear, and this makes people likely to act without deliberation. This suggests phishing messages that induce fear cause the usual cognitive processing to be bypassed. Similar to this, a fear appeal could be designed to reduce the spread of ransomware. The target of the fear appeal might be Windows users. Some of the recipients of the fear appeal may be upset at the prospect of losing all their information and, instead of performing a recommended action, they instead choose to do nothing (Renaud and Dupuis, 2019).

2.4.5 Effective Security Training

Even though the number of security awareness training programs are progressively growing, there is inadequate evidence to verify their effectiveness and impact on daily activities in a work environment (Waly et al., 2012). They assessed factors that influence user behaviour towards information security and the evaluation of training and awareness programmes to impact information security management behaviour in the health, business, and education sector. The results showed that the most effective organisation factors that contribute to increased compliance are communication, sanctions, reward and banishment, positive awareness, strong motivation, efficient feedback mechanisms and appropriate allocation of roles and responsibilities.

In addition to this, Waly et al. (2012) found that there were other issues such as lack of positive belief among employees, lack of intention, lack of positive attitude, lack of behaviour, lack of regular training, lack of effective training and lack of regular assessment, which impose barriers on the creation of a positive drive to implement and follow information security policy in the business sector. Cone et al. (2007) stated that some of the awareness training programs tend to be more informative without integrating into employees' daily activities which leads to disciplinary actions. On the other hand, NCSC(2019) recommends businesses integrate cyber security into organisation's objectives because cyber security impacts every aspect of a business. Therefore, integration into organisational risk management and decision-making for effective handling is recommended. Peker et al. (2013) state that a successful campaign constitutes a security awareness professional to have good communication skills, be familiar with learning concepts, and understand that training is beyond a tick box exercise. Additionally, not collecting metrics and not understanding what security awareness is really about, are factors that ought to be avoided. Some awareness training programs are only provided as a one-time session that cannot truly change users' behaviour toward information systems (Ghazvini, 2016). To add to this, He and Zhang (2019) identify best practices for engaging in cyber security training, they discuss that cyber security training and awareness programs fail to achieve their goals as employees feel bored and do not have a strong motivation to participate in their organisations training programs, since they do not provide any incentives or rewards for employees to complete such security training (Gross, 2018). They also identify that security programs are not designed in a format that satisfies the various learning styles and needs of different employees, (Kostadinov, 2018). This premise insight key recommendations that organisations can use to enhance the performance of their business cyber security training and awareness programs. Firstly, they recommend that training programs need to relate to employee's personal life, family and home. Secondly, security programs should focus on implementing good security behaviours, as defined in formal organisational procedures and guidelines, instead of merely telling people what not to do (Winkler, 2018). In Winkler's (2018) research it is noted that businesses should instil a relaxed alert state for employees where they feel relaxed, productive, and able to concentrate and minimise security fatigue for employees. Given this is understood and established in a cyber security context, it poses the question, how much knowledge is adopted in cyber security training?

The previous section presents the current landscape of factors that could influence change from an Information security perspective. This domain suggests that personal factors like self-efficacy and culture, are drivers for change. Whereas a fear appeal may positively reinforce expected behaviour or enforce undesired behaviour that could bring harm to the organisation. However, the security domain fails to highlight learning theories that directly address what learning entails, the underlying factor that contributes to successful learning and what underlying factors inhibit learning. An understanding of these contributing factors would aid in the success of learning cyber security training. As a result, the learning theories from the Psychology domain are explored to identify, how they may attribute to participant learning, and to bridge the gap between participant learning and training offered to employees in businesses.

2.5 Underlying theories and models of training

2.5.1 Behaviourism

Unlike the cyber security domain, the psychology domain centre on various learning theories and propose methods and strategies to attain the most effective level of education and learning. The current landscape discusses certain learning theories that advocate behaviour change, most of which are referred to when discussing educational learning theories (Zhou and Brown, 2015). One of the common learning theories is 'Behaviourism' originally coined by Watson (1913). The theory discusses a key term 'operant conditioning' which is a method of learning that employs rewards and punishments for behaviour (Skinner, 1971). In practice, operant conditioning is the study of reversible behaviour maintained by reinforcement schedules (Staddon and Cerutti, 2003). Skinner (1971) distinguishes between positive and negative reinforcement. Negative reinforcement is the termination of an unpleasant state following a response, it strengthens behaviour because it stops or removes an unpleasant experience. Whereas, as a positive reinforcement is strengthened by rewards, leading to the repetition of desired behaviour, the reward is a reinforcing stimulus. Often at times, negative reinforcement is conflated with punishment, however there is a difference. For example, negative reinforcement removes a factor that may inhibit a desired behaviour to strengthen behaviour. Whereas punishment is adding or taking away a factor to weaken behaviour (Rupere and Muhonde, 2012).

Skinner (1971) developed Watson's (1913) theory and studied operant conditioning by conducting experiments using animals which he placed in a 'Skinner Box'. The experiments objectively recorded an animal's behaviour in a compressed time frame, an animal can either be rewarded or punished for engaging in certain behaviours, such as pressing a lever (for rats) or key pecking (for pigeons). To exemplify this, a study of 243 was conducted by Hikin and Schriesheim (2004) and they looked at two different hospitality organisations and compared the effects of managers' feedback with no comments at all. The study found that feedback, improves performance even when that feedback involves negative or corrective comments. However, the theory has been critiqued that it is a one-dimensional approach to understanding human behaviour and that behavioural theories do not account for free will and internal influences such as moods, thoughts and feelings (Moore, 2013). For example, Skinner's use of animals negates the importance of human behaviour, which is driven by complex emotions and complex thought processes. Consequently, it is impossible for all these processes to be observed in the theory (McLeod, 2007). There has been positive correlation between positive reinforcement and desired behaviours. Rafi et al. (2020) researched the implication of positive reinforcement strategy in dealing with disruptive behaviour in the classroom. They suggest that Behaviour-Specific Praise (BSP) acts as a positive reinforcement strategy that states that students can only value the praise if it is specific and can help to recognise their efforts and achievements and encourage them on task-relevant behaviour (Musti-Rao and Haydon, 2011). This shows there is a correlation between positive reinforcement and achieving desired behaviour.

In a cyber security context, punishments are applied to change undesired behaviour. Herath and Rao' (2009) work focused on encouraging information security behaviours in organisations. Their findings suggest that punishment exerts a deterrent effect on offenders. Punishments, alternatively called as penalties or sanction, may include mechanisms such as denunciation, fine, dismissal from job and others. Considering this, punishment and deterrence have overlaps, in that they want to negate poor behaviour using punishment. The deterrence theory originally coined by Hobbes (1651) suggest that perceived threat of sanctions influence personal behaviours through the certainty and severity of punishment, I.e., as punishment certainty and punishment severity are increased, the level of illegal behaviour should decrease. There is considerable prior research related to deterrence in organisational settings including information technology. For example, Straub (1990) notes that deterrence measures are a useful primary strategy for reducing computing abuse. Following this research, Kankanhalli et al. (2003) studied whether the use of punishment led to enhanced security effectiveness and found that deterrents, as measured in man-hours spent in security efforts, led to better security effectiveness. An example of this is the punitive approach by organisations on employees for security breaches due to inappropriate or misuse of their device. In such case their employees are more likely to intend to use their smartphones securely (Ameen et al., 2021). While punishing employees for security misconduct, guilt may motivate people to choosing the right path, however, Tangney et al, (2007) report shame does not operate in the same way. Zhuang (2014) argues that guilt leads people to take greater care, changing their attitudes towards future risk, but that no similar attitudinal shifts are found for shame. When an organisation wants to persuade their employees to comply with procedures and processes, or to cease any unwanted behaviour, they often use fear, retraining, naming and shaming (Reason, 2000). However, blaming and shaming is also a more convenient parsimonious means of constraining the perceived source of the problem to an isolated deviant. This misses the opportunity to carry out a wider review of systems and contextual influences, which could reveal issues which will lurk, undetected, to trip up other employees in the future (Renaud et al., 2021). On the contrary, people can indeed respond to shame with acceptance (Leary, 2022). Leach and Cidam, (2015) suggest that shame can give rise to a reparative response if there is a perception that the situation is reparable (Duhachek et al., 2012). Examples include apologising, the changing of future behaviours, attempts to explain what happened, and to punish oneself, after ruminating about what has occurred (Brookes, 2019).

Considering this, Hense and Mandl (2014) pointed out the behaviourist principles of positive reinforcement and punishment work best in action, sports, and racing games, as players are regularly being provided immediate feedback regarding their actions. In a security context, rewards and punishments are used to either compensate employees for desired behaviours or punishment to deter employees from engaging in poor security practice. However, the security domain does not apply principles of positive and negative reinforcement from the psychology domain. The literature proposes that positive reinforcement may encourage employees to behave in a desired way, and negative reinforcement if used correctly may also assist the use of security in the workplace. Punishing employees for not adhering to cyber security policies may be ineffective to change attitudes and in the long-term, behaviour. Punishing employees fail to recognise pertinent factors that attribute to learning and adhering to cyber security. For example, if an employee experiences security fatigue, it is possible they pay little to no attention to security messages. Consequently, they are punished for a factor beyond their control, and this could become a distasteful experience and negate desired security behaviour.

2.5.2 Social Cognitive Theory

Another learning theory that is typically adopted, is the ‘Social Cognitive Theory’ (SCT), composed by Bandura (1986). The theory states that portions of an individual’s knowledge acquisition can be directly related to others within the context of social interactions, and outside media influences. Also, when people observe a model performing a behaviour and the consequences of that behaviour, they remember the sequence of events and use this information to guide subsequent behaviours. The first factor of the theory is perceived self-efficacy, which is concerned with people’s beliefs in their capabilities to perform a specific action required to attain a desired outcome. Outcome expectancies are the other core construct of SCT, which are concerned with people’s beliefs about the possible consequences of their actions. The final construct includes goals, defined as perceived impediments and facilitators (Conner and Norman, 2015).

The SCT has been widely used in health promotion Thomas et al. (2009) and has become a fundamental resource in clinical, educational, social, developmental, health and personality psychology (Luszczynska & Schwarzer, 2015). It is seen as an agentic and an empowering perspective in which individuals are proactive and self-regulating rather than reactive and controlled either by environmental or biological forces (Schunk and Pajares, 2010). Physical activity interventions grounded in behaviour change theory, like SCT, are widely considered to be more effective than non-theoretic approaches (Stacey et al., 2015). Such interventions typically set out to intervene on the ultimate outcomes (physical activity), but also influence intermediate constructs, which, in turn, are believed to influence physical activity behaviour (Lewis et al., 2002). The SCT suggests that positively impacting the intermediate constructs of self-efficacy, outcome perceptions (the expected benefits and efforts of adjusting health behaviours) (Bandura, 2004), intentions to engage in physical activity, perceived barriers of engagement in physical activity and the setting of physical activity goals, is essential to underpin change in the target health behaviour. In adopting a desired behaviour, individuals initially form a goal and then attempt to execute the action.

In a cyber security context, the SCT is not adopted in models for training and education. Rather the PMT and a subset of Bandura's (1986) social cognitive theory, self-efficacy is used to describe users learning (2.2). However, there are theories such as the Constructivist theory has little to no acknowledgement in the cyber domain. These theories could provide an alternative approach to learners learning.

2.5.3 Constructivist Approach

Constructivism is the theory that says learners construct knowledge rather than just passively taking in information. As people experience the world day in and day out, they reflect upon those experiences, build their representations and incorporate new information into their pre-existing knowledge.

Piaget' (1957) work heavily focuses on how children develop. Although he never linked his research on cognitive development to education directly, his theory plays a vital role in his contributions to learning theories (Brau, 2020). Similar to this, the social constructivism theory was developed by psychologist Lev Vygotsky (1978). A cognitivist argued that all cognitive functions originate in social interactions and that learning did not simply comprise the assimilation and accommodation of new knowledge by the learner; instead, it is the process by which learners were integrated into a knowledge community. He emphasized the role of language and culture in cognitive development. According to him, language and culture play essential roles both in human intellectual development and in how humans perceive the world.

Constructivism, unlike behaviourism and cognitivism, takes a holistic approach, where each learner, individually and socially, constructs their knowledge, meaning while they learn, learners make sense of their external environments by a meaning-making process that depends on previous internal experiences (Mattar, 2018). In the security domain, the Constructivist approach seems more applicable than behaviourism. To elucidate, as Constructivism identifies social and individual constructs, which seems to encompass behaviourism, self-efficacy and the social cognitive theory, in that considers various levels and aspects of influence, rather than one aspect like behaviourism and cognitivism does. For example, learners could acquire ideologies about cyber security from observation (behaviourism) and social media (social cognitive theory), but they can construct their own beliefs and make decisions based on this.

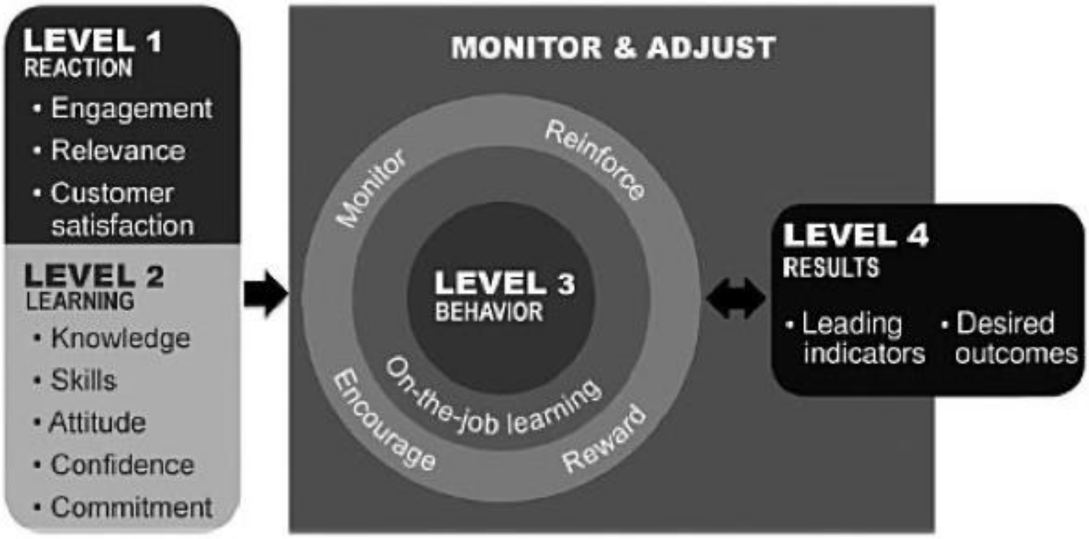
2.6 Evaluation and measurement of training

As well as understanding underlying theories that attribute to learning cyber security. Training evaluation is highlighted as a crucial element to successful learning and knowledge transfer. Training evaluation is a measurement technique that examines the extent to which training programs meet the intended goals. The evaluation measures used depend on those goals and can include evaluation of training content and design, changes in learners, and organisational payoffs. Whereas effectiveness is the study of the variables that likely influence training outcomes at different states (i.e., before, during, and after) of the training process. These effectiveness variables have the potential to increase or decrease the likelihood of successful training outcomes and are typically studied in three broad categories: individual, training and organisational characteristics.

2.6.1 The four-level approach: Kirkpatrick Model (1959)

Alsalamah (2021) argues that the strengths of the Kirkpatrick (2006) model lie in its simplicity and realistic way of helping practitioners think about training programs. Kirkpatrick stated that information about level four outcomes is perhaps the most valuable or descriptive information about training that can be obtained (Choudhury and Sharma, 2019). In the systematic review of training measures, Kirkpatrick and Kirkpatrick (2006) proposed a model suitable for general training, applicable to industry (Figure 1). The model suggests evaluating the four levels:

The reaction is the initial level, this is where the reactions of the training participants regarding satisfaction with the training are measured and recorded directly after its completion. Learning being the second level is where learning success is measured in terms of the scope of changes in attitude and knowledge, while easily measured through scoring patterns at the end of course tests. Behaviour examines improvements in efficiency for example, how behaviour has been altered, by evaluating the transfer of knowledge. Results are where all the effects a measure has on a company's success are to be included in the evaluation. The evaluation serves to examine the effectiveness of training measures and assesses both educational and economic effects of educational processes directly after their completion on three possible levels of effectiveness.



(Figure 1 Kirkpatrick Model of Evaluation, p.56)

The beginning of the model starts with Level 1, the Reaction. This reveals to the student their thoughts about the training experience. The next level is 2, the Learning level. It observes the student's resulting learning and increase in knowledge gained from the training. The final level measures employee performance after training and lastly long-term economic effects concerning organisations success. For example, the Return of Investment (ROI) of training measures, decreases rates of errors and complaints (Tonhäuser, 2016). Despite efforts to train, there is a problem with knowledge transfer and application after the completion of training. As the transfer problem has been widely identified in Professional Development (PD) where researchers and practitioners consistently conclude that the return on many training investments is low and organisational investments in training are too often wasted, a new perspective points out that the transfer problem is not only associated to a lack of adequate training but also a lack of understanding trainee's characteristics at the pre-training stage (Chang & Chiang, 2013). A similar point was identified in a cyber security case study that investigated why training fails to change behaviour, and findings highlighted that vocational training tends to be more persuasive when there is a match between the recipient's cognitive, affective or motivational characteristics and the content of framing of the message (Uskul, 2009), this suggests the importance of trainee characteristics.

Various training evaluation models follow similar structures. For example, the Hamblin model (Hamblin, 1974), Phillips model (Phillips et al., 2004) and Return on Investment (ROI) model (Phillips, 2009). These models adopt the Kirkpatrick model as a foundation for their modified version. The major commonality among these three models is that they are mainly beneficial for business-oriented organisations because their ultimate focus is on the return on investment (Choudhury and Sharma, 2019).

2.6.2 The five-level approach: Hamblin (1974)

Hamblin was one of the first to build on Kirkpatrick's model. The first three levels in his model closely mirror Kirkpatrick's model (see Figure 2). However, the final level is split into two: organisation and ultimate value (Tamkin et a., 2002).

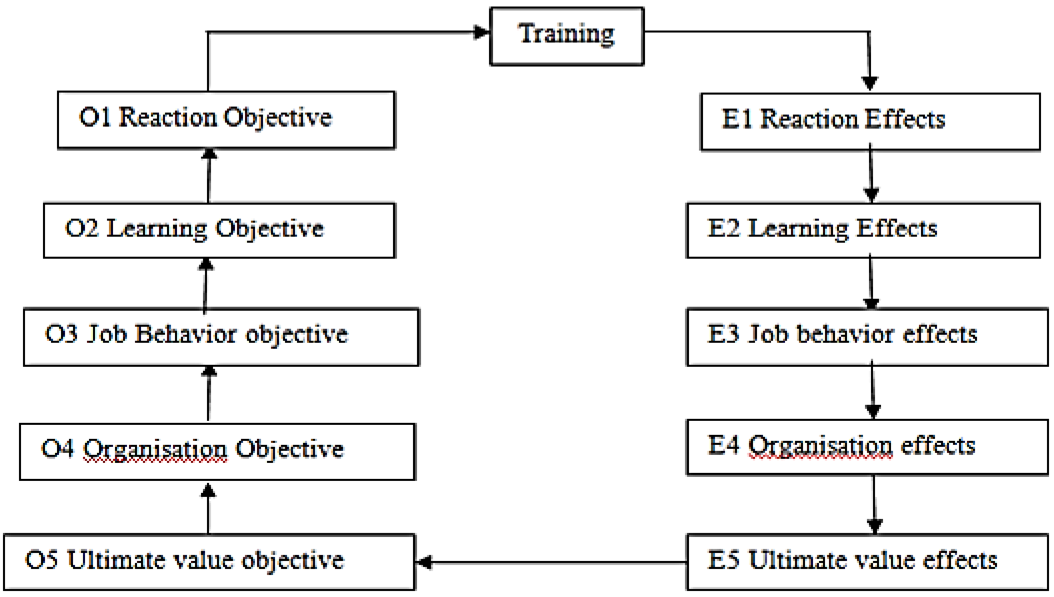


Figure 2 Hamblin 5 Level Framework (Choudhury and Sharma, 2019, p.202

('O' represents Objective and 'E' represents Effects)

The model suggests there is a cause-and-effect chain linking the five levels of training effects. This is defined as: Training leads to Reactions, which leads to Learning, learning leads to changes in Job behaviour, which lead to changes in the organisation and leads to changes in the achievement of ultimate goals.

(Table 1 illustrates the cause-and-effect chain.

Level	Dimensions	Descriptions
1	Reaction	This level represents what participants thought of the program, measured by the use of a reaction questionnaire (Choudhury and Sharma, 2019). It is largely comparable to Kirkpatrick's model where the trainers ask questions about the reactions of learners

		immediately following a course.
2	Learning	These are distinctive changes in knowledge, skill and attitude. This is normally examined through the use of performance tests, objectives tests, skills and task analysis, for example, to record knowledge retained.
3	Job Behaviour	The ultimate objective of the training program is job behaviour and the training is regarded as successful if the desired behaviour changes are achieved. This measures changes in job behaviour and identifies learning applied. To measure the changes, trainees are observed and their level of productivity.
4	Organisation	This measures the effect on an organisation, from participants' jobs to performance changes. This

		includes labour turnover, studies of organisational climate, use of job behavioural objectives to study the behaviour of non-trainees, and workflow studies (Choudhury and Sharma, 2019).
5	Ultimate Value	This level looks at financial effects, both on the organisation and the economy. Training should be defined in terms of the trainee's personal goals (improved financial reward, job opportunity and self-esteem) rather than those of the organisation. Some of this value is in form of the trainee's personal goals (improved financial rewards, job opportunities and self-esteem).

(Table 1, Hamblin Training Model Levels, Adapted from Sharma, 2019)

2.6.3 The five-level approach: Kaufman's Model

Kaufman and Keller (1994) argue that Kirkpatrick's model was designed for evaluating training and that organisations seek to evaluate other types of development events, and they argue the framework needs to be modified.

Based on the Kirkpatrick Models, Kaufman’s five levels of evaluation are as follows:

Level 1a: Input

This level is similar to Kirkpatrick’s reaction level but has been expanded to include the role, usefulness, appropriateness and contributions of the methods and resources used.

Level 1b: Process

This level also has similarities to the reaction level, but it expanded to include an analysis of proper implementation of intervention in terms of achieving its objectives.

Level 2: Micro (acquisition)

This is similar to the learning level and examined individual and as small-group mastery and competence.

Level 3: Micro (performance)

This links closely to the behaviour level in the Kirkpatrick model. This level examines the utilisation of skills and knowledge. The focus is on application rather than the transfer of skills and knowledge.

Level 4: Macro

This links closely to the results level in the Kirkpatrick model. This level examines organisational contributions, in terms of performance improvement evaluations and a cost-benefit analysis.

Level 5: Societal Outcomes

Kaufman’s fifth level focused on what he terms ‘mega-level clients’. This could be seen as a business clientele and or/to society.

The main difference between these models showed that the Kirkpatrick model has the power to give valuable information about our learners, their needs, what works for them, what does not work for them, and how they can deliver better performance. This is crucial for training evaluation to effectively measure the level of education in companies (Pineda-Herrero, 2010).

2.6.4 Context, Input, Process and Product (CIPP) Evaluation Model

The CIPP model was proposed by Stufflebeam (2003). It combines four stages of evaluation: Context Evaluation, Input evaluation, Process Evaluation, Product Evaluation and Context Evaluation. The first component represents the Context Evaluation. This is where the objective of context evaluation is to define the relevant context, identify the target population and assess its needs, identify opportunities for addressing the needs, diagnose problems underlying the needs, and judge whether project goals are sufficiently responsive to the assessed needs (Zhang et al., 2011). The methods for the context evaluation include system analyses, surveys, document reviews, interviews and diagnosis tests (Dalkey and Helmer, 1963).

Once the goals are assessed, evaluators can move into the input evaluation stage of the model. The second component is the Input Evaluation. This is where it looks at overarching goals, exploring background information and cultural context. The second component is where there is more focus on identifying the key stakeholders and examining the program budget. Information about planning and strategies for implementation including human resources and timeline.

The third component is Process evaluation. This monitors the project implementation process. It asks, “Is it being done?” and provides an ongoing check on the project’s implementation process. It is at this point that the activities of the program are assessed with the focus on continuous improvement, in terms of how well it is executed and what needs to be addressed for change. Process evaluation techniques include on-site observation, participant interviews, rating scales, questionnaires, self-reflection sessions with staff members, and tracking of expenditures (Zhang, 2011).

The final stage is the Product evaluation component. Product evaluation identifies and assesses project outcomes, in a cyber security context this refers to training. The purpose of a product evaluation is to measure, interpret, and judge a project’s outcomes by assessing its merit, worth, significance, and probity. A wide range of techniques are applicable in product evaluations and includes logs and diaries and outcomes, comparison of project costs, achievement tests and rating scales (Zhang et al., 2011).

Although the Kirkpatrick model endorses feedback about the training, it fails to assess potential participant needs or underlying challenges. Pursuant to this, participants could share a lack of engagement and disinterest, and this could cascade to different participants within the organisation (De Jaegher, 2020). At this point, a negative perception could be shared in the business, and negating people from this may become a laborious task. The CIPP model addresses this, by adopting a Content Evaluation component. Unlike the Kirkpatrick model, the CIPP model starts with Context Evaluation. It takes a proactive approach, rather than a reactive approach. For example, the model identifies the target audience and its needs and diagnoses problems underlying the needs, and judges whether project goals are sufficiently responsive to the assessed needs. On the other hand, the Kirkpatrick, Kaufman and Hamblin model assesses behaviour change as the barometer for a successful training program, without observing overarching goals, background information and culture, which the CIPP does. The CIPP model adopts various techniques to gather evaluation, some of which entail questionnaires, participant interviews, on-site observations, personal reflection sessions with staff members and tracking expenditure. Furthermore, the most common activities of evaluation seem to be the evaluation of student performance (i.e., assessment) and there is not enough evidence that evaluation results of any type are used to revise the training design (Eseryel et al., 2001). The thesis supports the CIPP model as it recognises the importance of gathering employee needs, Chapter 8 proposes details to effectively evaluate.

2.6.5 Vocational training

Vocational training is defined as the training in skills and teaching of knowledge related to a specific trade, occupation or vocation in which the employee wishes to participate (Europa, 2021). Vocational training was discovered in the early 20th century. It established vocational training as acceptable for certain future professionals who didn’t need a bachelor’s degree to do their jobs, such as plumbers, factory workers and carpenters (Moodie, 2002). Although vocational training teaches skills and knowledge necessary for a job, it is different to cyber training. The main aim of cyber training is to educate and equip staff against specifically cyber risks. Whereas vocational training focuses on grooming and tailoring individual for a specific job, instead of a specific risk or problem. The literature has minimal information about vocational training in a cyber security domain. This raises the potential question, is cyber security identified as a vocation?

Previous work has demonstrated the success of financial investments in vocational training from two perspectives. Vocational training prepares learners for a specific type of trade or vocation (Tsang MC, 1997). On one hand, the educational perspective primarily focuses on enhancing individuals’ competencies. While the economic point of view considers to what extent this measure enables the transfer of the learned material from a learning environment to one of the practical applications in the workplace. This positively influences the working process and employee performance, producing better economic results (Anitha, 2014). There are, however, considerable ambiguities regarding the effectiveness of further vocational training. Particularly, the efficacy of conventional training measures in the form of seminars, classes, or training is questioned regularly (Amankwa, 2014). However, in vocational training, the question of how the transfer of training problem arises both theoretically and practically and this has not been resolved adequately (Hutchins, 2010).

The main problem associated with the transfer of training is that formalised training measures often involve participants acquiring skills that they do not or cannot apply appropriately in their workplace. According to Weisweiler (2013) in the context of further vocational training, transfer of training is understood to mean the application and generalisation of new knowledge and skills in the workplace. Simply put, it is assumed that these trainees engage in unrelatable training material and often fail to optimally transfer what they have learned in training to their everyday work routine (Tonhäuse, 2016). When applied to cyber security these same vocational training courses have been adopted to try and improve cyber security competencies, but akin to professional development, these skills may not be applied in the workplace. One way to understand the impact of training is in the form of evaluation measures/models, which demonstrate the learning process and outcomes. Furthermore, undertaking a vocational course suggests an interest in the topic (Deci, 2000). On the other hand, cyber security appears to be a workplace imposition regardless of interest or any engagement measure (Ryan and Deci, 2017). Could this mean that motivation is a predisposition for interest, which can increase attention in training and information transfer?

2.6.6 Continual Professional Development in Training

Continual Professional development (CPD) is a process of recording and reflecting on learning and development, while training is the learning process in which individuals get to know about the key skills required for the job (Pianta, 2011). Professional development is typically used to strengthen training outcomes and it can be seen across most industries. For example, teachers advance in their careers through the acquisition of the knowledge and skills required to better address student needs (Benedict, 2014). In a cyber security context, businesses do not offer Continual Professional Development, rather employees complete one-off training, typical of the new employee induction process (Furman, 2011). In this case the employee has no further incentive to advance their career through the acquisition of knowledge with which to better protect themselves and/or employer through cyber security.

2.7 Factors affecting the transfer of training

A well-known framework for knowledge transfer was proposed by Baldwin and Ford (1988), who posited that transfer is a function of three factors. Namely trainee characteristics (individual factors), work environment (or environmental factors) and training design factors (situational factors). Trainee characteristics include ability or skills, motivation, and personality factors. The work environment includes climate factors like supervisory or peers support as well as constraints and opportunities to perform learned behaviour on the job. Training design factors include principles of learning, sequencing, and training content, learning retention. Holton et al. (1997) described that learning affects individual performance which leads to organisational performance. They also stated that individual characteristics and perceptions of environmental forces influence individual performance. Environmental factors include feedback, peer support, supervisor support, openness to change, and personal outcomes also affected individual performance.

In the Kirkpatrick model (2.6.1) reaction and learning play important roles, and training transfer helps organisations and employees achieve their aims with more effective performance. Based on this premise, Holton (1996) developed the Learning Transfer System Inventories (LTSI) model and considered 16 factors, which are likely to influence the transfer of training in the workplace. They are as follows; Learner readiness, Motivation to transfer, Positive personal outcomes, Negative personal outcomes, Personal capacity for transfer, Peer support, Supervisor support, Supervisor sanctions, Perceived content validity, Transfer design, Opportunity to use, Transfer effort performance expectations, Performance outcomes expectations, Openness to change, Performance self-efficacy and Performance coaching.

Alternatively, Noe and Schmitt (1986) conducted one of the first studies to explore the influence of pretraining motivation. They found that a composite measure, including three dimensions of motivation (this is, effort-performance expectancies, performance-outcome expectancies, and motivation to learn), was significantly related to learning and that learning had a significant influence on a measure of job performance (Tracey et al., 2001). These results highlight the importance of pretraining motivation for training effectiveness.

In light of this, Goldstein (1991) stated that the work environment may influence an individual’s motivation to learn and in turn, impact performance during training. For example, Baldwin, Magjuka, and Loher (1991) have shown that characteristics of the work environment, such as the amount of choice afforded to individuals to attend a training program, may have a direct influence on their motivation to learn, as well as knowledge and skill acquisition. They claim that the work environment has three dimensions that influence pretraining, the first is managerial support. The professional and personal relationships between managers and their employees can send strong messages about the value and importance of training. The second dimension of the work environment that may influence pretraining is job support. The third dimension is organisational support. Formal organizational systems, such as the appraisal and reward systems, may play an important role in preparing individuals for training. Baldwin and Magjuka (1991) found that when trainees understood they would be held accountable for learning, they reported greater intentions to use their training on the job.

The analysis of factors affecting the transfer of training shows that Baldwin and Ford (1988), Holton (1996), Noe and Schmitt (1986) and Goldstein (1991) share similar dispositions. There is a commonality in their studies that imply the importance of work environment and motivation. It is important therefore to consider these elements within a cyber security context. Consider, what are the implications of positive motivation, a work environment that promotes liberation and supervisory support for learning? For this reason, factors like motivation, the influence of social environment, leadership styles and memory and attention are further explored (see 2.7.3) with correlation to a cyber security context.

2.7.1 Pre-training Motivation

Pretraining motivation may have an impact on significant training results, according to theories put out in an effort to explain the variables that affect training effectiveness. Baldwin, Magjuka, and Loher (1991), for instance, discovered that pretraining motivation was connected to actual learning in a training programme created to enhance abilities in conducting performance reviews and in offering feedback. Pretraining motivation was linked to classroom performance, according to a different study (Baldwin & Karl, 1987). Finally, Mathieu, Tannenbaum, and Salas (1992) discovered that pretraining motivation for a programme on proofreading skills predicted learning and subsequent performance on a work sample test. According to these research, trainees' pretraining motivation has a significant impact on how much of the information taught to them during a training programme is retained. In this section, the components necessary for a successful training programme are explored. Firstly, a discussion of pre-training motivation, employee knowledge transfer, and the influence of social environments such as organisational culture and leadership style.

Researchers have suggested several steps to follow at the pre-training stage to anticipate a successful training transfer. Prasertsilp and Olfman (2014) suggest that at the pre-training stage, trainers should:

- Identify trainee requirements and set goals
- Develop a training method
- Select trainees and set them in groups
- Create training motivation
- The design required technology for training

Building on the development of training, Roediger, Putnam & Smith (2011) conducted research on the effect of testing after training. They found that the schedule of learning is emphasized over the type of learning involved; individuals will learn better if the practice is spread out over time instead of all at once (i.e., massed practice or cramming). However, evidence shows that cyber security training schedules are not spread out over time. For example, NCSC certified training scheme is designed to assure high-quality cyber security training courses, and average courses are spread from minutes to 3 days (NCSC,2019). Cyber security training often happens one-off (Pfleeger, 2014). This becomes problematic when there is a lack of practice of acquired knowledge and further application of use in the workplace. Practice testing refers to taking practice tests over unfamiliar material by self-testing. Many studies examined the effects of testing on memory retention (Roediger & Karpicke, 2006) and their results support its positive influence on learning.

2.7.2 Employee knowledge transfer

Holton et al. (2007, p.276) defined learner readiness as “the extent to which individuals are prepared to enter and participate in training”. A study conducted by Payne et al. (2008) measured learner readiness in terms of retention of relevant knowledge and skills; and disposition or motivation to retrieve and apply such knowledge. It was found that learning transfer is at a higher level when trainees are confident in their ability to retain the knowledge and motivated to apply such knowledge. This implies that trainees who know the training program are motivated to apply such knowledge to the real world. Similarly, it has been proposed that the anticipation of successful knowledge application from workshop to workplace requires trainees to show three dimensions of readiness at the training stage (Rachmalia 2017). These dimensions are motivational, behavioural, and cognitive readiness, for example, employees who perceive a supportive organisational climate may affect their cognitive and affective states, such as motivation (Chung, 2011). Similarly, behavioural readiness suggests that if people have similar attitudes (for example, physical, social and status traits) with colleagues, training is likely to positively attract trainees (Chung, 2013).

However, if people do not have similar positive attitudes to other groups, they are likely to be less interested, which may affect behavioural readiness (Guillaume, 2012). Bada (2019) researched why cyber security campaigns fail and supported that there is inadequate effort to understand the motivational characteristics of a trainee for persuasive messages. Before the training program, trainees evaluate the training content to see if the training program has practical value. Pre-training perceived utility is reflected in the motivation to transfer training at the post-training stage as well as motivation to learn. In cyber security, motivating participants is key, especially because cyber security processes and procedures are an expenditure rather than a vital process to business operations (Gordon, 2015).

2.7.3 Influence of Social Environment

While identifying the various educational training models, the literature also draws on principles from social and organisational psychology. For example, the influence that managers have on employees, social and cultural anthropology and andragogy. These areas of focus in psychology depict factors that cyber developers fail to acknowledge in the research and development of training of end users i.e., employees of a business. This section dissects a range of factors that could attribute to user behaviour change.

In this context social environment, organisational culture and work environment will be used interchangeably with the same meaning. Culture is the thinking, values and beliefs of the organisation (Ertosun, 2018). Organisational culture is the way things are done in the organization-working environment in the perfect way the organization culture wants to be (Reiss, 2012). Organisational culture is also an important factor that can have a positive security influence on the persuasion process. The delivery of cyber security training is usually preferred when they match the cultural theme of the message recipient (Bada et al., 2019). For example, cultural systems shape a variety of psychological processes, therefore if training suits the cultural norms, trainees are likely to follow it. To create a successful deliverable, cyber security training needs to embed the organisational culture and it should consider employee needs and practices within the workplace. In addition, cyber security training must be formed with employees, rather than imposed upon them, which is linked to motivation. There is also a clear need for visible and vocal contributions from senior management to provide legitimacy, and a clear signal on the importance of, an organisation’s cyber security training (Enisa, 2017). As a result, cultural factors are one of the most important factors for consideration when designing education and awareness messages (Kreuter, 2004).

Several factors in the literature have been identified as important predictors of training effectiveness which can be classified into these categories. These include the usefulness of the course to the trainee’s job (Baldwin and Ford, 1988) and principles of learning used (Decker, 1982). Furthermore, important course characteristics have been identified; self-efficacy (Ford et al., 1992), motivation, job involvement (Noe & Schmitt, 1986), ability (Robertson and Downs, 1989), which are important characteristics of the trainee. Additional characteristics of a course include managerial support (Ford et al., 1992), the amount of control or autonomy available in an employee’s job (Huczynski & Lewis, 1980), or more generally, transfer of training environment (Tracey et al., 1995), which are critical aspects of the work environment. Such features of the work environment have been thought particularly important to the transfer of training (Baldwin & Ford, 1988; Tannenbaum & Yukl, 1992), because while employees may be highly motivated individuals who have attended excellent training courses and are keen to use their new skills, constraints in the work environment may prevent them from applying what they have learned back in their jobs. One of the barometers for success in cyber security training is that needs ought to be embedded in the organisational culture and it should consider employee needs and practices. If cyber security training or activities become too burdensome, there is a risk of employees negating or ignoring cyber security messages and practices being implemented (ENISA, 2017). The influence of culture on trainees plays a significant role in trainees' perceived utility. This refers to a trainee's belief or opinion that the training program content is to be useful for their job (Chang & Chiang, 2013). It is crucial to note that if trainees perceive that the content of the training program is useful, they are more likely to use or apply the knowledge and skills learned from the training program in their jobs. This is exemplified in the Threat Analysis Report (2020), the report investigated the COVID-19 security culture while working from home. The results found that 53% of the participants report not having received any security guidelines from their employees regarding working from home. Results showed that 44.44% of the employees state they had no security advice on their new working reality (Georgiadou et al., 2021). This suggests that if there is an organisational culture that does not value cybersecurity then people in that organisation may perceive it as unimportant. It is crucial to note that previous work on security culture does not appeal to the multi-layered nature of culture (Faily and Fléchais, 2010). For example, previous work describes security culture as a concept influenced by security awareness (Thomson, 2005) or obedient behaviour (Helokunnas and Kuusisto, 2003)

One of the originators of culture (Schein, 1991) defined culture as a pattern of basic assumptions which are invented, discovered, or developed by a given group, and has worked well enough to be considered valid. These are taught to new members as the correct way to perceive and think about those problems. On the other hand, (Da Veiga and Martins, 2015) proposed that a culture must be established in which information is protected from risk and the privacy of the information maintained. This definition differs from that of Schein (1991) in that, this definition does not highlight how culture can be dispersed and shared in an organisation. A review of the literature shows there is no absolute definition of the term 'security culture' as scholars have differing ideas and definitions of what a security culture entails.

2.7.4 Influence of leadership styles

In addition to culture, Taomina (2008), examines the theories on leadership, employee enthusiasm, and lack of cooperation in organisational culture. A significant positive correlation between leadership and organisational culture shows that bureaucratic culture is more important and effective than flexible culture; bureaucratic culture is a highly significant correlation with socialization. Recommendation for the leadership should be flexible, attitudes of leaders are good for the organization and their employees and socialization need management attention in organisation culture. Yiing and Ahmad, (2009), examine the impact of organizational culture on leadership style and employee commitment with respect to job satisfaction, commitment, and performance. The results show that leadership is significantly related to employee commitment and culture plays a significant role to build this relationship, as far as the organisational commitment has a significant relationship with job satisfaction. The recommendation regarding this research is supportive leadership culture in organisation can build a strong relationship between organizational commitment, employee performance, and job satisfaction.

Eraut et al. (2001) examined the impact of the manager on learning in the workplace, and they discussed that the key person is the local manager whose management of people and role in establishing a climate favourable to learning, in which people seek advice and help each other learn quite naturally, is critical for those who are managed. They added that negative models could be a source of learning as well as positive models and often are elements of both. This highlights the influence managers have upon creating a security endorsed culture within the work place. Akin to this, managerial support (for example, encouraging trainees to use new skills and tolerating mistakes when they are practising them) has been identified as a key environmental variable affecting transfer (Ford et al., 1992) and is likely to be of central importance in creating a “transfer friendly” environment (Axtell et al., 1997). Similarly, Marx (1982) suggests that during the initial phases of transfer, when more errors are likely to occur, reinforcement from managers may be particularly critical in helping trainees to maintain the new skills.

An organisation's learning culture which reflects the values and beliefs about the importance of learning at work is positively related to the trainee’s transfer motivation (Zubairy et al., 2015). Kontoghiorghes (2002) shows that transfer motivation is high when trainees understand that they are accountable for the training application, that is when the organization expects trainees to use the training in the workplace. Thus, before the training program even started, the organisation's normative context already functions to promote or hinder the development of transfer motivation. This is vital in cyber security, if trainees take account of their actions there is more attention to transfer knowledge and the appropriate application in the workplace. There is a wide discussion about security-awareness campaigns and their effort to secure the human element, leading to secure online behaviour. In many cases, security awareness campaigns demand a lot of effort and skills from the public, while measures do not provide real insight into their success in changing behaviour. Often, solutions are not aligned to risks; neither progress nor value is measured; incorrect assumptions are made about people and their motivations; and unrealistic expectations are set (Bada, 2014).

In the category of environmental factors, peer support plays an important role in the training transfer process and influences training transfer (Burke & Hutchins, 2007), but this factor has not been examined sufficiently in training transfer models. Some researchers have attempted to examine the role of peer support in training transfer models and proposed that peer support can help trainees learn and maintain new skills. In light of this, supervisor support was examined (Montesino, 2002) and found a positive relationship between supervisor support and training transfer, while others argue otherwise (Chiaburu & Marinova, 2005), but there remains a gap in research in this area. Peer support is integral as it constitutes the social environment of a user and could affect knowledge transfer and application in real-life scenarios.

2.7.5 Motivation

The previous section introduces the notion that employees who experience positive learning culture in the workplace are transferred into trainee motivation. This is developed further in this section, we identify cross-pollinating factors that could attribute to behaviour change in the workplace, namely motivation, memory and attention. These have been grouped because it seems motivation is a driver for individual memory and attention to cyber security.

Intrinsic motivation is the motivation to do something for its own sake, for the sheer enjoyment of a task. Extrinsic motivation is the motivation to do something to attain some external goal or meet some externally imposed constraints. Feelings of self-determination, control, and satisfaction have long been linked to an intrinsically motivated state (Hennessey, 2015). It seems cyber security is adopted by trainees out of obligation, rather than as an intrinsically motivated action (Bada, 2014). The first pedagogical assumption of the need to know is closely linked to motivation. The sense of free will to choose content is an internal motivator that is responsible for ensuring quality in any given experience. If an adult learner does not perceive that a learning event will add value or satisfaction, they are unlikely to be motivated to commit (Ferreira et al., 2018). Adults are motivated to learn to the extent that they perceive that learning will help them perform tasks or deal with problems that they confront in their life situations. Furthermore, they learn new knowledge, understandings, skills, values, and attitudes most effectively when they are presented in the context of application to real-life situations. Adults are responsive to some external motivators (better jobs, promotions, higher salaries, and the like), but the most potent motivators are internal pressures (the desire for increased job satisfaction, self-esteem, quality of life, and the like). Tough (1979) found in his research that all normal adults are motivated to keep growing and developing, but this motivation is frequently blocked by such barriers as negative self-concept as a student, inaccessibility of opportunities or resources, time constraints, and programs that violate principles of adult learning.

The construct motivation was established by Noe and Schmitt (1986) and defined it as “the trainee's desire to use the knowledge and the skills mastered in the training program, on the job” p. [501]. According to the authors, they suggested that motivation to transfer is affected by environmental favourability. Whereas according to Seidel (2012), transfer competence is the employee’s specific disposition. This is a requirement for a change in working behaviour taking place in situations that are characterized by new and/or changed work tasks (Tonhäuser, 2016). Transfer competence is signified by the work environment in terms of context, and by training in terms of content. Intrinsically motivated behaviours emanate from the self and are marked by the enjoyment and satisfaction of engaging in an activity. Conversely, extrinsic motivation refers to the motivation to engage in an activity to achieve some instrumental end, such as earning a reward or avoiding a punishment. Messages tend to be more persuasive when there is a match between the recipient’s cognitive, affective or motivational characteristics and the content of framing of the message. Also, messages are more persuasive if they match an individual's ought or self-guides, or self-monitoring style (Uskul, 2009). People might be motivated to follow a cyber security campaign’s advice but if that causes certain limitations on the sites they can visit online, then this can automatically result in emotional discomfort, thus leading to ignorance of a suggested ‘secure’ behaviour.

To support students’ intrinsic motivation teachers may also present learning activities in need-satisfying ways. The primary way that teachers can present a learning activity in an autonomy-satisfying way is to offer choice (Katz & Assor, 2007). With choice, the teacher allows students to decide for themselves to engage in one activity rather than another or to put themselves in one situation rather than another. The reason why choice is a pathway to autonomy satisfaction is that to make a choice, students initially need to look internally at themselves to consider their interests, goals, priorities, and preferences. When students’ behaviours and decision-making are guided by their interests, goals, and so forth, then students have the sense that their behaviours and decisions originate from within themselves. When choice allows students to pursue their interests and personal goals, then “offer choice” becomes an instructional pathway to autonomy satisfaction (Patall et al., 2013). That said, there is considerable teaching skill involved in offering autonomy and satisfying choices. Before choice can be expected to translate into autonomy satisfaction, it needs to be accompanied by the presence of additional autonomy supportive acts of instruction (e.g., taking the student's perspective). It needs to be meaningful (i.e., an authentic opportunity to explore an interest, pursue a personal goal, or express an identity), and students need to feel competent and informed enough to make that choice (Patall et al., 2021). Earlier research supports this notion, for example, Reeve et al. (2003) gave undergraduates “action choices”, how to allocate their time or “option choices” for example which puzzle to solve. Their study found that action choices have a stronger impact on the sense of psychological freedom and volition and this, in turn, plays a role in intrinsic motivation. Developing and educating employees are today’s necessities as new technology to enhance learning is being introduced periodically so everyone can stay updated and skilled in their usage. A major element of effectively assisting faculty members is to understand the nature of how adults learn best and then create an environment and processes that are conducive to learning effectively (Mujtaba, 2004).

2.7.6 Working Memory and Attention

Attention is described as the ability to select one stimulus, redirect the focus on the appropriate stimulus, focus on many stimuli, maintain focus in a situation where there is no stimulus present, and perform things simultaneously (Kałdonek-Crnjakovi´c, 2018). In life, various situations require people to focus attention on two locations simultaneously, employees may devote attention to emails, while remotely managing customer accounts remote (Huttermann et al., 2013). Attention is directly related to short-term memory, an ability to store information, and working memory the ability to manipulate this information in one's mind over a short period, to perform a wide range of cognitive tasks (Barrouillet and Camos 2014).In addition to this, it is important to note that individuals vary in their attentional abilities, and this could potentially impact knowledge retention from cyber security, and in turn limit knowledge application in the work environment (Matthews et al., 2001). Some individuals have higher attention capacity, while others have reduced attention capacity. This relates to the prevention paradox, a term initially introduced by an epidemiologist. It states that the majority of harm comes from people with moderate problems (Thompson, 2018), in this instance attention issues.

The most relevant aspect of attention that is relevant to knowledge transfer in digital environments is its restricted capacity (Hommel, 2019). Humans have limited neural resources to process the complexity of the surrounding environment. Moreover, research shows there is an infinite number of ways in which we could act in any given situation at any given time. For example, a human makes 35,000 conscious decisions in a day (Hoomans, 2015). The cognitive ability to allocate our attention selectively allows us to prioritise only some elements of the environment while filtering out others (Lodge, 2019). A renowned example of this filtering is known as the cocktail party effect. This is when an individual is standing in a room full of people speaking to one another, very little effort is required to tune into only a single speaker of interest. In this instance, the selected speaker can be understood easily while all surrounding conversations turn into incoherent ambiguous background noise. This phenomenon, selectively attending to only a single auditory source amongst many, shows the cognitive capacity to voluntarily filter information according to our internal goals. On the other hand, there are instances where our attention is captured involuntarily. For instance, at the cocktail party selectively listening to only one speaker, but seemingly from out of nowhere, one hears their name being spoken by someone previously ignored. Auditory filtering would automatically shift to tune into this new speaker, making their conversation clear while the previous speaker's words become incoherent. Therefore, although attention can greatly focus our thoughts and actions on only some aspects of our environment, how we allocate our attention depend on both our internal goals as well as external factors.

From one of the many definitions of memory; memory is the faculty of encoding, storing, and retrieving information (Squire, 2009). Psychologists have found that memory includes three important categories: sensory, short-term, and long-term. Each category has various attributes, for example, sensory memory is not consciously controlled, short-term memory can only hold limited information for a limited time, and long-term memory can store an indefinite amount of information till infinity (Zlotnik, 2019). Each person's working memory capacity varies from one individual to the other and various investigations have demonstrated that individuals with high working-memory capacity out-perform individuals with low working memory capacity on a range of tasks (Robert et al., 2009). For example, individuals with lower working memory may prefer to take in information using a verbatim, shallow, or surface processing strategy, rather than try to extract the message (Engle et al., 1999).

There are voluntary and involuntary forms of attentional allocation greatly impact many other cognitive functions (Posner, 2016). For example, visual memory is the ability to hold in mind visual information, such as shapes, colours or letters for simply a few seconds. Visual working memory provides a type of cognitive buffer that temporarily stores perceptual objects during decision-making and action planning, and its highly predictive of intelligence (Baddeley, 2003). However, this form of memory is restrictive, as lab-based experiments have shown that as more items are required to be remembered, the sphere in which those items can be remembered decreases (Ma, 2014). Given the highly limited capacity to hold items in memory, attentional control can play a contingent role in governing whether a subset of visual information should hold priority in working memory. If a visual object is expected to be more important than others, voluntarily allocating attention to that object improves the precision with which it is remembered, however, this comes at a loss of memory precision for non-attended objected (Bays, 2014). Due to attentional goals, indeed the neural resources involved in holding items in visual working memory appear to dynamically change. Therefore, attentional distraction can result in the ability to hold information in memory even for short periods. On the other hand, there are instances where our attention is captured involuntarily. For instance, at the cocktail party selectively listening to only one speaker, but seemingly from out of nowhere, one hears their name being spoken by someone previously ignored. Auditory filtering would automatically shift to tune into this new speaker, making their conversation clear while the previous speaker’s words become incoherent. Therefore, although attention can greatly focus our thoughts and actions on only some aspects of our environment, how we allocate our attention depend on both our internal goals as well as external factors. Akin to the cocktail party, a work environment may demand full focus and attention on a particular task, for example, writing financial reports for business expenditure, yet there are other discussions and tasks around office business plans, cyber security and the weather. This will cause the individual to zero attention to their primary task, while external discussions become incoherent ambiguous background noise. Although there may be genuine intentions from the trainee to follow cyber security, the cognitive incapacity in human memory can inhibit this, coupled with external factors.

Although there are established training methodologies to ensure optimal training outcomes, this has not always been applied well, especially in the cyber security context. Given the limitation of human memory, training courses may have unrealistic expectations of how much attention people can allocate and remember. In addition, evidence in the literature shows that humans have attentional goals and involuntarily place a priority on these tasks. Therefore, if people are receiving continual notifications from an online environment, then this may reduce their ability to attend to any cybersecurity-related notifications or issues that may arise (Huang and Pearlson, 2019).

2.8 Adult learning (Andragogy)

The term andragogy is derived from the word pedagogy, which means child-leading (Chan, 2010). It was originally coined by the German educator Alexander Kapp in 1833 and it was developed as an adult education theory by Malcolm Knowles (1978). The term 'Adult learning theory' was originally known as andragogy, and wad first defined by the German educator Alexander Kapp in 1833 (Bedi, 2004). For Kapp, andragogy consisted of learning strategies that focused on the adult learner and how to engage them in their learning experiences. By the 20th century, American psychologist Edward Thorndike had shown that, contrary to conventional wisdom, adults do have the ability to learn (Knowles, 1978). From this, Knowles (1978) reframed Kapp's andragogy into a theory of adult education, differentiating it from pedagogy entirely, noting, that adult education required special teachers, methods and philosophy (Wang, 2015). One of his assumptions was that adults learn mainly out of necessity, subsequently, key factors ought to acknowledge when training adults. He identified six characteristics of adult learners (Lieb, 1991, pp. *1-2):*

- *"Adults are autonomous and self-directed: Adults need to be free to direct themselves. Their teachers must actively involve adult participants in the learning process and serve as facilitators for them. Specifically, they must get participants' perspectives about what topics to cover and let them work on projects that reflect their interests".*

- *"Adults have accumulated a foundation of life experiences and knowledge that may include work-related activities, family and responsibilities, and previous education: Learning ought to be connected to this experience base. To achieve this, should draw out participants' experience and knowledge which is relevant to the topic. They must relate theories and concepts to the participants and recognise the value of experience in learning".*

- *"Adults are goal-oriented. Upon enrolling in a course, they usually know what goal they want to attain. They, therefore, appreciate an educational program that is organized and has clearly defined elements. Instructors must show participants how this class will help them attain their goals. This classification of goals and course objectives must be done early in the course".*

- *"Adults are relevancy-oriented: They must identify a reason for learning something. Learning must be applied to their work or other responsibilities to be of value to the. Therefore, instructors must identify objectives for adult participants before the course begins. This means,* *also, that theories and concepts must be related to a setting familiar to participants. This need can be fulfilled by letting participants choose projects that reflect their interests".*

- *“Adults are practical: Instructors must explicitly tell participants how the lesson will be useful to them on the job. Adults want to focus on the aspects of a lesson most useful to them in their work”.*

- *“Adults should be treated as equals in experience and knowledge and allowed to voice their opinions freely in class. Instructors must acknowledge the wealth of experiences that adult participants bring to the classroom”*

According to Knowles (1978) using the andragogic principles, the instructor can tailor the instruction to meet student interest by involving the students in planning the learning objectives and activities and solving real-world business problems. The principles promote trust between the student and the instructor and enhance self-awareness in students, this buttresses the first andragogic characteristic Knowles (1978) stated that needs to be acknowledged in adult learning. This draws the light on the cyber security training programs, how many content developers consider andragogy when designing training for clients? How many awareness professionals work with their team to identify what their learning needs are, and more specifically what knowledge gaps they have and how best cyber training can assist in addressing them? In crisis-oriented training, employees are likely to think, how do I get out of this situation? Rather than, how can I better understand this situation to prevent it from occurring again? Under such circumstances, anxiety may produce short-term efforts, but not long-range results. Instead, training should have short-, medium-, and long-range objectives, and should attempt to achieve and maintain specific standards. In addition, it should be viewed as a company-wide process in which technical, managerial, and conceptual skills are cultivated. The key to effective training is proper scheduling of training activities that-based on a systematic need analysis-are congruent with the overall organizational plan. A schedule of training activities that provides all employees with an awareness of their own performance standards, the performance standards of the organization, and the activities of fellow employees at the same organizational level fosters cooperation, rather than competition, among employees (Ference, 1982).

According to Knowles (1987, pp. 168-179), there are four basic questions for structuring any learning experience:

- *“What content should be covered?”*
- *“How should the content be organized?”*
- *“What sequence should be followed in presenting the content?”*
- *“What is the most effective method for transmitting this content?”*

Under an andragogic approach, the teacher’s role is to design a process whereby the learners both help create their answers to these questions as well as participate in their implementation. Furthermore, Knowles (1987) outlines certain principles are the basis for creating practices and procedures that guide the organisation and provision of andragogic learning experiences. They are as follows:

- *The adult learner must be able to define what they want to learn (this is governed by personal need, intrinsic motivation and autonomy).*
- *The plans for the learning program should be made jointly between “teacher” and “student”.*
- *The adult must be involved in the evaluation of the learning program.*
- *The environment of the learning program must be safe and non-threatening.*
- *The program should relate to and include the adult’s existing experiences and cognitive structure.*
- *Learning activities should be experiential and “hands-on” rather than passive and pedagogical.*
- *Learning should lead to practical solutions to experienced problems. The curriculum should be problem-based, rather than subject.*
- *The proper role of the “teacher” is one of process facilitator and co-learner rather than a content expert (Clardy, 2005 pp. 10).*

Knowles (1987) andragogic principles seem to not have been applied in a cyber security training context. The development of training content for cyber security has little to no attributes of andragogy, however, if it was applied to cyber security, it would mean employees could define exactly what they desire to learn as step 1 says in Knowles (1987) principle. There seems to be a correlation between step 4 and organisational culture. For example, if the security culture in the workplace is positively reflected and is safe, this could contribute to the learners learning experience. In addition, Knowles (1987) step 5 states, that programs should relate to and include adults' existing experiences and cognitive structure. This concept seems to relate to constructivism, in that learners construct knowledge, and training programs should accommodate these constructs in the training content. This means rather than receiving irrelevant content, employees are learning about topics pertinent to them. Knowles (1987) translates these principles for adult education into the following practices and procedures. Learners should be prepared for the learning program: This is informing the learner of the differences between being taught and self-autonomous learning, how to build learning relationships, how to identify learning resources, and the skills of self-directed learning (Knowles, 1984). A climate conducive environment for learning should be created: Although it is equally important to ensure a physically comfortable environment. The real focus must be on creating a psychological climate of safety, acceptance, trust and respect. There are similarities between climate conducive and organisational culture, as they both seek to create comfort learning in organisations (Reiss, 2010). In a cyber security context, the preparation and readiness of the awareness professionals on one hand, and employees (learners), on the other hand, play a significant role in creating a conducive learning environment in adult education (Leberman and McDonald, 2016). The participants must be physically prepared and ready to participate in the learning activity, even when the facilitator has made advance preparations in terms of intellectual development and the necessary skills. These can be accomplished if the setting is one that encourages learning (Madu and Obiozor, 2012).

A mutual planning procedure should be used: that involves the learner in planning what the learning will cover. According to Knowles (1984) this is a cardinal principle of andragogy. Diagnosing learning needs: One simple way to include the adults in planning involves the following process.

- *The first way is to establish desired learning competencies and the learner's current abilities.*
- *The second way is to identify discrepancies between those desired competencies and the learner's current abilities are noted. The result is a self-assessment of what the learner wants to learn.*

- *Specifying learning objectives: The adult should be involved in establishing learning objectives. Learner input does not have to be the sole, determinative or final basis for defining objectives.*
- *Designing the learning program: The adult should be involved in selecting and planning the sequence and nature of learning experiences and resources used in the process.*
- *Operating the program: This is where the teacher acts more in the capacity of the training facilitator, resource person and mutual student than as an independent expert. Knowles (1978) identified several specific actions that a teacher should perform to execute the role of a facilitator. This includes creating the right mood or atmosphere; helping participants clarify learning expectations and intentions; organising and making available a wide range of learning resources.*
- *Program evaluation: The learners should evaluate how well their learning outcomes were met, the adequacy of their learning as well as their progress with the material.*

These functions, then, represent how the learner's environment acts on the individual. These are the external conditions of learning that, when combined with certain prerequisite capabilities within the learner, bring about the desired change in performance (Knowles, 2014). Andragogy may be seen as a principle related to 'Program Evaluation' in the CIPP Model. For example, the final stage of the model is the 'Product evaluation' that identifies and assesses project outcomes. The purpose of this stage is to measure, interpret and judge a project's outcome by assessing its merit, worth, significance and probity. Akin to this, one of Knowles' principles for learning states that "Program evaluation procedures can help determine if the participants in the learning activity reached their educational objectives and desired outcomes; they can be used in the planning process and for program improvement, and they can be used for program justification and accountability" (Galbraith. 1990, p.8-16). This shows there could be an overlap in the CIPP model and andragogy, in that both the model and andragogy, aim to determine if the training achieved the intended goals and outcome. If these were adopted in a cyber security context, then businesses may begin to be able to measure training worth and significance. Doing this may enable businesses to establish if the training meets learning outcomes and therefore make informed decisions about training. Lawson (1998) supports the importance of andragogy in helping adult learners make career transitions and claims that andragogy can be a powerful tool in influencing the delivery of services to adults.

It seems from Knowles (1987) principles, we can gather the importance learners have in the selection and development of cyber security training. It highlights the expected involvement learners ought to have to ensure successful adult learning. In a cyber security context, these principles are not applied to the selection, development and delivery of cyber training? How many content developers apply this and involve learners? If these principles were applied it would seem to create a learning conducive atmosphere for learners (Leberman and McDonald, 2016), learners would be motivated to learn because they had direct involvement (Knowles, 1987) in selecting training content and training material would be relevant to learner needs. This study adds knowledge to cyber security training for adult learners, these are conveyed in 0

Content Developer Results.

2.9 Content Developers

In this section, the role of content developers is discussed highlighting relevant industries to which it applies. Recent blogs and articles have put forward that content developers research, prepare, write and edit online content and are responsible for developing a company's company strategy as well as creating its deliverables. However, there is no clear and consistent definition. The role of content creators has been used in business-to-business (B2B) marketing. Branding and marketing communications have recently become significant managerial areas in B2B marketing (Mäläskä et al., 2011). For instance, sharing content by like-minded professionals within brand communities has increased, which promotes B2B connections (Andersen, 2005; Bruhn et al., 2013). Additionally, many social media platforms, like Facebook, Twitter, Slideshare, and blogs, have drawn increased attention for B2B marketing since they enable quicker and more individualised interactions between clients and suppliers, which deepens ties (Kho, 2008). However, in the cyber security domain the role of a content developer is rarely discussed, nor is there amass research about the importance of their role and what it entails. Therefore, in this research a different perspective is represented to highlight who content developers are and the importance of relevant content.

Taatgen (2021) has highlighted that for training to be effectively transferred, contents should reflect and be identical to the actual job task. Similarly, Veleda et al. (2007) suggested that for a higher level of training transfer, trainers should ensure that training contents match the actual job task. These similarities help trainees to visualise related training with their actual job, which ultimately helps trainees to apply learned skills and knowledge at the workplace. Bhatti and Aldossary (2021) conducted a study on the effect of training effectiveness, and the effects of training contents, social support and instrumentality on the transfer of training. The findings of their study suggest that training contents are critical for a higher level of training transfer because when trainees observe training contents that are similar to their setting, they feel confident in transferring the learned skills and devise teaching strategies that are compatible with the training contents. On the other hand, if training contents are not similar to their work setting, training transfer will decrease, and all resources and efforts allocated by the management will be wasted. For example, if the training programme is about the safe use of modern technologies, and these technologies are not available in the rea educational setting, the training transfer will slow down (Bhatti and Aldossary, 2021). It is therefore always advisable that training contents should be familiar with the actual educational setting to maximise the rate of transfer. Bhatti et al. (2013) observed that when trainees found training content similar to the real educational settings, they would show more confidence and actively participate in the training activities. In turn, they would believe that when training contents were similar to their job, it increases their job tasks and ultimately increase their job performance.

Equally important as identifying the vital behaviours that people must enact is identifying the crucial moments when they are most likely to fail in meeting these goals (Patterson et al., 2011). There will be moments when people are much more likely to fail, whether it be a beginner at fitness who quits when they get the flu or an office IT user who allows someone tailgate via the back door because she doesn't want to appear unpleasant. Security professionals can enhance the possibility that their users succeed if they can foresee these situations and either offer individuals with the tools to deal with them beforehand or leverage personal, social, and environmental elements to provide enough incentive at these crucial times (Robinson, 2013). By keeping lines of communication open, they can also collect data on when and why people fail and use that feedback to improve the program (Patterson et al., 2011). Influence strategists need to identify vital behaviours, meaning behaviours which they wish to change before they start trying to change them. Equally important is identifying the crucial moments when they are most likely to fail in meeting these goals (Patterson et al., 2011).

2.9.1 Supporting adult learning through Training Facilitators

When we look at the concepts of teaching, Carl Rogers (1969) is a known theorist. Rogers (1969) defines the role of the teacher as that of a facilitator of learning. He claims that the critical element in performing this role is the personal relationship between the facilitator and the learner, which in turn is dependent on the facilitator's possessing three attitudinal qualities. They are as follows: (1) realness; (2) prize, acceptance and care and (3) empathetic understanding and sensitive and accurate listening. Rogers (1969, pp. 164-166) provides the following guidelines for a facilitator of learning:

- *"The facilitator has sole responsibility to do with setting the initial mood or atmosphere of the group or class experience. "*

- *"The facilitator helps to elicit and clarify the purposes of the individuals in the class, as well as other general purposes of the group. If the facilitator is not fearful of accepting contradictory purposes and conflicting aims and can permit the individuals a sense of freedom in stating what they would like to do, then the facilitator is helping to create an atmosphere for learning. "*

- *"The facilitator relies on the motivation of each student to implement training purposes that have meaning for him or her as the motivational force behind significant learning. Even if the motivation of the student is to be guided and led by someone else, the facilitator can accept such a need and motive and can serve as a guide. For the majority of students, the facilitator can help to use a particular individual's drives and purposes as the moving force behind their learning".*

- *"The facilitator endeavours to organise and make easily available the widest possible range of resources for learning. For example, writings, materials, persons, equipment, audio-visual aids- every form of resource that the student may wish to use for their enhancement and the fulfilment of their purposes. "*

- *"The facilitator regards themselves as a flexible resource available to be used by the group. They are available as a counsellor, lecturer, and advisor, a knowledgeable person with experience in the field ".*

- *“The facilitator accepts the students' emotionalized attitudes, endeavouring to give an approximate degree of attention to the individual or the group.*

- *As the acceptant classroom climate becomes established, the facilitator is increasingly able to become a member of the group”.*

- *“The facilitator takes the initiative in sharing their thoughts with the group. The facilitator takes an unbiased approach, to ensure they do not impose or dissuade students. The facilitator is at liberty to share their feedback as individuals to students, personal satisfaction or disappointments. In such expressions, it is the facilitator’s “owned” attitudes that are shared, not judgements of evaluations of others”*

- *“Throughout the training experience, the facilitator remains observant of the body language and expressions indicative of deep or strong feelings. These may be feelings of conflict, pain, and the like, which exist primarily within the individual. This is where the facilitator endeavours to understand these from the person’s point of view and to communicate their empathy to the students. If the facilitator accepts such attitudes or tensions, they can help to bring them into the open for constructive understanding”.*

- *“The facilitator endeavours to identify and accept their limitations. When they experience non-facilitative attitudes, they will endeavour to get close to them, to be aware of them. Once the facilitator has expressed their concerns and frustrations, not as objective facts in outward reality, they will find the air cleared for a significant interchange with the students. Such a dialogue can go a long way toward resolving the attitudes demonstrated by the learners and thus make it possible to be more of a facilitator for the learner*

If there was an application of Roger’s (1969) guidelines in cyber security for adult learning, there is a potential this could create a conducive learning environment (Reiss, 2012) where employees are comfortable to share attitudes and thoughts about security. In doing so, awareness professionals may observe employees’ feelings and consequently address them (Rogers, 1969). According to (Mujtaba 2004, p.74) “A major element of being or becoming an effective educator involves understanding how each group of participants learn best and then integrating activities that best suit their learning styles regardless of teaching modality”. Furthermore, adults have accumulated a foundation of life experiences and knowledge that may include work-related activities, family responsibilities, and previous education. While considering the characteristics of adult learners (Knowles, 1987, facilitators should acknowledge the wealth of experiences that adults bring with them that can be integrated into the learning modules (Holmlund et al., 2022). The facilitator or trainer should effectively balance the presentation of new material, discussions, sharing of relevant experiences, and the time allotted. Trainers and facilitators should recognise that adult learning is aligned to problem-oriented, personalised and the need for direction and personal responsibility (Taylor, 2013). Collaborative learning experiences are normally designed and implemented based on pedagogical principles, whilst security issues are largely ignored (Camp, 2011). This may lead to undesirable situations that have a detrimental impact on the learning process and its management, such as students falsifying course assessments, presenting a convincing false identity to others, intrusion upon controlled or private conversations, alteration of date stamps on submitted work, and a tutor gaining access to the personal data of students (Bandara, 2014).

2.10 Chapter Summary

This Chapter outlined the current disposition the cyber domain hold about the barriers to learning cyber security, for example, fear appeals, self-efficacy and the Protection Motivation Theory (PMT). It is apparent that the computing domain place an onus on employees, for example, their learning is reliant on their personal judgement and through Cyber Security Culture (CSC). However, this perspective fails to recognise learning theories pertinent to adult learning and factors that affect learning like attention, motivation and organisational culture. This was followed by underlying theories about learning and introduced theories that could be applied to cyber security to further understand barriers to learning. Next, learning evaluation models were highlighted, and the strengths and weaknesses of each model were evaluated and applied to security. Then specific, factors affecting the transfer of training were highlighted, for example, motivation and attention, the influence of social environment and leadership styles. The final part of this Chapter identified what adult learning is through the lens of andragogy, what training development should look like and support learners through training facilitators. Overall, the literature highlights some challenges in adult learning. For example, cyber security does not apply learning principles from a psychological domain which could suggest that training is unsuitable for employee needs. The literature also highlights that cyber security training does not apply principles from andragogy, to add to this, training is developed without learner knowledge which is also pertinent in andragogy. From the literature review, the next (Chapter 3) focuses on the development of the rationale and the methodology of the research.

2.11 Research Questions

The research plan changed over the course of the research project; this is discussed in 3.1.1. As a result of this Study 1a and b, do not have research questions about the research, instead there are proposed aims and objectives to encourage discussion and themes ahead of **Error! Reference source not found.**.

2.11.1 Study 1 Aims

- To investigate the existing cyber security training procedures intended for behaviour change.

- To investigate the relationship between social environment, attention and motivation.

2.11.2 Study 1 Objectives

- To explore the influence of the social environment in the workplace on cyber security, SMEs will be interviewed.
- To review the current literature to identify gaps in cyber security training, by evaluating the Education and Training domain.
- Participants will undergo interviews to explore if cyber security training considers user requirements, motivation, or training outcome.
- Participants will be asked what social environment factors affect their attention

The research questions for Study 2 are as follows:

1. How do content developers cyber training selected, devised and delivered?

2. How does the procurement and delivery of cyber training affect how people receive, retain and apply cyber knowledge in the workplace?
3. How does organisational culture affect how cyber training is perceived in the workplace?

2.11.3 Study 2 Aims

- To identify the procedures and processes content developers take to create and deliver cyber training
- To identify what factors, affect users from learning and changing behaviour.
- To identify if any communication between content developers, end users or awareness professionals.
- To understand challenges SMEs, have with cyber training.

2.11.4 Study 2 Objectives

- Gather data to understand user challenges with cyber security and how this could affect their learning and application of cyber security measures.
- Interview awareness professionals who look for cyber training for staff in their business.
- Interview end users/employees who receive training.
- Interview content developers, those that procure cyber training for businesses.
- Analyse collected data to identify if any correlations between content developers training, awareness professional's concerns and end users need.
- Participants for cyber security training will be investigated, to explore cyber security training and if any preliminary factors are considered.

Chapter 3 Methodology

3.1 Chapter Introduction

In this section, the research challenges are discussed alongside, the original research plan and the strategies to circumvent the challenges. The research methodology is then presented in a Venn-diagram, followed by the results from a pilot study. This Chapter discusses the rationale for the chosen methodology.

3.1.1 Original Research Question

The project originally collaborated in a larger project called the 'Scalable Cyber Treatments Accelerating Productivity Practice for SMEs' (SCI > APPS). SCI>APPS was an integrated training and self-support research programme. The aim of the SCI>APPS research trial was to ascertain the best way of overcoming the barriers that SMEs face when attempting to increase productivity through behaviour change. However, the project was renamed to 'Cyber Well' during the project. The primary research questions for the Cyber Well project aimed to evaluate, 'Does the deployment of a cyber game with nudge learning increase the cyber and data knowledge resilience in SMEs? Does this style of teaching encourage attitudinal changes and increase productivity in SMEs related to cyber behaviours and certification in a more effective way than typical cyber push-learning training?'. The project was not solely governed by this research, but instead by the Department for Business, Energy and Industrial Strategy (BEIS) project leaders, hence why these research questions were asked. However, there was an opportunity to draft interview questions, input related questions for this research and also conduct the interviews.

3.1.2 Original Project Plan

The original project plan had a control group intended to provide SMEs with just basic information on data management and cyber security via an electronic newsletter and presentation. The idea was to distribute an online survey to evaluate participants' initial aptitude and knowledge, followed by a film-based webinar. The trial would have used a randomised control approach (RCT) to examine the impact and value of two flexible and innovative behavioural change interventions. The trial would have used a webinar in a Randomised Controlled Trial (RCT) to examine the impact and value of an innovative behavioural change treatment focused on Cyber and Data management learning and video delivery techniques. A control group would've run in parallel to the treatment, providing SMEs with just basic information on data management and cyber security via a PowerPoint presentation.

After the webinar, the participants would've completed a final survey to measure their post aptitude and knowledge after engaging in the webinar. The survey was developed independently from the PhD research, which meant some of the survey questions were not supported by the literature. However, some of the outcomes from the survey would provide a baseline of current attitudes and aptitudes toward cyber security. The survey questions would have contained questions relating to attitudes and items relating to knowledge. Attitude items would've been grouped into four categories (1) attitude towards the importance of cyber security policies, (2) attitude towards cyber risks, (3) confidence of where to seek external cyber security advice, (4) and attitudes toward good cyber security practice. In each instance, a lower score on an individual item or sub-scale would've represented a more positive or productive attitude towards cyber security. Knowledge items would've consisted of multiple-choice questions, with participants receiving a score out of 15 for how many of the 15 items they gave the correct response for. The attitude and knowledge questions would've been identical at each of the main stages of data collection, namely at baseline, at end of training and at two-month follow-up. The questions would have been coded to match the correct variables. In reporting terms, for the knowledge measure questions, a higher score is a better score. For the attitude questions, a lower score is a better score, since it represents a less risky attitude.

At the end of the second part of the survey, the original plan was to conduct interviews to evaluate any differences participants observed at the beginning of the initial aptitude and knowledge survey or after the webinar. The purpose of the second survey would've been to capture any differences in behaviour and attitudes from the beginning of the first survey to when they completed the pre-recorded training. Any disparities or differences in their answers could later be questioned in the next phase, the interviews. The interviews would've helped the team measure how the SMEs felt about their increased understanding of cyber security and assess ways in which behaviour change and knowledge transfer were impacting their current or future productivity.

On the contrary, there was an opportunity to give input in the design of the data collection and in turn use this for the PhD research. The original bid for the project aimed at 300 participants, however, the project launch date was the same as the first UK lockdown in March 2020, and therefore the target number was not reached. The total number of participants that signed up reached a total of 166. The survey would've followed up with interviews, specific to motivation, the influence of an individual's social environment in the workplace and questions regarding cognitive dissuasions, such as attention. The survey was part of a larger project, which meant there was limited direction from the PhD itself, however, the results served as a baseline for employee attitudes and knowledge skills.

After COVID 19, the businesses the project targeted and signed up, slowly withdrew. The gravity in which the pandemic came, affected the direction and outcome of the project. For example, the initial target number of participants was 300 SMEs. Due to various reasons, primarily the fact that the research project launched on the day of the first UK lockdown in March 2020. The total number of participants that signed up reached a total of 166, however, only 67 completed and returned the questionnaire. The BEIS team restructured the project to match the current state of affairs, i.e., COVID-19. This meant that the direction of the project changed. Rather than investigating the effect of cyber game on learning and productivity, the project transformed into 'A design to test innovative new ways of encouraging Small and Medium sized Enterprises (SMEs) to adopt existing technologies and management practices to improve their productivity. Likewise, the project name changed to 'Cyber Well' to reflect the vision of the restructured project.

3.2 Research Challenges

There were challenges beyond the control of the project, mainly COVID-19, which meant some ideas to collect data were circumvented, redesigned or cancelled altogether. For example, the project data collection started in 2019, with a project affiliated with the Dorset Growth Hub. The Dorset Growth Hub is funded by the European Regional Development Fund and offers professional guidance to Dorset pre-starts, start-ups and micro businesses and SMEs looking to grow. The idea was to disseminate a webinar training project called 'Psyber SME Business Tool' which targeted Small to Medium-sized Enterprises (SMEs). The overall aim of the project was to capture preliminary habits and behaviours toward cyber security and Information Assurance. The project was intended to commence in April 2019, however, this was pushed back till September 2019, and unfortunately, the project was then cancelled. Although the project did not happen as intended, the literature produced useful foundational knowledge about perception, habits and attitudes.

3.3 Study Venn Diagram

As a result of COVID-19 the project structure changed. The structure of the PhD is demonstrated in a Venn diagram. Study 1a is represented in a lighter shade of blue, the BEIS survey that insights baseline knowledge of the participant aptitude. Study 1b BEIS Interview is represented in a sky blue shade, while Study 2 Training Selection is represented in a darker blue shade. The deeper colour also signifies funnelling from a broad subject area (study 1a and study 1b) to a narrower focus area (study 2).

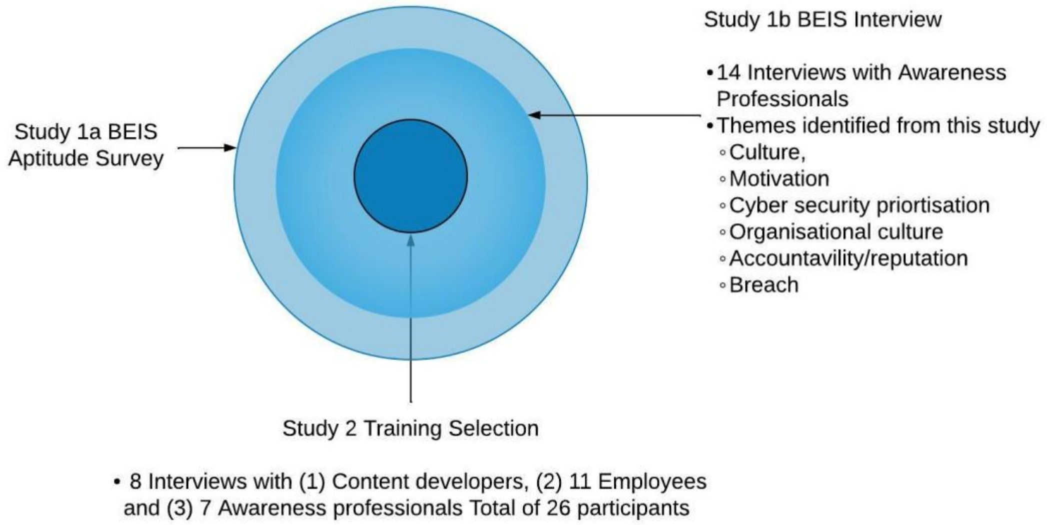

Study 1b BEIS Interview
•14 Interviews with Awareness Professionals
•Themes identified from this study
◦Culture,
◦Motivation
◦Cyber security priortisation
◦Organisational culture
◦Accountavility/reputation
◦Breach
Study 1a BEIS Aptitude Survey
Study 2 Training Selection
• 8 Interviews with (1) Content developers, (2) 11 Employees and (3) 7 Awareness professionals Total of 26 participants

Figure 3 Study Venn Diagram

3.3.1 Revised Project Plan

As described in 3.2 the project structure changed, consequently, the recruitment method changed. Recruitment would come through the Dorset Growth Hub database of about 2000 SMEs, Silicon South and the Dorset Engineering and Manufacturing Cluster. The participants were organisations recruited based on their location, so when the eligibility requirements expanded to include Southwest countries were recruited and eligible. Each organisation that signed up was allotted one place on the research project no more than one person.

The intended participants to engage in the trial were aimed at 300 SMEs (100 per intervention and control) across Dorset’s Creative and Digital (150) and Engineering and Manufacturing (150) sectors. The programme targeted smaller businesses (micros with <10 employees). The total number of participants that signed up reached a total of 166, however, only 67 completed and returned the questionnaire.

3.4 Pilot Study

The pilot study was conducted in anticipation of waiting for potential participants to reply to interview invitations and are not the main results of the thesis. Due to the impact of COVID-19, there was a low response rate from businesses, so therefore, as a precautionary measure, the research took the initiative to explore themes identified in the literature in case there were no future opportunities to collect data. The pilot study took a qualitative approach and there was a total of 4 interviewees participated in the interview.

The main interview focus areas were:

- The culture within the workplace

These questions looked at physical workspace dynamics, frequency of cyber security training, how work dynamics might cause different priorities, the relationship between work pressures and cyber security and if cyber security was a burden.

- Attitude questions

These questions looked at who participants thought was responsible for information security, how much responsibility they take and how often they thought cyber security training should happen.

- Social influence

These questions looked at participant compliance with security policies and whether they complied if colleagues.

- Rewards and Punishments

These questions looked at incentives for compliance, the influence of colleagues on compliance and general motivation to comply with cyber security.

- Health-related questions

These questions looked at health-related issues that could affect cyber security training and whether gender differences contribute to compliance and understanding of cyber security. The themes that appeared in the analysis of the 4 interviews were:

- Prioritise work over cyber security
- Little to no cyber security training
- Work pressure reduces alertness
- Social environment influences behaviour

The interviews were not thoroughly analysed, as they were treated as a pilot study due to a low scale. However, the themes introduced some challenges employees within SME's experience on a day-to-day basis in the workplace, the results saw how these same factors hinder learning and a positive attitude towards cyber security. For example, the perception of how cyber security is seen in the workplace influenced poor security habits. The use of interviews in the pilot study encouraged its application for study 1b and study 2.

3.5 Methodology Rationale

As discussed in 3.1.1, Study 1a and study 1b are part of a larger project, and therefore the methodology was chosen by the BEIS project leaders. The study was broken into Study 1a and 1b. Study 1a is a survey that provides a baseline introductory study into broadly how a trainee's social environment could impact productivity to cyber security. While study 1b investigates the process for selecting, devising, and delivering cyber training to businesses and whether the output of training content address needs on an individual level and organisational level. Study 2 is the main study for this research, and there is full governance and autonomy of the methodology choice. Since Study 1a and study b are part of a larger project, the chosen method was a mixed method approach. Further details about the study 1a's methodology and results are discussed in Chapter 4, followed study 1b's methodology and results in Chapter 5.

Study 1a and study 1b adopted a mixed methods approach, an approach selected by the BEIS project leaders. Mixed methods' is a research approach whereby researchers collect and analyse both quantitative and qualitative data within the same study (Bowers et al., 2013). A mixed method design is appropriate for answering research questions that neither quantitative nor qualitative methods could answer alone (Tashakkori and Creswell, 2007). For example, the research questions for the study were 'Does the deployment a cyber game with nudge learning increase the cyber and data knowledge resilience in SMEs? Does this style of teaching encourage attitudinal changes and increase productivity in SMEs related to cyber behaviours and certification in a more effective way than typical cyber push-learning training'. These are multifaceted questions that neither a single survey nor only interviews would be able to answer. Therefore, a mixed methods can be used to better understand the relationships or discrepancies between qualitative and quantitative data; they can give participants a chance to speak up and share their experiences throughout the research process; and they can facilitate various lines of inquiry that strengthen the evidence and allow questions to be addressed more thoroughly (Wisdom and Creswell, 2013).

3.6 Chapter Summary

In this Chapter, the original research question, alongside the original research plan is discussed to start with. Then the project Venn diagram was illustrated alongside the project challenges. There was a pilot study conducted in anticipation of collecting data and this served as a qualitative baseline ahead of future data collection. Finally, the Chapter discussed the methodology rationale.

Chapter 4 Study 1a BEIS Aptitude Survey

There was an opportunity to collect data through a funded project by the Department for Business, Energy, and Industrial Strategy (BEIS). The studies were divided into, Study 1a and Study 1b. Study 1a represents the BEIS Aptitude Survey, while Study 1b represents the BEIS Interviews. There was an original research proposal called the 'Scalable Cyber Treatments Accelerating Productivity Practice for SMEs' (SCI > APPS). SCI>APPS is an integrated training and self-support research programme. One of the drivers for the project is that smaller businesses' productivity can suffer from poor digital data management and careless cyber security behaviour (Selznick, 2017). The aim of the SCI>APPS research trial will ascertain the best way of overcoming the barriers that SMEs face when attempting to increase productivity through behaviour change. The trial will use a randomised control approach (RCT) to examine the impact and value of two flexible and innovative behavioural change interventions:

- Intervention 1- Cyber and data management webinars and 'nudge' tool
- Intervention 2- The Accreditation Challenge Game online + phone app + 5-minute video case studies.

4.1 Data Analysis from Study 1a BEIS Aptitude Survey

The quantitative data from the Cyber well project was recorded using Qualtrics. This was determined to be the best survey and data management option for this project. The BEIS project ensured consider scalability when making decisions related to data collection. As such, using a high-quality data aggregation management system protects the data from manual error, tracks participant progression, enables sending of automated email reminders and organises the data. Qualtrics would easily support a national roll-out and is considered a reliable, precise Graphical User Interface (GUI) for online data collection (Mathur, 2019).

The survey questions contained items relating to attitudes and knowledge toward cyber security Appendix B Survey Questions). The attitude questions were grouped into four categories: attitude toward the importance of cyber security policies, attitude towards cyber risks, confidence of where to seek external cyber security advice, and attitudes toward good cyber security practice. Knowledge questions consisted of multiple-choice questions, with participants receiving a score out of 15 for how many of the 15 questions they gave the correct response for. The attitude and knowledge questions were identical at baseline, at the end of the training and the two-month follow-up. The questions were coded to match the correct variables. Regarding reporting, for the knowledge measure questions, a higher score is a better score. For the attitude questions, a lower score is a better score since it represents a less risky attitude.

A total of 67 participants provided sufficient data for analysis at baseline. Survey completion at baseline and each follow-up point were characterised by participants either providing a complete set of responses to the survey items or, in the case of a small number of participants, not responding to knowledge and attitude questions at all. Following completion of the baseline measures, participants were randomised into either the control condition or treatment condition. The blocked groups ensured that the mix of micro-SMEs (1-09), small SMEs (10-50) and medium SMEs (51-250) and whether the individuals had a cyber-based job role (IT or non-IT) were distributed as evenly as possible across both the treatment and the control groups. This was done by listing each organisation at baseline in an Excel sheet, stratified firstly by whether the participants work in an IT role and then by organisation size. An extra column was then added, which was filled with random numbers using the random number generator function within Excel. The data was then sorted using this column of random numbers, and the first half of each strata (for example non-IT and micro-SME were allocated to the control group, with the remaining half of the non-IT micro-SME strata allocated to the treatment condition. This was repeated for each combination of IT/non-IT and micro/ small/ medium SME size. From the baseline data, 33 (49.3%) participants in total were allocated to the control condition and 34 (50.7%) participants were allocated to the treatment condition. Of these, 11 (16.4%) participants from the control group and 13 (19.4%) from the treatment group completed the end of treatment survey. A further 7 (10.4%) participants from the control group and 10 (14.9%) participants from the treatment group respectively completed the survey at follow-up. All the companies that completed the two-month follow-up had also completed the baseline survey. Two companies did not however complete the end of trial follow-up, meaning that they only provided data at baseline and two-month follow-up.

It was determined by the BEIS team that a sample size of 269 would be required for the planned inferential analysis, based on the requirements to detect a medium effect size (f = 0.25 standard deviations), a criterion of 0.05 and a power against the alternative hypothesis of 80%. The achieved sample size was markedly lower than this value, suggesting that the planned inferential analysis would be unreliable if it were to be undertaken. On that basis, the decision was made to limit the quantitative analysis to descriptive analysis only. The project team decided to increase the qualitative interview analysis to substantiate the available quantitative data with richer insights.

4.1.1 Descriptive analysis

The mean values in Figure 4 to Figure 8 are for four attitude measures at baseline, end of treatment and two-month follow-up, split by the full sample at each time point and by the sample of participants who completed the survey at baseline and at both follow-up points. Note that a lower score represents a more positive attitude. As can be seen, there was an improvement in each of the four attitude scores from baseline to post-treatment and two-month follow-up. [Figure 20] to [Figure 34]. Appendix B depicts the responses to each of the individual attitude questions (Appendix C Response Rate for response rates).

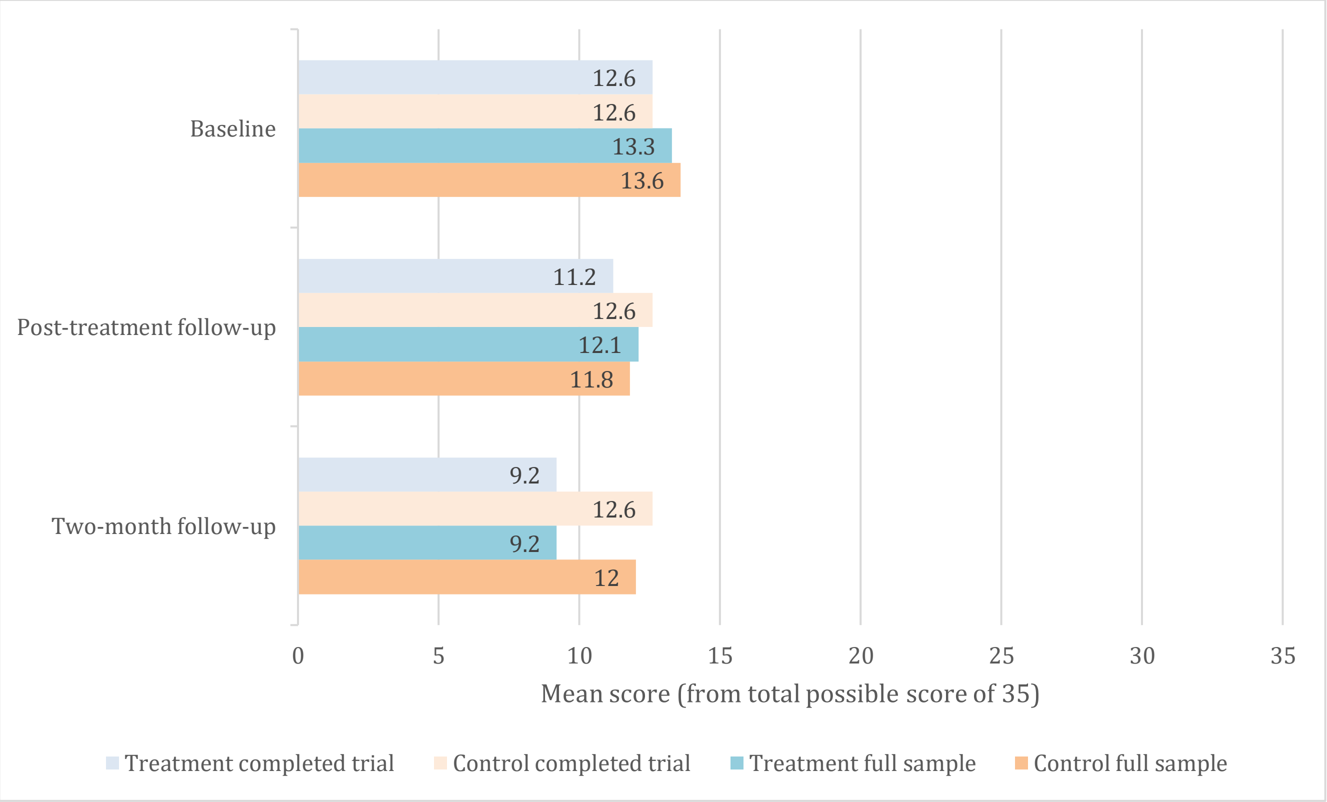


Figure 4 Changes in attitude towards importance of cyber security at baseline, post-treatment follow-up and two-month follow-up in both treatment conditions.

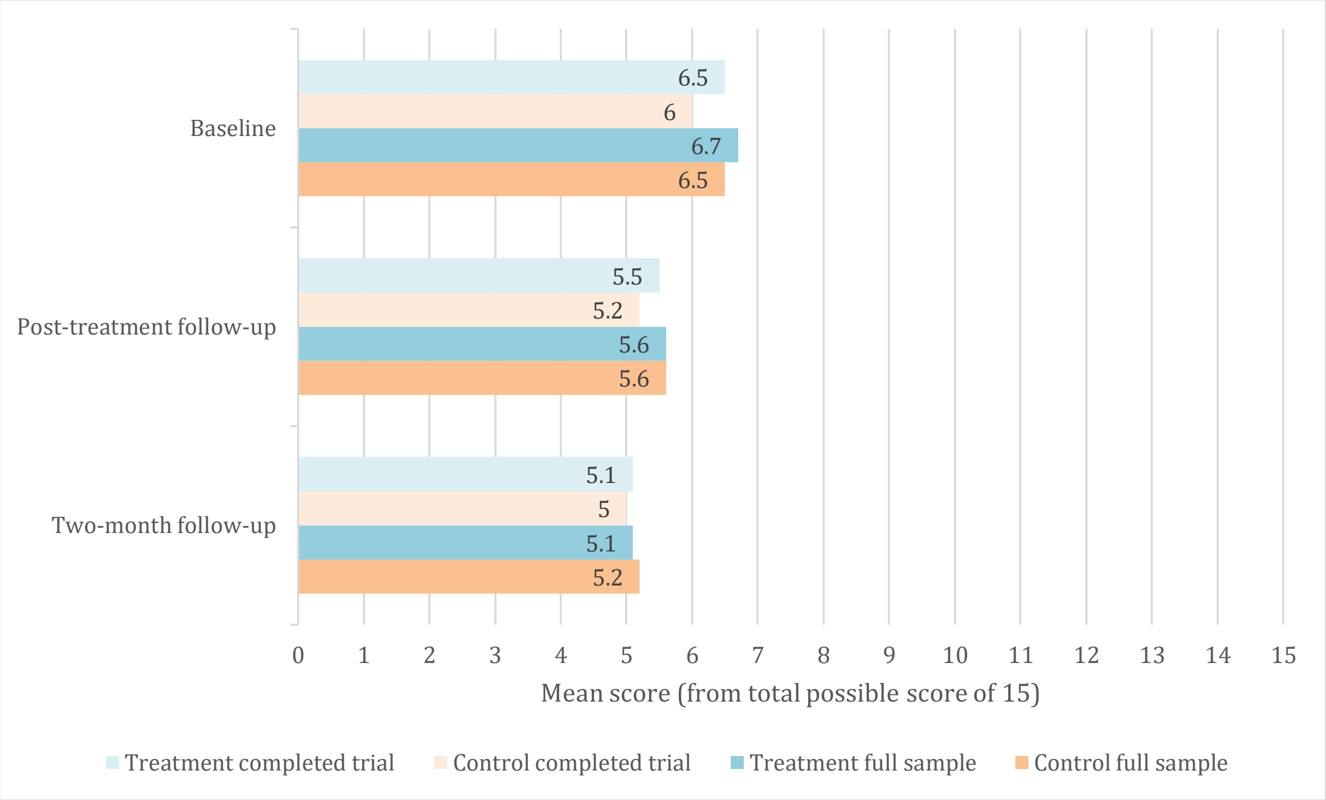


Figure 5 Changes in attitude towards cyber risk at baseline, post-treatment follow-up and two-month follow-up in both treatment conditions.

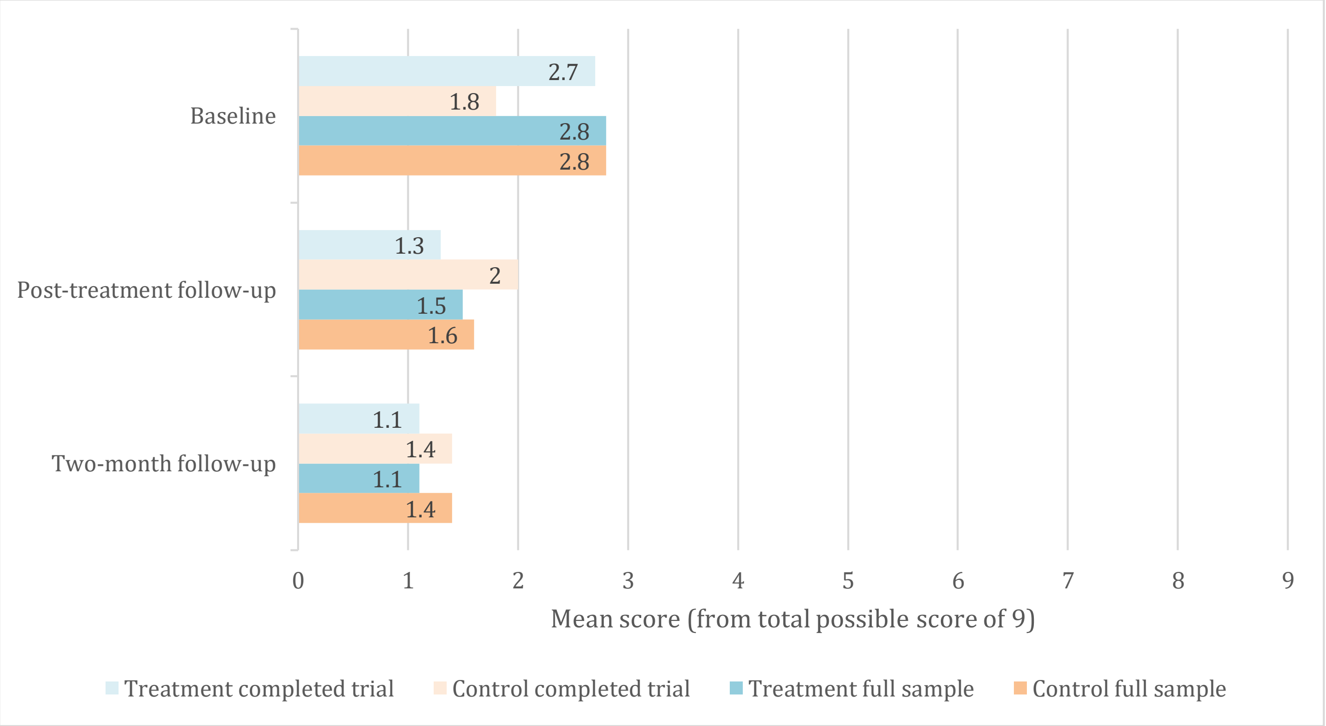


Figure 6 Changes in attitude towards seeking external support for cyber issues at baseline, post-treatment follow-up and two-month follow-up in both treatment conditions.

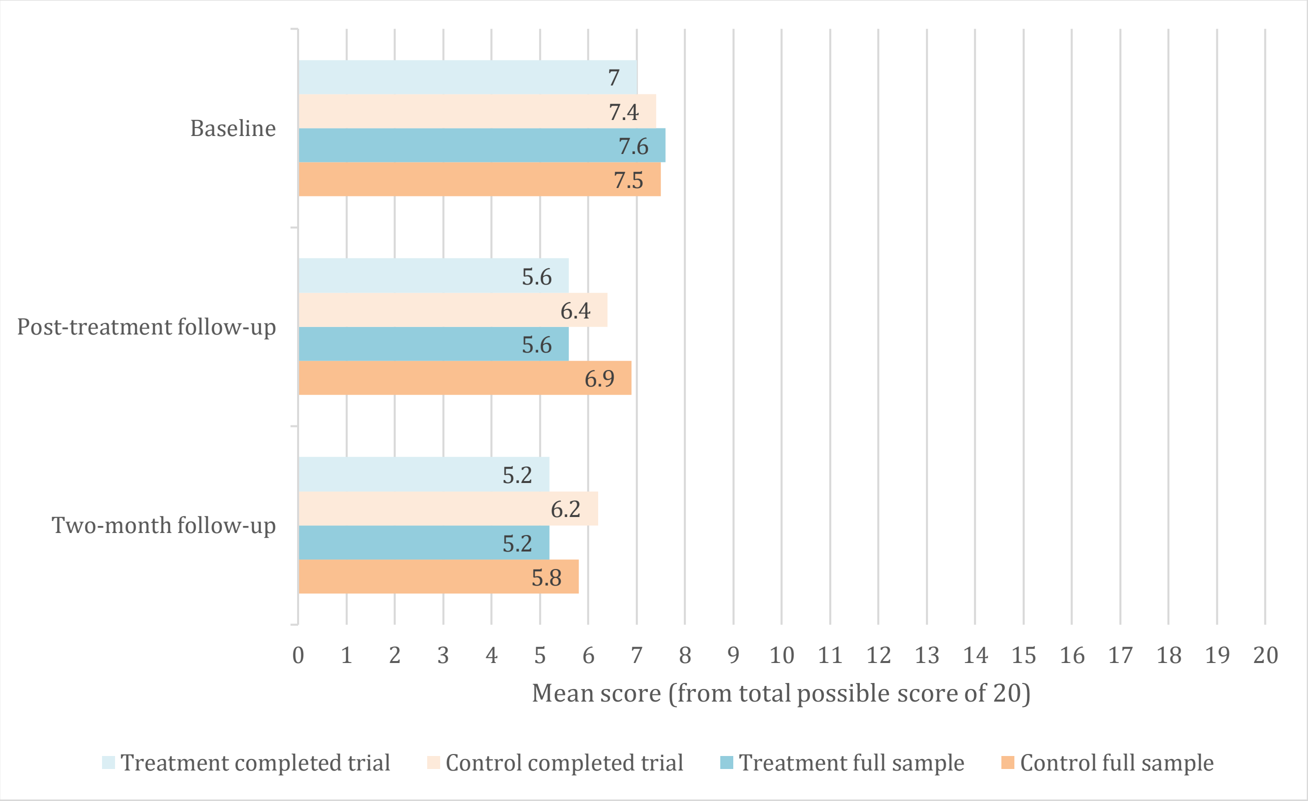


Figure 7 Changes in attitude towards good cyber practices at baseline, post-treatment follow-up and two-month follow-up in both treatment conditions.

Figure 7 depicts the mean knowledge scores at baseline, end of treatment and two-month follow-up. Note that a higher score on the knowledge scale represents a better score. Appendix C Response Rate shows the percentage of participants who provided the correct answer at baseline to each of the individual multiple-choice questions used to determine cyber security knowledge.

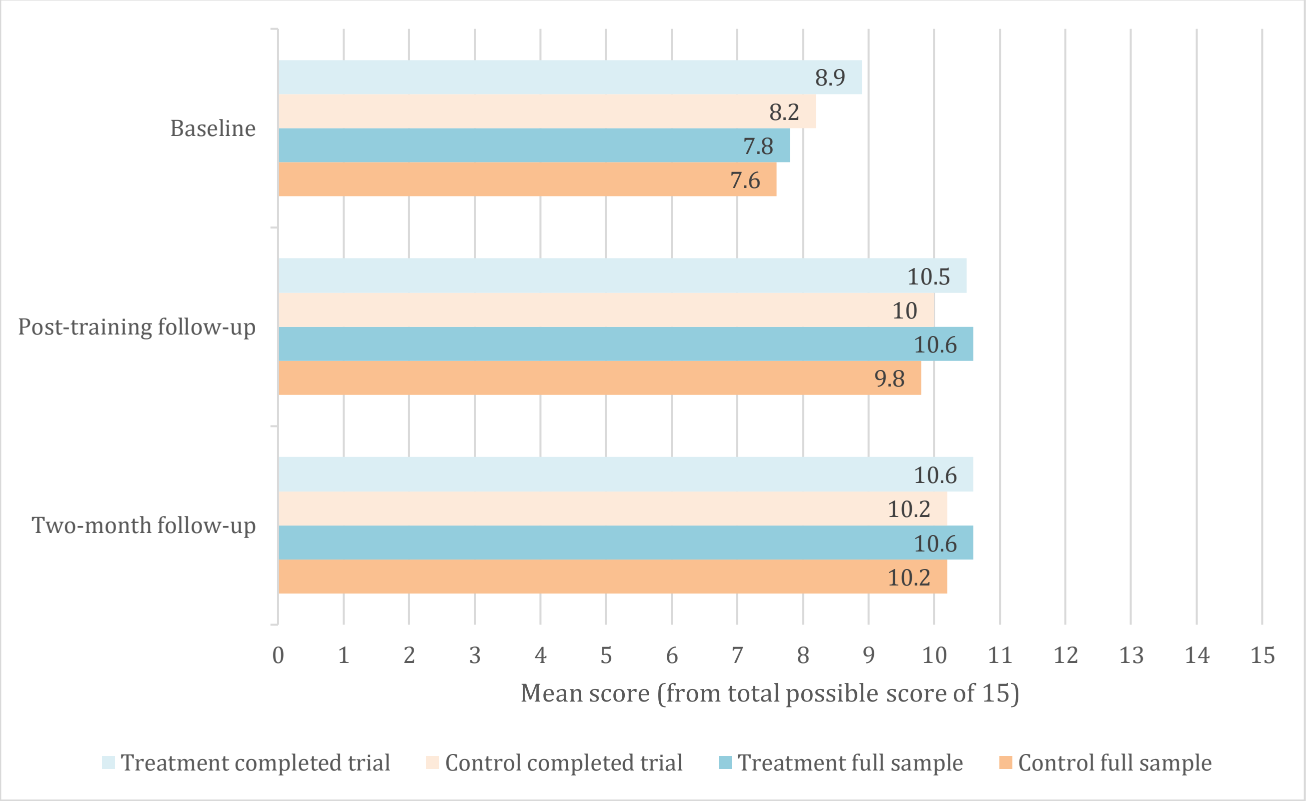


Figure 8 Changes in cyber security knowledge at baseline, post-treatment follow-up and two-month follow-up in both treatment conditions.

In Figure 8 it shoes the changes in cyber security knowledge at baseline, post-treatment follow-up and two-month follow-up in both treatment conditions. The descriptive analysis demonstrates that at baseline most participants rated cyber security as being important to their work and personal lives. Some other attitude question prompted a more mixed response: the perception of risk associated with the use of cloud-based storage of data for example differed across respondents, as did the perception of Cyber Essentials as being something that would impact on the organisation's ability to generate new business. Participants also varied in their confidence in how much they understood cyber security risks, and in how confident they felt they know where to get external support from. Responses to the knowledge questions on the baseline survey highlighted several areas where participants appeared to be lacking in knowledge on cyber security topics. These included issues around authentication, types of password attacks, the nature of cyber security policies, and the benefits of monitoring and auditing technologies.

4.2 Results Study 1a BEIS Aptitude Survey

The descriptive analysis demonstrates that at baseline most participants rated cyber security as being important to their work and personal lives. Other attitude questions prompted a more diverse response. For example, the results showed that the perception of risk associated with the use of cloud-based storage differed across respondents, as did the perception of Cyber Essentials as being something that would impact the organisation's ability to generate new business. There was also variation among participants' confidence in how much they understood cyber security risks, how much they understood cyber security risks, and in how confident they felt they know where to get external support from. Similarly, responses to the knowledge questions in the baseline survey highlighted several areas where participants appeared to be lacking in knowledge on cyber security topics. These included issues around authentication, types of password attacks, the nature of cyber security policies, and the benefits of monitoring and auditing technologies.

Analysis was conducted to determine statistically significant changes in the quantitative measures taken at baseline, end of trial follow-up and two-month follow-up. The data in the results section were collected only by those participants who completed the programme and responded to the surveys, not the change amongst the treatment and control group as a whole. The results demonstrated that participants in both the control and treatment conditions had improved attitudes towards the importance of cyber security; improved attitudes towards cyber security risk; and improved attitudes towards good cyber practices, at the end of the trial follow-up. In addition, there was a statistically significant improvement in knowledge scores in both groups between baseline and end-of-trial follow-up. However, it is important to note the sample size was smaller than anticipated due to COVID-19, and reliable inferential analysis could not be done. This was still done at the request of BEIS; however, the results are treated with caution.

The descriptive analysis demonstrates that at baseline most participants rated cyber security as being important to their work and personal lives. Participants also varied in their confidence in how much they understood cyber security risks, and in how confident they felt they know where to get external support from. Responses to the knowledge questions on the baseline survey highlighted several areas where participants appeared to be lacking in knowledge on cyber security topics. These included issues around authentication, types of password attacks, the nature of cyber security policies, and the benefits of monitoring and auditing technologies.

Chapter 5 Study 1b BEIS Interview Methodology and Results

As described in 3.1.1 the participant number was not reached, and as a result, the survey serves as baseline data to insight into the knowledge level of the participants.

The project team randomly selected 40 participants who were invited to interview. 20 of these participants were evenly selected from the treatment and control who had completed the training, and 20 were selected evenly from the treatment and control who had not completed all of the training. This was to ensure that data from those who dropped out were also accounted for. Unfortunately, of these 40 invited only 14 consented to be interviewed. All 14 of the selected participants were from the group who had completed the entirety of the research and were all from the intervention group. The participants were contacted via email and scheduled a time for an interview. These 14 interviews followed a transcribing process, where the audio recording was converted into transcripts.

The design of the interviews after the second aptitude and knowledge survey followed an open-ended style, which allowed room for flexibility. One of the benefits of this approach is that, if a participant gives a vague answer, the open style gives room to rephrase questions and further clarify what their answers mean. The interviews were designed in conjunction with Bournemouth, Christchurch and Poole Council (BCP) which meant some questions were not directly relevant to the overall project. The interactive nature of the interviews allows further probing into deeper topics of interest during the data gathering process (Beautement et al., 2016). Interviews were adopted as they are flexible, a useful method for data collection and effective for collecting participant experiences, beliefs, and behaviours towards a particular subject area (Ryan et al., 2009). Consideration was made to alternative and additional data collection tools, such as overt observations, however research demonstrates that this method can create a Hawthorne effect Wickström and Bendix (2000). This is where the researchers' presence influences the participants' behaviour due to their assumptions or apprehension, this has a way of manipulating data and in turn, creates a set of unreliable data (McCambridge et al., 2014). Similarly, we considered focus groups as a research strategy. It is defined as a planned series of discussions designed to gather perceptions on a particular subject area, in a non-bias or non-threatening environment (Larson et al., 2004). Although there are several benefits to using focus groups, they are less suitable for this study; mainly because of restrictive measures within commercial settings. After an evaluation of research techniques, it became evident that interviews are the most effective and appropriate for this research. The inclusion criteria for the research were Small and Medium-sized Enterprises (SMEs) Karmowska and Marciniak (2015), operating within Dorset, UK.

5.1 Data Analysis of Study 1b BEIS Interview

The data from these interviews were analysed using Braun and Clarke's (2006) six-phase approach, Thematic analysis. This method helps to ensure that codes are not retrofitted, but instead objectively inform the research outcomes. One of the reasons this method was chosen is because it can be widely used across a wide range of epistemologies and research questions (Nowell, 2017). It is a method for identifying, analysing, organising, describing, and reporting themes found within a data set (Braun and Clarke, 2006).

Since Cyber Well was being led by BEIS and they had their requests, the full measure of Braun and Clark's six-phase approach was not fully explored. This is later explored in Study 2 Training Selection (Chapter 6) where there was more flexibility.

One of the attributes of thematic analysis is that it ensures that information-rich qualitative data is not lost in analysis. Thematic analysis is flexible, it can be applied to content that is independent of theory and can be tested across a range of theoretical approaches. The thematic coding followed these six stages:

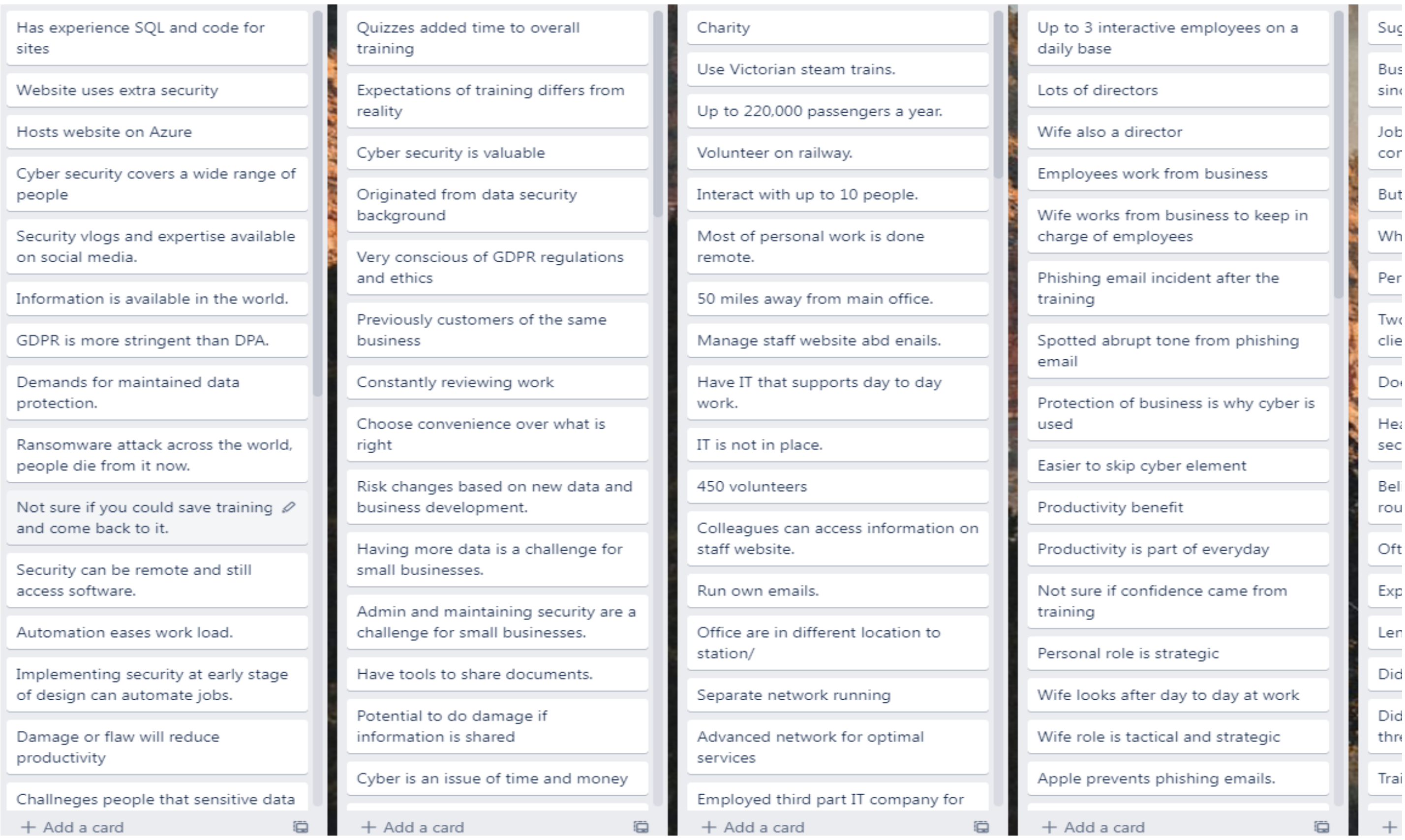
Stage 1: Familiarising with the raw data - this includes transcribing recorded data into a written transcript, reading through the text and taking initial notes and generally looking through the data to get familiar with it. The interviews were recorded using MS Teams. The participants were sent Participant Information Sheets (PIS) via email before the interview, detailing contents around how and where their data will be used and stored and the fact that they will be recorded.

Stage 2: Generating initial codes- In this phase, the collected data is coded. Coding involves methodically reviewing the data and searching for segments that appear interesting, relevant, provoking-in relation to the research question- and then writing brief descriptions (code) next to them. It is an exploratory process (Braun and Clark, 2021 p. 64).

…. This is where segments of data are identified as potentially interesting, relevant or meaningful to the research question and codes are assigned besides the meaningful parts of data. Coding isn't just about summarising and reducing content, it's also about capturing personal analytical perceptions of the data (Braun and Clark, 2021 p. 35). Once the entire dataset is systemically and thoroughly coded, the code labels are collated and then compile the relevant segments of data for each code.

Stage 3: Generating initial themes- In this phase, a shared pattered should be identified across the dataset. Clusters of codes that seem to share a core idea or concept are complied. These are seen as potentially providing a meaningful angle to answering the research question. Braun and Clark (2021, p. 35) discuss that theme development is an active process; themes are constructed by the researcher, based on the data, the research questions, and the researcher's knowledge and insights. The difference between a code and a theme is that codes typically capture a specific meaning, themes describe broader, shared meaning. Once potential themes capture the data and address the research questions, all the collated coded data is grouped to its relevant candidate theme.

One of the concerns the BEIS team members had was 'Confirmation Bias'. This connotes the seeking or interpreting of evidence in ways that are partial to expectations, or a hypothesis in hand (Nickerson, 1998). They were concerned there may be bias towards the analysed interview results, based on existing hypotheses or predispositions. To mitigate this, two peer reviewers from the BEIS team reviewed the initial codes and the consequential themes. The codes were then gathered and converted into digital cards, on a platform online called 'Trello' (Figure 9 Organising Codes in Trello).



- Has experience SQL and code for sites
- Website uses extra security
- Hosts website on Azure
- Cyber security covers a wide range of people
- Security vlogs and expertise available on social media.
- Information is available in the world.
- GDPR is more stringent than DPA.
- Demands for maintained data protection.
- Ransomware attack across the world, people die from it now.
- Not sure if you could save training and come back to it.
- Security can be remote and still access software.
- Automation eases work load.
- Implementing security at early stage of design can automate jobs.
- Damage or flaw will reduce productivity
- Challneges people that sensitive data

- Quizzes added time to overall training
- Expectations of training differs from reality
- Cyber security is valuable
- Originated from data security background
- Very conscious of GDPR regulations and ethics
- Previously customers of the same business
- Constantly reviewing work
- Choose convenience over what is right
- Risk changes based on new data and business development.
- Having more data is a challenge for small businesses.
- Admin and maintaining security are a challenge for small businesses.
- Have tools to share documents.
- Potential to do damage if information is shared
- Cyber is an issue of time and money

- Charity
- Use Victorian steam trains.
- Up to 220,000 passengers a year.
- Volunteer on railway.
- Interact with up to 10 people.
- Most of personal work is done remote.
- 50 miles away from main office.
- Manage staff website abd enails.
- Have IT that supports day to day work.
- IT is not in place.
- 450 volunteers
- Colleagues can access information on staff website.
- Run own emails.
- Office are in different location to station/
- Separate network running
- Advanced network for optimal services
- Employed third part IT company for

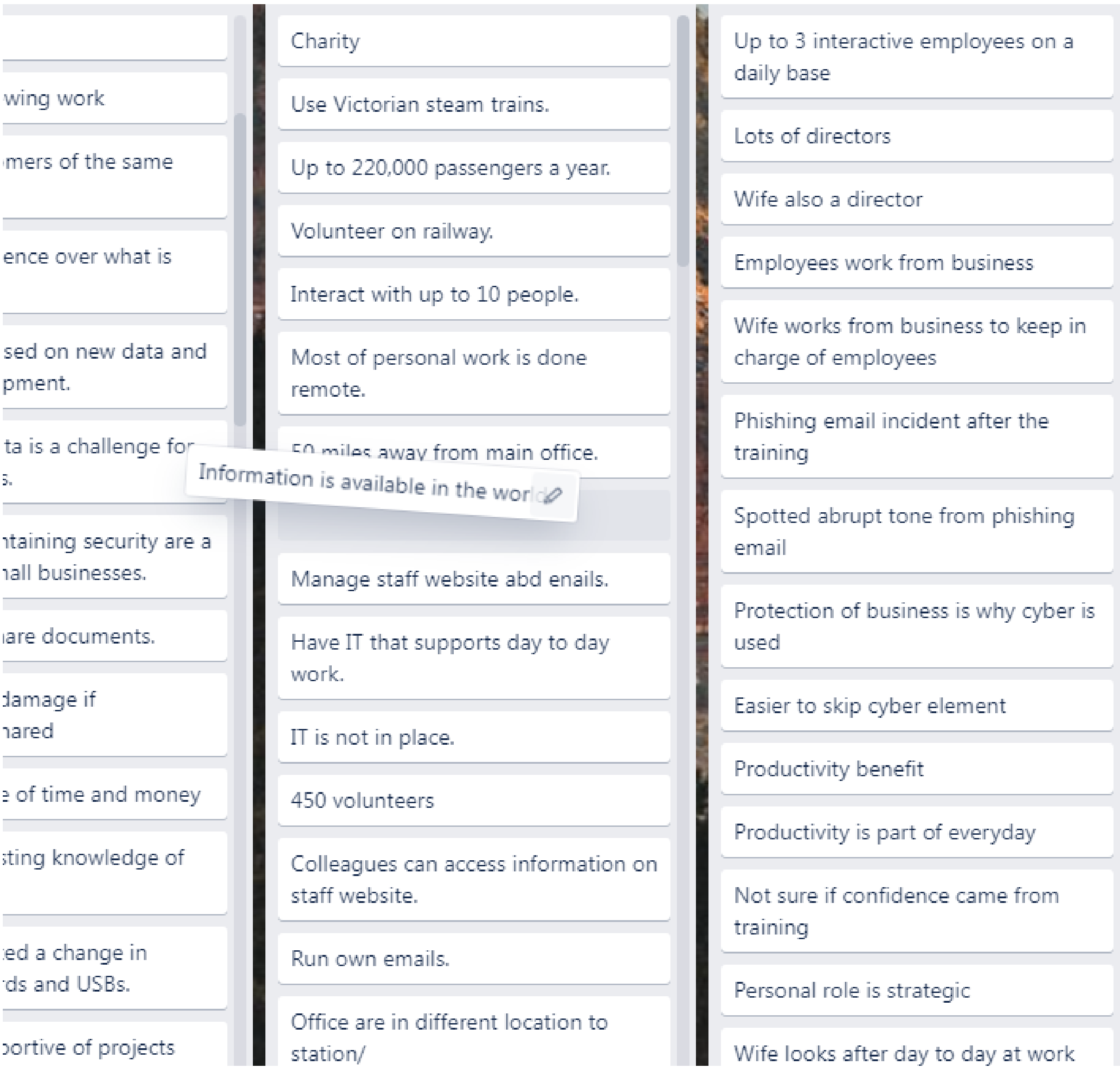
- Up to 3 interactive employees on a daily base
- Lots of directors
- Wife also a director
- Employees work from business
- Wife works from business to keep in charge of employees
- Phishing email incident after the training
- Spotted abrupt tone from phishing email
- Protection of business is why cyber is used
- Easier to skip cyber element
- Productivity benefit
- Productivity is part of everyday
- Not sure if confidence came from training
- Personal role is strategic
- Wife looks after day to day at work
- Wife role is tactical and strategic
- Apple prevents phishing emails.

- Sug
- Bus sin
- Job cor
- But
- Wh
- Per
- Two clie
- Do
- Hea sec
- Bel rou
- Oft
- Exp
- Len
- Did
- Did thre
- Trai

Figure 9 Organising Codes in Trello

Stage 4: Reviewing themes- This phase required two levels of reviewing and refining themes. This is where the themes are assessed against the codes extracted, and then the full dataset. Braun and Clark (2021, pp. 35-36) suggest that in this phase, certain candidate themes can be merged; one or more may be split into new themes; candidate themes may be retained; some may be discarded.

One of the ways this was achieved was by discussing the themes with the peer reviewers via Teams. Any disparities or differences in opinion were discussed and resolved by moving the code cards, to reflect discussed points (Figure 10).



wing work

mers of the same

ence over what is

sed on new data and
pment.

ta is a challenge for
s.

ntaining security are a
nall businesses.

are documents.

damage if
hared

e of time and money

sting knowledge of

ed a change in
rds and USBs.

portive of projects

Information is available in the worl

Charity

Use Victorian steam trains.

Up to 220,000 passengers a year.

Volunteer on railway.

Interact with up to 10 people.

Most of personal work is done remote.

50 miles away from main office.

Manage staff website abd enails.

Have IT that supports day to day work.

IT is not in place.

450 volunteers

Colleagues can access information on staff website.

Run own emails.

Office are in different location to station/

Up to 3 interactive employees on a daily base

Lots of directors

Wife also a director

Employees work from business

Wife works from business to keep in charge of employees

Phishing email incident after the training

Spotted abrupt tone from phishing email

Protection of business is why cyber is used

Easier to skip cyber element

Productivity benefit

Productivity is part of everyday

Not sure if confidence came from training

Personal role is strategic

Wife looks after day to day at work

Figure 10 Moving Codes in Trello

The themes from the interviews were finalised in a team meeting. This meeting enabled the creation of a visual relationship between the key themes and the sub-themes identified by the analysts (Figure 10). The theme map infers conclusions from the interviews and creates an identifier for the key themes from the interviews. The blue boxes represent the themes, the green boxes represent the sub-themes and the yellow box represents the sub-sub themes. The dotted orange lines depict the relationships between the theme that were identified as being important by the researchers. As is often the case in qualitative research there were potentially a greater number of sub-themes and connections which could have been identified however to ensure that the results of the analysis remained actionable and meaningful the research focussed on the elements that are most relevant to the project aims.

Some of the dispositions considered in this phase included questions like:

- Do the themes make sense?
- Does the data set to support the themes?
- If themes overlap, are they separate themes?

Stage 5: Defining and naming themes- this phase is where fine-tuning happens. The analyser asks themselves questions like ‘What story does the theme tell?’. This is also where one assesses, any relationship between the theme. Subsequently, a punchy and informative name is given for each theme.

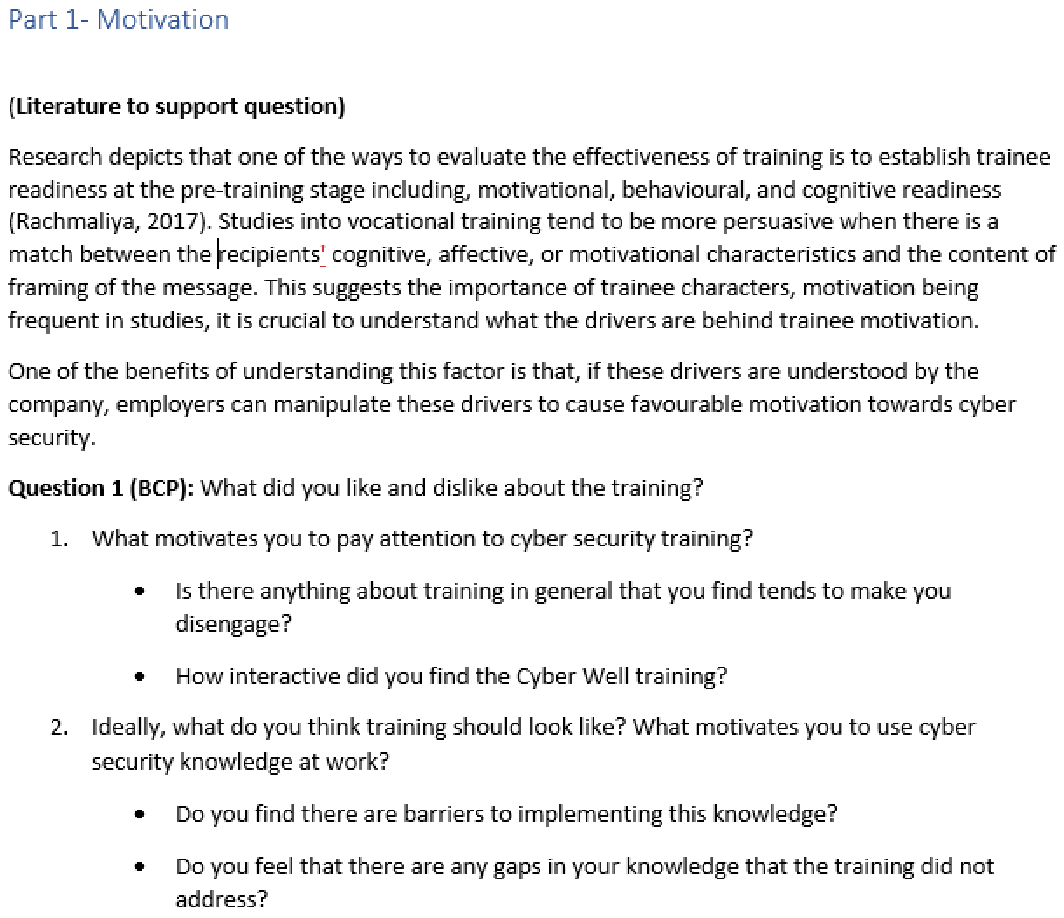
Stage 6: Writing up This is the final phase of the thematic analysis process. Ultimately, the aim is to weave together an analytic narrative, to tell the reader a convincing story about the dataset that addresses the research questions. The final writing for the BEIS report required producing the introduction, methodology and conclusions of the dataset.

5.2 BEIS Study 1a Interview Results

5.3 Introduction

In this Chapter, the results from Study 1b BEIS Interviews are presented. Study 1b consisted of 14 online interviews with SME business owners who are also awareness professionals in their business. To recap, study 1b BEIS interview does not have specific research questions as this was part of a larger project but instead aims and objectives to discover key areas like attention, motivation and social environment.

The interview questions for this study centred; source of employee motivation, influence from managers and peers and whether this affects perception towards security, there were questions about the influence of their social environment and also questions relating to human limitations like memory and attention while under pressure *(Figure 11).*



Part 1- Motivation

(Literature to support question)

Research depicts that one of the ways to evaluate the effectiveness of training is to establish trainee readiness at the pre-training stage including, motivational, behavioural, and cognitive readiness (Rachmaliya, 2017). Studies into vocational training tend to be more persuasive when there is a match between the recipients' cognitive, affective, or motivational characteristics and the content of framing of the message. This suggests the importance of trainee characters, motivation being frequent in studies, it is crucial to understand what the drivers are behind trainee motivation.

One of the benefits of understanding this factor is that, if these drivers are understood by the company, employers can manipulate these drivers to cause favourable motivation towards cyber security.

Question 1 (BCP): What did you like and dislike about the training?

1. What motivates you to pay attention to cyber security training?
    - Is there anything about training in general that you find tends to make you disengage?
    - How interactive did you find the Cyber Well training?
2. Ideally, what do you think training should look like? What motivates you to use cyber security knowledge at work?
    - Do you find there are barriers to implementing this knowledge?
    - Do you feel that there are any gaps in your knowledge that the training did not address?

Figure 11 Sample of Study 1b BEIS Interview Questions

Subsequent to the methodology, the corresponding ‘Cyber Well’ theme map is illustrated in Figure 12. Using a visual mapping technique is very useful, both as a general analytic practice and in three specific ways: (1) to start thinking about provisional themes in their own right; (2) for exploring how provisional themes might relate to each other; and (3) for starting to consider the overall story of the analysis (Braun and Clark, 2021 p. 86-87). The initial stage of mapping is tentative, it helps to figure out patterns of meaning and possible connections, interconnections, and disconnections (Braun and Clark, 2021 p. 86-87). Braun and Clark, 2021 suggest keeping research questions in mind when developing themes, however they caveat this by saying it does not mean looking for a direct answer to that question. Instead, it means to generally keep in mind what interests are in the topics and exploring patterns that might illuminate understanding of the issue. In so doing, a theme map was developed following Braun and Clark (2021) recommendation and the final version is presented in Figure 12.

The themes identified from Study 1b BEIS Interviews are listed from [5.3.1 to 5.3.9]. In this Chapter, there are subthemes derived from subsequent themes, and these are presented in the *italic text title*.

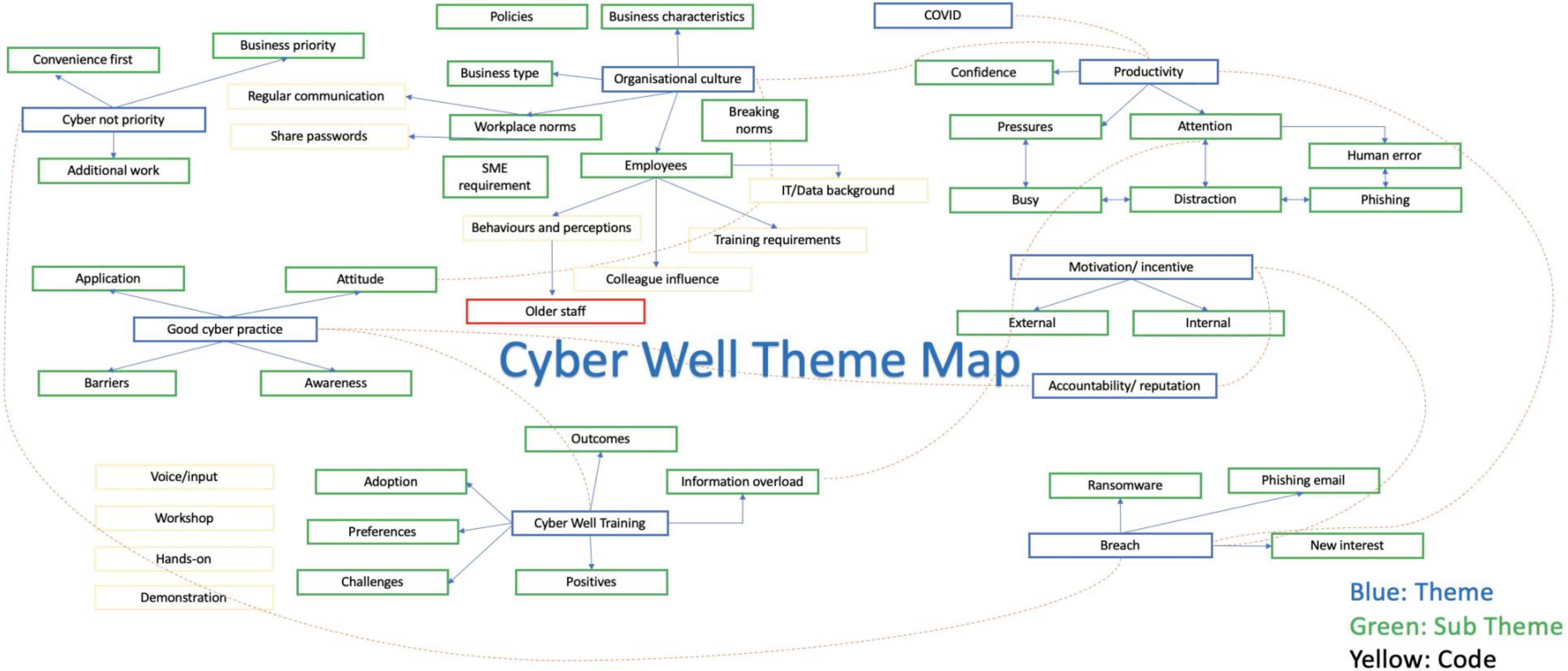


Figure 12 Theme map for Cyber Well

5.3.1 COVID-19 theme

The first prevalent theme that appeared across over half of the interviews was ‘COVID-19’. This theme was discussed in 57% of the interviews, and over half of the participants referenced COVID 19 in their interview responses. One of the responses demonstrated the effects COVID-19 had on their business, for example, “*We went into a bit of a slow period as everybody did. Obviously, the initial response was lock down, can't come in”* [P11].

Some of the responses indicated that COVID-19 was a driver of the change in their business infrastructure and dynamics. For example, 4 out of 12 deferred to working from home as a result of the global pandemic. In addition, COVID-19 served as a business hindrance for some participants, as some business plans and development were terminated. For example, *“What we're doing is we're actually building a recording studio, commercial music studio. And it's, been affected by COVID. So, it's not built yet”* [P3]. One participant described the domino effect on their business, specifically in their air traffic control industry, for example they said *“One of our key customers is a supplier to the air traffic control. industry. So, air traffic control pretty much died. So that is kind of affected a little bit. Yeah, it has been a lot quieter than usual”* [P1].

It is important to highlight the relationship between the COVID and productivity theme as they are closely linked together. The impact of COVID restricted regular service and business and in turn caused staff to be unproductive because of furlough. As a result of the national lockdown, a couple of participants described how their individual work dynamics changed, by staying at home. For instance, *“I’m a volunteer so I work from home. Yes, we have we have some offices and obviously during COVID, the lockdown, a large proportion of our staff were on furlough, because we were not able to work*” [P14].

On the other hand, the analysed data revealed that 33% of the participants changed their modus operandi as a result of COVID. For example, one participant described that most employees worked from home and conducted all business meetings online, while other employees were on furlough *“We all work from home now and just doing meetings online as a team”* [P5].

The results thus far indicate that a lack of work demand directly affected participants' productivity in the workplace. The results gradually suggested that COVID was the reason for some unproductivity in the workplace. For example, *“I’m on furlough and go back in November, so I have not been productive”* [P12].

In hindsight, 36% of the participants revealed that COVID did not have adverse effects on their business, as they worked from home before COVID. Similarly, one participant described that COVID created avenues and opportunities to plan and organise business plans and growth. For example, *"It has in the sense that it has been an enabler for us, we've got some funding now. On a whole, we are not as affected as other businesses"* [P2]. Similarly, *"I think for us COVID was good because we got to plan our projects"* [P2].

The global pandemic is an ongoing prominent factor affecting businesses. Buil-Gil et al., (2021) recently discussed the effects of COVID 19 on people's everyday activities. They hypothesise that perhaps the natural experiment produced by lockdown measures, the closure of businesses and education centres and the move towards home working is what has affected the most significant number of people. This could explain why 57% of businesses referenced COVID 19 in the interview and why their modus operandi changed.

5.3.2 Productivity theme

In analysing the interview data, a key theme that was developed in analysis is productivity. Several codes compose productivity as a theme, though it can be treated as single entities, some conflate and link. These are confidence, work pressures, busyness, attention, distraction, human error and phishing.

For example, some businesses identified that daily work pressures, for example, completing a task caused them to unintentionally pacify cyber security from their minds to fulfil tasks. For example, *"if you're really busy, and you're like, trying to trawl through your emails as quickly as possible, you could quite easily click on something without realising. And then before you know, it's too late"* [P7].

Similarly, 3/14 of participants claim this to be a natural response of being under pressure. For example, *"Generally that's natural. Anybody works under pressure there is always that risk"* [P1]

As previously mentioned, attention was a code derived from the dataset, and it is highlighted here. As 8/14 participants, explicitly say their attention reduces while under pressure from work. For example, *"Natural for attention to decrease under pressure"* [P13].

More severely, some participants discussed the fact that they missed integral clues that would reduce the risk of cyber threats, as a result of being busy. For example, *"Busy* *causes distraction and we miss things"* [P4]. Some of these risks are experienced as phishing emails, as a result of low attention to cyber security and in turn a heightened risk of human error. For example, one participant described their experience when they sent an email intended for internal communications, to an external organisation. For example, they said "*When I've been under pressure in my working life, I've put the wrong name in an email and is gone to the wrong organisation, or the wrong person but it's alright it's internal, probably, when it's going external, that's pretty bad. Do I think pressure affects me in that way? I rush too much. And there is a risk I'll send information to people who shouldn't have it. In terms of the rest of it, I suppose being under pressure, does stop me backing up as much as I should"* [P4].

Some participants identified that the investment and implementation of cyber security have increased their business productivity. For example, through the implementation of Two-factor Authentication (2FA), businesses have intrinsically incorporated cyber into daily practices and feel more productive. For example, *"You are much more productive once you've got the security behind you"* [P3].

On the other hand, some participants found that a lapse in cyber security can hinder productivity in their work tasks. For example, if there is an extra layer of security to access data or complete a task it contributes to the time that could be used for the actual task. One participant said *"If the job needs working out, that's your main priority to actually go out and deliver it. So, the security side is obviously important, but it becomes, always balancing those priorities. What do I need to do today?"* [P9].

This evidence shows that attention, pressure and distractions are significant factors that inhibit true focus on cyber security. This has ripple effects on businesses because it makes them subject to cyber breaches as they are more prone to it.

5.3.3 Breach theme

In analysing the interview data, a key theme that was developed during analysis is the 'event of a breach'. Every participant refuted the idea of experiencing a breach, however out of the 14 participants, 2 experienced a breach. Both participants describe the consequential effects of a breach through time frame and loss of value, for example, *"It caused us problems for a week"* [P14]. *"Productivity Very pertinent issue and it does come at a price, both in time and money*" [P2].

There is a link between experiencing a breach and productivity which is illustrated by their response. Their response indicates the obliteration a breach caused their business, one participant is still coping with the remnants of the breach. The common factor between these 3 participants is the interest developed thereafter the training and the urgency to intellectually equip the business and ensure safety measures are implemented. For example, *“We've done some training over the last few years, our internal staff because we've had a number of phishing attacks of various types.”* [P14]

In addition to this, the participants claimed their productivity at work is reduced if they experience a breach. One participant described their time-consuming process of checking previous emails to retrieve useful data files as a result of a breach that occurred a year prior. For example, “*So we've lost all our files. So, if we've got an order that we want to send using a file from a year ago, we don't have that file, so we now have to go through all of our emails, search to the original email. And if we can't, we have to, basically, we have to do the work again”* [P7]. The same participant described that their level of productivity is affected by reduced data availability. For example, *“There is reduced productivity if there is data loss”* [P7].

A key theme from the interviews is ‘breach’. There was a common trend, between those who encountered a breach and their level of productivity. These themes inter-link, while a breach such as ransomware inhibits the businesses’ productivity. The analysis depicts that victims of a breach, discovered interest in cyber security after an event of a breach, for example an investment towards cyber security. Pursuant to this, victims of a breach become motivated to use cyber security, as demonstrated in the next theme.

5.3.4 Organisational Culture theme

This theme appeared in every interview which suggested the integral nature and effect organisational culture has on businesses. The theme reflected that there was an element of organisational culture which invokes behaviour supporting cyber security or contrary behaviour. The very nature of organisational culture drives employee productivity towards or afar cyber security. For example, every participant (except lone businesses) stated they would follow cyber security if their colleagues did. For example, *“If your colleagues have a good attitude towards it and take it seriously then you have license to also take it seriously”* [P9]. To buttress this, these participants identified that they did not want to be left behind by their peers or be an instigator of cyber risk to their business. For example, *“Well, you have that herd mentality which affects you a bit, if nobody is doing it the pressure to perform in that manner is less”* [P6].

Furthermore, the analysis illustrated that employees religiously followed cyber security because of the hierarchy and influence managers and supervisors inherently have. For example, one participant said *"I think the environment is important, it comes from the top. When it comes from the top it's harder to say no. If your colleagues have a good attitude towards it and take it seriously then you have license to also take it seriously"* [P2]. The same participant also discussed how the influence of managers cascade down to what others do within the organisation. For example, *"What your colleagues do is entirely driven from what's demanded the top"* [P2].

On the contrary, one manager expressed difficulty to explain cyber security to older staff which resulted in a constant query about procedure changes and the entire implementation of cyber security. For example, *"I'm trying to get him to realise that there's certain things that need to be done slightly different. And they sort of say why. So perhaps they could do the training"* [P13].

One of the sub-themes that emerged from the interviews is workplace norms. They felt it was crucial to build an environment conducive and permissible to encourage confidence and trust. For example, *"we make our environment fun and somewhere we can learn and grow"* [P2].

In light of this, three businesses identified that it would be difficult to evolve a new employee's mentality or mindset. They described this as disparities in interest between employees and senior staff. For example, *"People are not invested as the CEO"* [P8]. One of the comments that emerged from the data highlights the little influence an individual has to change a mass of people in an established environment. For example, *"Difficult to maintain culture when new staff come in"* [P12].

This suggests the difficulty trainers could experience when educating participants. They also mentioned the fact that an individual trying to change people's norms, could create discomfort in the workplace. For example, *"I don't think I've seen an environment where someone single handily comes into a room with 15 other people change the atmosphere. That is what undermines everybody's comfort"* [P2].

On the other hand, some of the codes from the interviews suggested some businesses felt they thrived in an environment where errors and mistakes are welcomed to educate each other and avoid future threats or mishaps. For example, *"I trust my colleague to pick me up on any mistake I make, and I want to learn from them so I'm not the person that brings threats in"* [P2].

One of the participants who worked as a manager discussed his technique to encourage and engage in cyber practices. For example, *“I send reminders out to my team to be mindful of phishing emails”* [P13]. This indicates that the environment is very important for learning and growth.

Pursuant to being able to make errors, some businesses have a background in IT, and have internalised GDPR in their mindset and day-to-day activities. Some of which has given aid for support to make errors and learn in the workplace. For example, *“We come from a background where we manage data, so we are conscience about GDPR regulations and it’s about ethics. “Are we doing it in a way it is secure for others?”* [P2].

In addition, the analysed data suggests that some businesses have background knowledge in IT, most of which compose a foundation for cyber security. For example, “ *“I think as a result of the developers background, knowledge and experience and our kind of local authority, grounding, we get it. The level the culture around security and ethics”* [P3].

These businesses simultaneously adopt cyber security on a day-to-day basis, they have internalised cyber security and therefore do not need additional thought. For example, *“Obviously, we're all pretty much trained”* [P5].

Amongst organisational culture, 10/12 participants have expressed that they are equally responsible for cyber security in addition to their job description. For example, *"I take care of cyber stuff and security as well as my normal day to day job”* [P9]. Similarly, one participant said *“Cyber security is part of my job”* [P10]. This could suggest that businesses do not prioritise cyber security enough to outsource this.

Some indicate their manual effort to remind staff about the use of cyber security in the workplace and reinforce knowledge of the risks they could potentially be susceptible to. For example, *“we regularly remind people not to open up things that look a little bit suspicious”* [P11].

5.3.5 Motivation/Incentive theme

This theme relates to the factors that cause participants to either use cyber security or dismiss its relevance. There were a series of factors that motivated the participants in this study, for clear understanding of categories of motivation was deduced.

5.3.5.1 External motivation

This can be identified as motivations or incentives to use cyber. Some motivations were classified as external, for example being subject to legislation under GDPR. For example, one participant explicitly said, "we are subject to legislation so we need to protect data we take and I don't want to go to jail" [P2].

In addition, some participants discussed the relationship between their community, and how they wouldn't want to jeopardise their reputation. For example, they said "we deal with quite a few local authorities, and some government agencies, and obviously, what you don't want to do is end up causing an issue for them" [P1]. One participant also described the importance of maintaining a healthy relationship with their clients, by ensuring they do not exhibit any cyber risk to their business. For example, "We take, the way we work with our clients quite seriously, because it's usually quite a personal relationship. So if we mess up on any area, then, you know, it's a personal sort of issue [P14].

5.3.5.2 Internal motivation

As described above, some motivations are classified as internal. For example, these are participants who described some internal reward or benefit for adhering to cyber security. One participant was motivated to follow cyber security practices because their company data was also being handled by themselves. For example, "Motivated because your data is there too" [P5].

Another participant described the fact that adherence is important to their business, as it is beneficial to them. For example, "it's important for our company to get things right from this point onwards, for the benefit of the company" [P2]. In addition to this, one participant discussed the level of care and concern they apply to their client, due to personal relations and in turn reputation. For example, "we take, the way we work with our clients quite seriously, because it's usually quite a personal relationship. So if we mess up on any area, then, you know, it's a personal sort of issue" [P7].

Similar to this, one participant discussed that their motivation for cyber security is in inherent, because their motivation comes from their job responsibility. For example, "I am motivated because cyber is my job responsibility" [P9]. Another participant spoke about the fact some of their responsibilities are cyber-related, and not part of their job role. For instance, *“there's a number of people who've got a responsibility outside of their job role. So cybersecurity is something that I pick up, around our compliance, data protection and all that stuff as well, so it seems logical if I pick that up” [P11].*

5.3.5.3 Motivation from breach

The results highlighted the fact that participants who experienced a breach in the past, dealt with cyber security was a matter of urgency. For example, one participant who fell victim of a breach said, “Motivation comes from the fact that cyber risk is an issue for businesses” [P9]. Another participant who previously fell victim of a breach described how they negate cyber related issues for the benefit of their clientele. For example, “I don't want to get caught out by any viruses, or any kind of issues like that, obviously from a business perspective, personally, and obviously, for our clients, I don't want to end up having a problem that we've caused to them equally” [P5].

One of the key notions is that businesses, reject the idea of falling victim to cyber crime because they recognise the internal and external damage it will do to their business. For example, one participant described overlapping motivations, one originating from a personal perspective and the other from an organisational perspective. For instance they said, “So I have two motivations, the personal and also the organizational” [P3].

5.3.5.4 Motivation from topic interest

While some participants were internally motivated, others were externally motivated and others' motivation arose as a result of a breach, some participants draw motivation from ascertaining a genuine interest in the subject. When asked where motivation comes from, one said “Motivation comes from having a genuine interest in the topic” [P3]. Another participant said, “Motivation comes from seeing value in it” [P4].

Similar to this, when participants were asked follow-up questions, as to why they thought other participants did not show likened interest in the topic area, they said “There's got to be some reason, which is positive for you to take away from It” [P9]. One participant described that a level of excitement must exist before they do additional learning outside of their work scope. For example, they said, “If I am excited about the training, I would find time out myself to learn and do the training” [P1].

The overall results about motivation suggest that internal motivation served as a stronger driver for users to pay attention to cyber security and in turn apply it, rather than external motivation, even if that means an extra step to complete a task. Participants discussed internal motivation factors as drivers, more than they did external motivation.

5.3.6 Accountability/Reputation

This theme is closely related to motivation/incentive. If participants are motivated to use cyber security, they will take accountability for actions because their reputation is at stake, which is also an incentive in itself. For example, one participant discussed the relationship between the importance of being GDPR compliant and client privacy. They said, "*Customers want to see you are GDPR compliant and that their data is safe"* [P4].

The participants identify that customers want a trusted reputable service provider and realise that their business will suffer if customers are not happy. This could suggest that reputation is an integral factor and motivator for businesses to comply to cyber security. For example, one participant said, *"If customers are not happy, you lose business"* [P9].

5.3.7 Good cyber practice

To recap, the interviews were part of the Cyber Well BEIS project, and some responses illustrate different behaviours exhibited after the training. This theme is interlinked with the aforementioned themes. For instance, good cyber practice from the interview data was impacted by COVID restrictions and ripple effects caused to businesses. Similarly, good cyber practice is either fuelled by positive organisational culture or poor organisational culture.

This theme 'Good cyber practice' composes various codes, such as 'barriers' and 'awareness towards cyber security. This theme contrasts with existing cyber practices, which participants showed before and after the Cyber well training. The interview data suggest that some businesses did not have a password on devices used for customer data, and after the training, they realised their cyber errors. For example, *"Now I have a password on your laptop, for example. But I did not before, which is ridiculous"* [P4].

Some participants openly discussed poor cyber security practices they engaged in before the Cyber Well training. For example, one business owner mentioned the fact they had no password on their laptop since it was for work use. They said, *“I did not have a password on my laptop, since I use it at home for work”* [P1]. As well as this being a depiction of poor cyber behaviour, it also depicts an attitude that this particular participant has towards cyber security.

In some cases, business devices were given to members of family during the national lockdown, so they could do their work. For example, *“I have borrowed my son my work laptop so he could do his work”* [P8].

Another participant discussed the enticement to put a USB stick straight into a device when in need of a file to complete a task. After the Cyber Well interview, it became apparent to the participant that they can implement strategies to mitigate the risk of using a malicious USB stick. For example, they said, *“If you have a USB and there’s a file that you need, the temptation is to just stick in your laptop and utilise it. Part of the benefit of this to us is that we can have policies in place to protect our customers from the power of convenience”* [P2].

In light of this, there were changes implemented to ensure data is secure. For example, after the training, some businesses implemented two-factor authentication (2FA) as an extra layer of security. For example, *“We now use 2FA for everything, so we’re more secure”* [P10].

After the training, most of the participants identified they have a policy gap, which was a prerequisite of the training. However, the interview data suggests that businesses have not implemented this, some have accredited this to time limitations. For example, *“We know we have a policy gap, but we just don’t have the time for that yet”.* Similar to this, another participant mentioned the challenges they encounter with developing and establishing a security policy, coupled with time constraints. For example, *“One of the challenges is bringing together your security policy and process of reviews, and as a small company you’re doing other things and you have to do that. And it’s so time consuming”* [P2]. The data synthesise that good cyber practice is enhanced if the business considers the intrinsic and extrinsic motivations.

5.3.8 BEIS Cyber Well training

A key theme identified from the interviews is the factors that compose the cyber well training. The interview was centred around the experience and knowledge ascertained after the training, so participants were asked evaluative questions about how much benefit the training provided and what they learnt. From these questions, participants discussed exactly what could have been done differently about the Cyber Well training that could add value to their learning, for example, the training content and design. One participant discussed that examples that were used in scenarios for the training, didn't necessarily reflect what their business environment looked like. For example, *"the scenarios ought to have reflected personal business environment"* [P12].

5.3.8.1 Training expectations

In the same vein, some participants described what they expect to see from the cyber training material. For example, some participants specifically spoke about accessing training material at their convenience and audio flexibility in terms of being able to listen on the go. For example, one participant said "I wonder if they could deliver some of the training in an audio state, so if I'm walking to work, I can listen. So, all that time I'm sat listening to, can be listened to while I'm going to work. Maybe like how a CD works, one is 3 minutes, the other is 5 minute" [P1]. Similar to this, another participant said "training should be audio recordings, for ease of use and convenience" [P9]. Likewise, another participant said, "Training should incorporate voice and speech input to answer questions" [P13].

When participants were asked what factors aid learning cyber training, some discussed preferred methods of learning. For example, one participant said, "I learn better when its hands-on and I can see it" [P8]. It is important to highlight that when discussing preferred methods of learning, participants with learning difficulties also had specific niches they expect from training. For example, 2/14 of participants stated that they were diagnosed with dyslexia and so training that encompassed a lot of verbatim elongated learning, instead of aided learning. For example, "I'm dyslexic, so quite visual, and well presented like I'm not very good at reading stuff off the screen or off paper, it has to be interactive. So, discussions or videos and kind of small group discussions, stuff like that is good for me" [P12].

Training limitations

Participants discussed learning factors that contribute to the success of their learning. For example, one participant described that if training becomes too time-consuming then there is a likelihood for people to be discouraged and pay less attention to training. They said "It's like any learning tool, you need it, straightforward and, easy to adopt in terms of what you're *doing. I think, if it becomes too complicated on the cybersecurity side, then people just start switching off and thinking oh it's going to take too much time to implement and it's just not practical." [P10].*

In the same vein, some participants found that the training expectation did not match the reality. For example, 42% of the participants suggested the training was repetitive. For example, "I think the videos and questions to cement the knowledge is a good format, perhaps less repetitive and easier to look back to. It seemed like I couldn't keep the details to have, as a kind of guide to remind me" [P13]. Another participant described that the training exceeded the time they anticipated time, and they gave onus to the fact that they had to process the information. For example, they said "Every time I started watching something and it said it would take an hour, it took longer especially because of processing the information. The whole thing twice as long than I thought" [P2].

Similarly, 2 out of 14 participants suggested the training created an ostrich effect. The 'Ostrich Effect' is a cognitive bias that describes how people often avoid negative information, influencing feedback that could aid and monitor their goal progress. Like ostriches, people will bury their heads in the sand instead of dealing with the situation. This avoidance can often worsen situations (Kahn, 2015). This participant described how much the training scared them and how it created an ostrich effect. They said, "The biggest thing it did to me was scare…It reminded me of all the treats out there. And it probably turns me into an ostrich in that, what can I do about it" [P4].

Training positives

There was a positive response from every participant, suggesting they benefitted from participating in the training. Results show that 85% of the participants would recommend the training to another business. Before the Cyber well training, many were oblivious to cyber risks, for example, shoulder surfing and unintentional insider threat, and they were ignorant to how these risks can occur in a workplace and have effects within the business itself. For example, they said "I didn't even realise stuff like shoulder surfing would even have been sort of a problem in the workplace. You don't expect things like that to happen behind your back. Yeah. So it was good in the sense that it explained a lot of things that I'd never even heard of before" [P7].

As a result of the training, there was a heightened awareness of these risks and further precautions taken thereafter. In addition, the training yielded awareness from the participants with 13 out of 14 stating they are more aware of cyber risks as a result of the training. For example, the same participant who experienced a breach and did not have initial motivation said "We're a bit more aware of what's at stake. So, I think that kind of motivates us more on a day-to-day basis now, because we're more aware of it anything dodgy that comes in or anything that could happen" [P7].

Another participant who was a sole trader discussed hand in hand how the training boosted her confidence and raised her awareness levels to be cognizant of cyber risks. For example, they said, "it did improve my confidence, and made me feel that I did kind of know what threats I was looking for so that was reassuring" [P13].

5.3.9 Cyber is not a priority

This is a key theme that was developed in thematic analysis. It demonstrates that businesses focused their attention and harnessed time into personal business goals i.e. making money. In this section of results, the participants shared some limitations they experience as a small business. For example, one participant discussed the fact that they had other business priorities, so therefore cyber security was not on their radar. They said *"It wasn't really on the radar of being honest"* [P12].

In addition to this, participants spoke about the culmination of work burdens and cyber security and how these coupled together can be burdensome for small businesses. For instance, they said, *"I think the burden of admin and increase in process in order to maintain security is something for a small team or a start-up is burdensome"* [P12].

Participants further went to talk about problems they experience in general as a small business they mention how these problems affect the way they learn and interact with training material. For example, one participant spoke about being a small business and having ample things to do, in a short time frame. They also spoke about the difference between finding information available between cyber security and other sectors, for instance, there is minimal guidance as to where to get additional materials from. They *said "As a small company you're doing other things and you have to do that. And its so time consuming and there isn't really anywhere to get this guidance, but with other things I can just pick up something"* [P2].

The participants spoke about priorities, and some of their responses showed that their work comes before cyber practices or policies. For example, one participant expressed the burdensome nature of prioritising work life and cyber security and would find it easier if it was just work priorities. They said, *"It's a pain already prioritising because my life would easier if I didn't have to, my work day would be easier if I just prioritised my work"* [P2].

Another participant explicitly discussed that, although cyber security is important, delivering work goals are a business priority in itself. For example, they said *"If the job needs working out, that's your main priority to actually go out and deliver it. So, the security side is obviously important, but it becomes, you're always balancing those priorities. What do I need to do today?"* [P10].

One participant discussed that cyber security is introduced when an issue emerges, as supposed to treat it as a priority. They mention that this is a significant issue for small businesses. They said *"it probably becomes more of a general firefighting issue for a lot of people. And they deal with it when there's an issue, rather than putting it as a higher priority in terms of what they're doing. Certainly, for smaller businesses, I think that that can be the tendency"* [P10].

Some of these responses can also be described as 'attitudes towards cyber security, as they project their perception in the way they prioritise security. For example, one participant spoke about the fact because they are a small business, there are minimal reasons as to why they would be considered a target for a cyber attack. They said *"I just thought we're a small company, why would they attack us? But I suppose our customers are big customers. So they use us to get to them? I don't know* [P7]. The same participant also said, *"We all choose convenience over what the right thing to do is or doing the sensible thing at times"* [P2]. The latter responses in this theme could also represent the culture these participants share in their business, as it shows a general attitude towards cyber security. Following on from this, one participant discussed how they choose convenience over what is deemed as right. This also shows a shared attitude within the workplace. They said *"We all choose convenience over what the right thing to do is or doing the sensible thing at times. For example, you have a USB and there's a file that you need, the temptation is to just stick in your laptop and utilise it"* [P2].

5.4 Discussion Results from Study 1b BEIS Interview

In this Chapter, the results from Study 1b BEIS Interview are discussed. The results reflect the key themes highlighted in the study. It showed the relationship associated between each theme, and how relevant correlations were drawn upon.

From the results, the key themes are COVID, Productivity, Breach, Organisational culture, Motivation, Accountability/Reputation, Good cyber practice and Cyber Well Training. The questions presented to the participants highlighted interesting social factors that impact motivation to change behaviour, such as influence from peers and managers. However, the results also highlighted that there are challenges participants experience in changing behaviour. Some of which are defined by the organisational culture i.e., the norms and values of the workplace, and some by human limitations, like short memory and attention.

The results from the interviews showed some themes frequently occur, for example, the influence and impact of organisational culture in the perceptions and behaviours of employees, motivation and issues with the design of training content, further discussed in 5.4.1 to 5.4.3. For example, some participants experienced challenges with the structure and content of security training. This was quite prominent, as some participants had dyslexia, while others had preferences for listening and engaging, for example, they preferred audio training so they could listen while doing other tasks. One of the practical implications is reflected in this study, as there was little to no research conducted regarding the importance of training design, how organisation culture encourages and discourages security behaviours and how a cyber security breach contributes to motivation.

5.4.1 Organisational culture

The theme organisational culture was an apparent theme being discussed across the interviews. When participants were asked about how their social environment influenced their perceptions of cyber security, the participants spoke about the influence. They discussed the impact of influence from their colleagues, especially managers, had on their perception and how this perpetuates into behaviours toward cyber security. They discussed factors like workplace norms and breaking norms to fulfil work tasks, like sharing passwords. This theme showed that organisational culture may partly be responsible for employee behaviour depicted in the workplace. This finding buttresses Banduras' (1986) Social Cognitive Theory (SCT) that states that portions of an individual's knowledge acquisition can be directly related to others within the context of social interactions, and outside media influences. Also, when people observe a model performing a behaviour and the consequences of that behaviour, they remember the sequence of events and use this information to guide subsequent behaviours. This demonstrates the impact organisational culture has on employee perception and behaviours towards cyber security.

5.4.2 Motivation/Incentive

The second theme that was developed from thematic analysis was 'Motivation/Incentive'. The results differentiated between internal and external motivation. In driving participants, the internal factors appeared more frequently than external factors, for example, the participants discussed how their personal relationships and loyalty to clients motivate them to adhere to cyber security. One of the practical implications from this study is that motivation was not the focus, as this was part of a larger project, BEIS. However, all 14 participants mentioned motivation as factor that drives learning. This warranted further research into the factors affecting the transfer of training, and detailed questions about what motivates employees were asked in Chapter 6 (Training Selection Study 2 Interview Results).

5.4.3 BEIS Cyber Well Training

The final theme which appeared as prominent from the results was 'Cyber Well Training'. This is the training participants engaged with in Study 1b, the BEIS project. Participants presented their feedback about the Cyber Well training. They discussed factors such as challenges with the content and structure of cyber security training and they discussed how the content of cyber security training impacts the level of attention they place on the training itself. This theme warranted a further search into the literature, to identify what methods content developers use to select, devise and deliver training to businesses. Do content developers seek to understand the needs of the training participants? For example, do they research who their target audience is and seek to understand what conditions or factors enhance behaviour change? As a result of this, it is recognised that organisational culture plays an impactful role in changing behaviour and participants have challenges with the delivery and content of the training.

This raises the question, who creates cyber security training and what methods are taken to construct the undertaken training. As a result of this study, a further literature review was conducted, as it became apparent that the initial literature review sufficed for Study 1a and 1b, however the results from these studies highlighted there may be gaps in the literature that may need addressing. Pursuant to this, a further literature review was conducted about the design and structure of cyber security training and factors affecting training transfer. The analysis and results showed there are more questions to be answered and study 1a and study 1b served as a baseline or introduction to study 2.

5.5 Chapter Summary

In this Chapter, the key themes from Study 1b BEIS Interviews are presented. The key themes are COVID-19, Productivity, Accountability/Reputation, Good cyber practice, Cyber not priority, Organisational Culture and Cyber Well training. The results showed that COVID-19 impacted business logistics, activities and business structure and this was associated with levels of productivity employees imbibed in. This warranted a second study to investigate the drivers of attitudes, organisational culture and challenges experienced with security training. This is further discussed in 5.4. This Chapter discusses the relationship between experiencing a breach and becoming motivated as a result. Finally, the chapter ends by asking questions about training construct.

Chapter 6 Training Selection Study 2 Interview Results

The results from the qualitative collection in Study 1b BEIS Interview exhibited factors that hinder employees from following cyber security. Some of the challenges discussed hadn't been acknowledged in the cyber security literature, for example, some participants discussed the content and context of the training and how at times training could be out of context, unrelatable and indigestible because it doesn't appeal to them due to being complicated or boring. Therefore, further research was conducted into specific areas, for example, adult learning i.e., andragogy and the role leadership plays in learning. It became apparent after the literature review that there was little to no evidence that discuss the selection, development and distribution of cyber security training. As a result of this, a second study was conducted to investigate this. Specifically, three groups, were Awareness professionals, content developers and employees.

The second study involved interviews with awareness professionals, Content Developers and Employees of a business who receive cyber security training. There was also difficulty in finding UK content developers. Overall, there was difficulty in finding participants, due to the COVID-19 pandemic. Therefore, one of the techniques for recruitment was to create recruitment text and send it to potential participants who worked in professional jobs. The second technique was to manually find businesses online and contact them, the third technique was to contact prior participants from previous studies. These techniques did not yield the anticipated results, as some businesses explained that ongoing research and interviews were not a business priority. The next technique was to reach out to awareness professional developers at Bournemouth University, as this is also a business. So, a recruitment flyer was created this time for visual appeal and forwarded to employees who received cyber security training through email distribution, Twitter and LinkedIn. There was also a £20 Amazon prize incentive to persuade people to participate, especially due to other high priorities. There was a success there, the head of content development and the manager participated in the interview. This study went through Bournemouth University's ethics approval process, to ensure risks were identified and mitigated. This proved successful, as there was an influx of interviews, totalling 25 from the University. In each case, we ask volunteers to take part in an interview, incentivising participation within the case of the survey presented here a raffle prize. Making the process voluntary rather than mandatory carries both advantages and disadvantages. The success of semi-structured interviews is heavily dependent on the level of rapport the interviewer can develop with the participant – a participant that opens up to the interviewer is likely to give more honest and detailed responses (DeJonckheere & Vaughn, 2019). This is particularly true in the case of security interviews, that discussion can potentially touch upon self-reporting of transgressions, rule-breaking and circumventions. A good rapport is then necessary to build the trust that is necessary between interviewer and participant (Bell et al., 2016).

6.1.1 Research Question for Study 2

The research question for this study was invoked by the results from (Study 1b BEIS Interview) results. This will be further discussed in Chapter 5.

For example, the results showed that participants paid more attention to cyber training if it related to their work situation. In addition, they're more likely to learn materials from cyber training, if it addressed their needs. As a result of this, a further literature review was conducted. Specifically, into what factors impact adult learning, training effectiveness and barriers to cyber security training. The literature review highlighted disparities between how successful training is developed and delivered, in comparison to how it is developed and delivered to businesses. The disparity prompted the questions:

- How is cyber training selected, devised and delivered?

- How does the procurement and delivery of cyber training affect how people receive, retain and apply cyber knowledge in the workplace?
- How do social environment and cultural factors affect cyber training is treated in the workplace?

6.1.1.1 Research Challenges

There were recruitment challenges for these three groups. For example, several emails were sent to participants from Study 1b BEIS InterviewStudy 1b BEIS Interview to participate in this study. However, the companies that replied said COVID-19 is still a hindrance to them, and therefore they couldn't contribute to the research. One of the strategies to overcome this entailed visiting the Silicon South website to view SME contacts to email and call each one. After several attempts, the responses were synonymous with that of the companies from Study 1, i.e.COVID-19 had hindered their time flexibility and resources.

6.2 Recruitment

The recruitment criteria were that employees should have engaged in cyber security training in their current role and Awareness professionals ought to seek cyber security training for their staff in their current role. One of the ways to access content developers was via social media. Recruitment posts were written and distributed across Twitter and LinkedIn. A few content developers responded; however, they were abroad. This is a valuable finding to the overall project.

The most difficult groups of people to interview were awareness professionals and employees. After two months of attempting to recruit participants, the strategy changed. For example, rather than searching for these groups in the industry, it was advised to interview Employees within the University given staff have engaged in Cyber training. A poster was designed to recruit employees within the University, with a £20 Amazon prize incentive, to encourage participation. The poster was distributed via email to Head of Departments (HODs), who sent this to staff in their department.

6.3 Study Structure

There were written interview questions for Content developers, Awareness professionals and Employees. These questions were driven by the results from Study 1b BEIS Interview, and further by the literature review. The questions went through a ratification process, where they were sent to supervisors who corrected and suggested words that would encourage participants to open up.

After recruiting participants, Participant Information Sheet (PIS) was sent to the corresponding participants to ensure they were aware of rights, in terms of GDPR and privacy, and details of what the interview would entail. Due to COVID-19, there were no opportunities to interview people face to face, nor have them sign consent. Therefore, written consent was asked via email. The interviews with the employees within the University were scheduled via Teams. s participant had the option of showing their video or not. Each interview started by introducing the participants to what the project was about and reiterating what the PIS sheet said. The interviews followed an open-ended structure, by asking questions that opportune the participants to elaborate their answers. Open-ended questions were asked because they seem better suited to probe for more sensitive or stigmatising information (MacLaughlin, 2005). This indicates there is a benefit of asking additional open questions if the topic is of a sensitive nature (Friborg, 2013).

Each interview was recorded on Teams and automatically transcribed by the Teams software. However, some interviews did not completely transcribe, so instead an online transcriber called ‘Otter’ was used. Before choosing Otter, there were privacy and data management concerns, for example, where? And for how long would the recordings stay on their platform? Otter uses Amazon Web Services (AWS) for its data storage in the AWS region West, United States. Otter uses S3 storage and enables AWS Server Side Encryption (SSE) on data a public cloud storage resource (S3 buckets). It encrypts the key itself with a root key that regularly rotates. Amazon S3 server-side encryption uses a 256-but Advanced Encryption Standard (AES-256) (Lai, 2022). After completing the interview, each employee participant was emailed their £20 Amazon Voucher incentive.

6.4 Data Analysis

Thematic analysis provides a highly flexible approach that can be modified for the needs of many studies, providing a rich and detailed, yet complex account of data (Nowell, 2017). This is beneficial for this research, as it will provide common themes across interviews, which can create narratives.

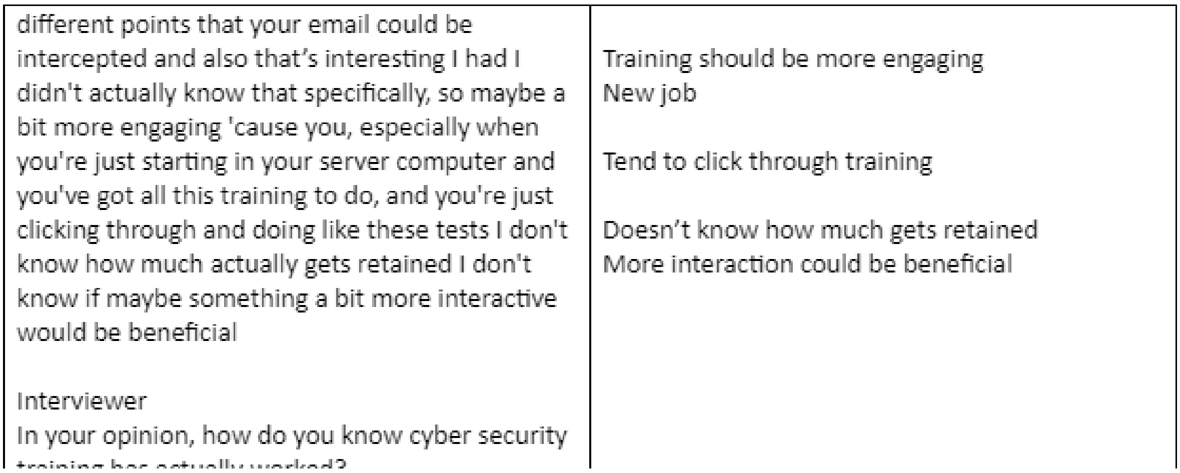
This qualitative phase aims to analyse and gather rich data. Therefore, we have considered the use of thematic analysis as it is a widely used method of analysis in qualitative research. Braun and Clarke (2006) argue that thematic analysis should be a foundational method for qualitative analysis, as it provides core skills for conducting many other forms of qualitative analysis.

6.4.1 Familiarisation and Coding (Phases 1-2)

Familiarisation is the process in which the research engages and gains insight into, what can seem like an amass of data (Terry, Hayfield, Clarke and Braun, 2017). The first phase is about generating early provisional ideas. Familiarisation involves moving through the entire dataset. Keeping notes in this stage ensures these early analytics observations are remembered and can be referred back to (Terry, Hayfield, Clarke ad Braun, 2017). Furthermore, the initial themes identified from qualitative phase study 1, can further be interrogated for deeper understanding. Thematic analysis can be adopted with all sorts of technology to code data. The way you can label data segments includes:

- Handwriting code labels on the printed data- for example, coding with wide margins to facilitate this.
- Writing code labels on sticky notes and attaching those to printed data.
- Writing each new code label on a hard-copy file card and clearly noting where to find each associated extract of data.
- Typing the code label beside the data in an electronic version of the dataset formatted into a two-column table.
- Using the comment box in Microsoft Word to select a section of text
- Attach electronic sticky notes to a PDF version of the dataset.
- Using one of the many software programmes specifically designed to assist coding and analysis of qualitative data, referred to as Computer Assisted Qualitative Data Analysis Software (NVivo, Atlis.ti).

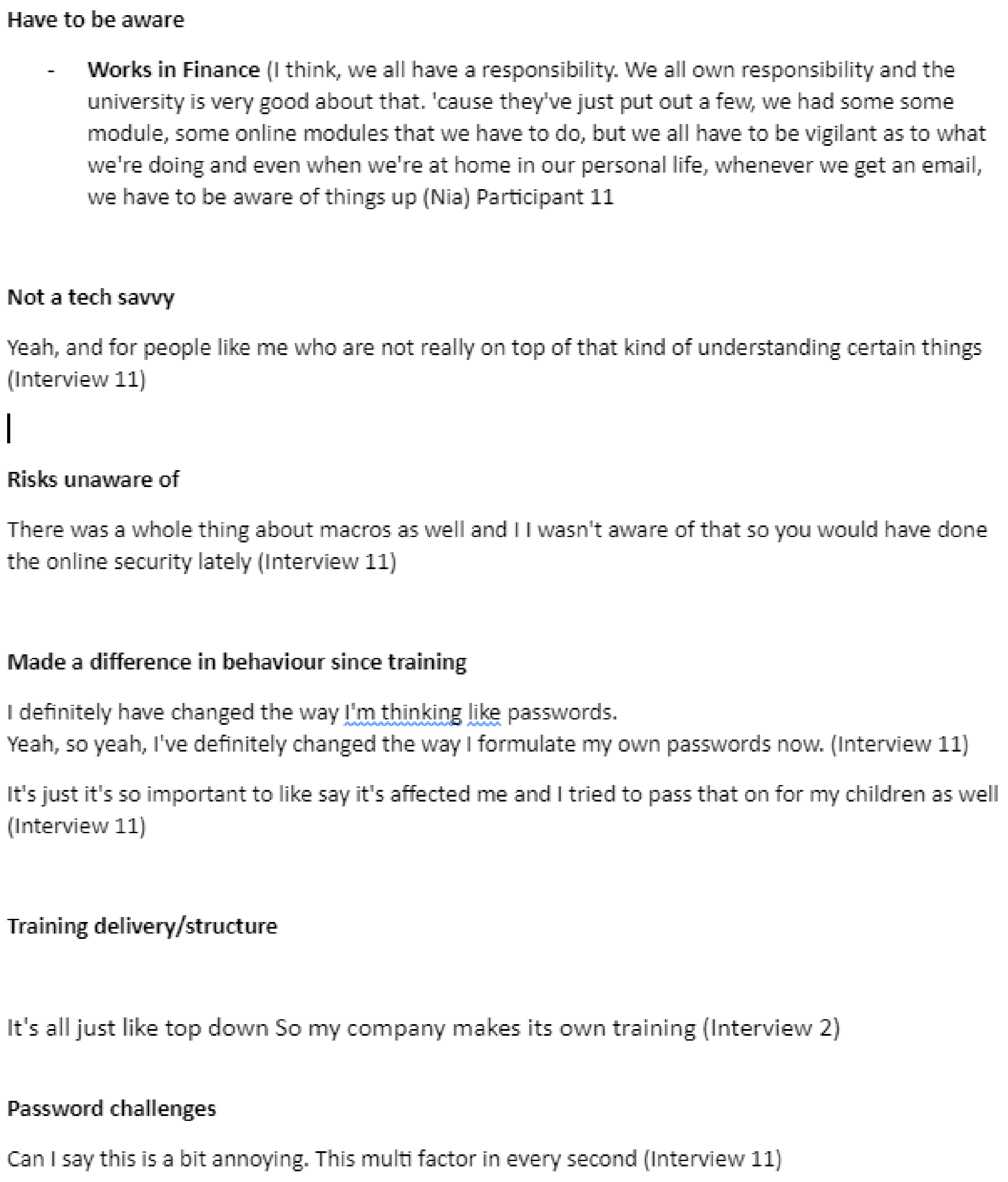
It's possible to start with one approach and move to another. For example, one might start with some hard-copy coding first, then develop coding further using CAQDAS Braun and Clark (2021, p.65). For the purpose of this project, handwriting code labels were adopted as a first step to code the dataset. The transcribed interviews were copied and pasted into a separate margin (Figure 13) on the left, and the codes were written on the right side. For anonymity the participant's name was changed to 'Interviewee'.



different points that your email could be intercepted and also that's interesting I had I didn't actually know that specifically, so maybe a bit more engaging 'cause you, especially when you're just starting in your server computer and you've got all this training to do, and you're just clicking through and doing like these tests I don't know how much actually gets retained I don't know if maybe something a bit more interactive would be beneficial Interviewer In your opinion, how do you know cyber security training has actually worked?	Training should be more engaging New job Tend to click through training Doesn't know how much gets retained More interaction could be beneficial

Figure 13 Handwriting code labels on printed data

As the Braun and Clark (2006) six phase framework was explored, the dataset went through another type of coding. After handwriting code labels on the printed data, Microsoft Word was adopted to select a section of text and tag it with a code label. For example, in this project any code that was deduced from the dataset was copied and pasted into a separate word document under a code label, where other similar codes were collated Figure 14 Using Microsoft Word to select a section of text



Have to be aware

- **Works in Finance** (I think, we all have a responsibility. We all own responsibility and the university is very good about that. 'cause they've just put out a few, we had some some module, some online modules that we have to do, but we all have to be vigilant as to what we're doing and even when we're at home in our personal life, whenever we get an email, we have to be aware of things up (Nia) Participant 11

Not a tech savvy

Yeah, and for people like me who are not really on top of that kind of understanding certain things (Interview 11)

Risks unaware of

There was a whole thing about macros as well and I I wasn't aware of that so you would have done the online security lately (Interview 11)

Made a difference in behaviour since training

I definitely have changed the way I'm thinking like passwords.
Yeah, so yeah, I've definitely changed the way I formulate my own passwords now. (Interview 11)

It's just it's so important to like say it's affected me and I tried to pass that on for my children as well (Interview 11)

Training delivery/structure

It's all just like top down So my company makes its own training (Interview 2)

Password challenges

Can I say this is a bit annoying. This multi factor in every second (Interview 11)

Figure 14 Using Microsoft Word to select a section of text

The final stage of the coding is ‘Writing code labels on sticky notes and attaching those to printed data’. In this stage, the codes collated from using Microsoft Word to select a section of text are printed and code labels are written on each sticky note, attaching them to corresponding printed data Figure 15. This option offers a physical and visual representation of the codes, which extends flexibility to moving the codes around.

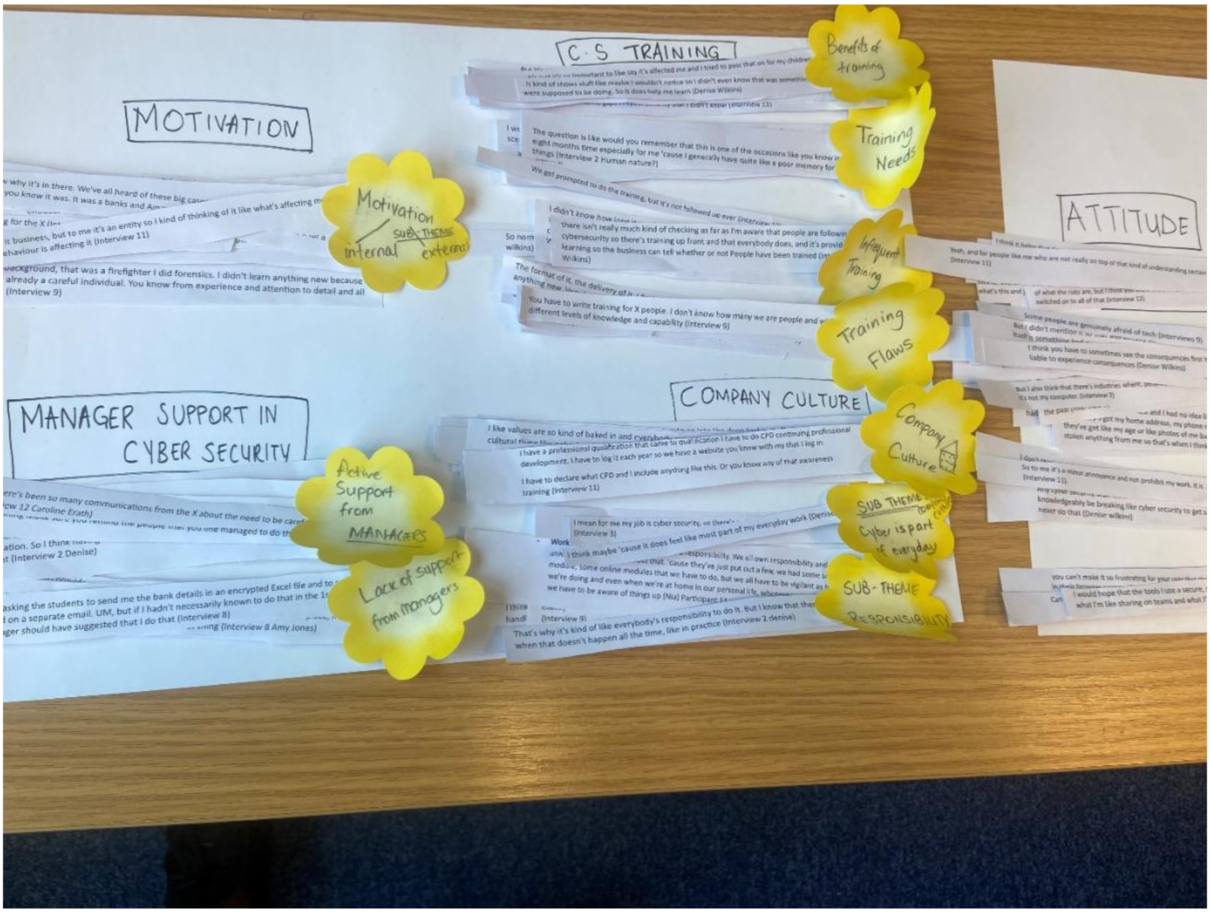


Figure 15 Code labels on sticky notes

There is no absolute test for whether coding is good enough, but Terry et al. (2017) found an exercise they call ‘take away the data. This is to test both developing coding and whether the code labels do a good job capturing meaning.

One of the primary factors Braun and Clark. (2021, p.54) consider in the coding stage is that, when looking at the list of code labels, one must ask whether they provide a summary of the diversity of meaning contained in the data set. For example, if the dataset was lost, could the codes create an understanding or narrative by itself. While there are no ‘right’ or ‘wrong’ codes, a good code label ideally contains enough information about the content of that data extract, and sometimes analytic interpretation, that is meaningful without needing to refer back to the data (Terry et al., 2017).

The thematic analysis does not require the researcher to code every line of data. It is good to remember that coding is a process both of data reduction (a way to reduce down and start to synthesise a mass of data), and a way of starting to organise the data and researcher observations of it into patterns (Terry et al.,2017).

The coding process is iterative and flexible, and code revision and development are part of this. Codes developed later in the process might capture a particular concept more clearly than earlier ones, and researchers tend to refine and revise codes throughout the process. The researcher will circle back through the data, to clarify, or modify, earlier coding, which also helps with coding consistency-avoiding having hundreds or even thousands of unique codes with lots of overlap.

One of the benefits of coding is that it helps the analyst make sense of the data, develop insight, and provide a rigorous and thorough foundation for the analysis.

After coding the entire data set thoroughly, this phase ends with the production of a complied list of codes that adequately identify both patterns and diversity of relevant meaning within the dataset (Terry et al., 2017).

6.4.2 Thematic analysis (Developing themes Phase 3)

In this stage, themes are the very active process of pattern formation and identification. Theme development first involves examining codes (and associated data), and combining, clustering or collapsing codes together into bigger or more meaningful patterns. For example, this could be as simple as identifying rich and complex code that potentially captures several other similar codes, which can be promoted into a provisional theme (Charmaz, 2000).

In this process, a central organising concept needs to be identified- a ‘clear core idea or concept that underpins a theme’ (Braun et al, 2015, p.102) that is unitary across the set of codes. This central organising concept helps determine what a theme is all about and whether any code fits within it. At this stage where themes are constructed through an iterative and reflective process of engagement, Braun and Clark (2021, p.72) see these as provisional themes. For example, imagining them as provisional themes gives room to discard, and explore other possibilities, before eventually settling on a final set of themes.

Braun and Clarke (2006) suggest using visual aids, such as thematic maps, to facilitate this process of shifting mapping of various patterns. Using visual aids, provides a way of identifying what the boundaries of, and the relationships between, each theme might be, as well as how different themes relate to each other and tell an overall narrative about the data. For the project, a thematic map was drawn, to present the themes discovered Study 1 (Figure 6). Such tools provide a way of identifying what the boundaries of, and the relationships between, each theme might be, as well as how different themes work together to tell an overall story about the data. A good quality theme is distinctive, with minimal 'bleeding' of codes between themes; themes should also be linked to, and work with, the other themes in the analysis- and each needs to have its own distinct central organising concept. The choice of mapping tools to construct themes is dependent to the research.

6.4.3 Reviewing and Defining Themes (Phases 4-5)

Thus far, the analysis has only developed candidate themes- the next phases are vital in the TA process, as the themes are further shaped, and some are dropped. The first stage of review involves checking whether the candidate themes capture the meaning in the collated coded data segments. Any disparity of mismatch between what is contained in the data extracts, and what the research claims those extracts demonstrates, which could reflect poor coding or poor theme development. This stage requires the researcher to check that their candidate themes work efficiently across the whole dataset, which entails moving back and forth the entire dataset, instead of just working with the collated coded segments. In this project we followed the same step, by going back to the dataset to ensure, nothing has been misses, and that as the analysis has been developed, it has not shifted entirely away from the key narratives in the data. One of the ways Braun and Clarke (2006) recommend distinguishing between themes is that most of the codes will only be allocated to one theme. If many are allocated to more than one theme, they risk obscurity. In this review stage, reviewing analysis involves making choices about the best and boundaries for inclusion and exclusion.

6.4.4 Producing the Report (Phase 6)

This is the final stage, where the overall report is finally produced. Braun and Clarke (2006) distinguish this as a separate phase for thematic analysis because there is a distinct final period of focus and refinement, where the researcher weaves together data, analysis, and connections to literature into a singular output that answers the research questions. This was adopted in producing the report. In this phase, they advise that when writing the report, one should move from an analytic point in the research process, coming back to the bigger picture of the overall project. While reporting the report, a key factor Braun and Clarke (2006) highlight, is the differentiation between the two styles for writing around data in TA: illustrative and analytic. For example, if data extracts are solely being used within the analytic narrative, then the evidence from data illustrates key elements of the story are being illustrative. On the other hand, writing analytically is when particulars of extracts are discussed by the researcher, with specific aspects composing the basis for analytic claims. For this project, the report was written in an analytic style. For example, the quotes from the interviews were discussed in relation to answering the research question.

6.5 Training Selection Study 2 Results

6.5.1 Chapter Introduction

In the Chapter, the motivation for Study 2 Training Selection is highlighted. This is followed by content developer results. The content developer interviews derived six themes; Selecting content for cyber security training, content structure, training delivery, beliefs about training participants, test training content and content developer challenges. In this Chapter, the themes identified from Study 1b were presented and discussed. The results highlight that employees are influenced by work norms and what they observe others do. For example, if the norm is to share passwords across the office, employees would also imbibe this culture. More importantly, a common theme across the interviews was the flaws in the Cyber Well training. The employees feedback their experience with the training and it became apparent that training delivered to SMEs are less bespoke and often left them feeling even more confused and insecure than they did prior to training. This raised the questions, How is cyber training selected, devised and delivered? How does the procurement and delivery of cyber training affect how people receive, retain and apply cyber knowledge in the workplace? Due to the unanswered questions, a further literature review was conducted and another study called ‘Training Selection’.

The employees in study 1b discussed that the Cyber well training incorporated irrelevant material and exceeded the expected time, which meant levels of motivation and attention decreased. The results from study 1b highlighted disparities between how employees claim training is delivered to them and what the literature suggests about how training should be selected and delivered. For example, Knowles (1987) suggests adults should be involved in defining learning objectives, which is a cardinal principle of andragogy. Whereas, the results show that managers often give employees training, with little to no autonomy or say on what training content should address.

This section will present the results from Study 2 Training Selection. Three interview groups were interviewed. These were content developers, awareness professionals and employees. The content developers are cyber professionals who develop training content and material for businesses. Awareness professionals are the internal cyber professionals, often managers and team leaders, who request and deliver training to staff. While employees are the recipients of the training material. The questions around the content developers centred understand what process of training selection they go through to derive training content, what quality control processes they imbibe in, how they test training content and how much of user needs are gathered, considered, and included in the design of cyber training. The awareness professionals were asked questions about how they choose their training for the business. They were asked what challenges they experienced as a business, how much user needs are researched or explored, and how much of this if any at influences how the process of training selection or delivery? Thirdly, employees within organisations were asked questions about who influences their decision-making process to adhere to security, what are their motivations to follow cyber security and also questions around what factors hinder their willingness to learn and in turn change their behaviour.

6.5.2 Content Developer Results

The results are divided into three sections; content developers, awareness professionals and employees. Each result section will be discussed with correlating arguments, relating to the literature.

6.5.3 Selecting content for Cyber Security Training

The first theme derived from the interviews was 'Selecting content for Cyber Security Training'. This theme represented the process content developers take when they choose what training material they want to incorporate into training. The participants gave various methods by which they go about selecting training, in which the thesis define as subthemes. There are subthemes across interviews with content developers, awareness professionals and employees. The subthemes can be identified in the *italic title text.*

Subtheme of Selecting content for Cyber Security Training-Training Framework

When participants were asked what process do, they go about selecting content for training, they had various methods. For example, one content developer said "I pick out their framework or what I want to teach, for instance if it's Ethical hacking, I could pick a framework like PPT or the OSSTMM or NIST or CIS controls and look at it. It's the most detailed way from my perspective because I'm obviously going to try all of them and see the one that works. But again, some of these frameworks, different ones work for different sectors" [P6]. These participants specifically discussed cyber security frameworks they observe and review when they look at training. For example, "There's a standard called NIST, an American based standard, and that's what we follow where I work next. Yeah, so I try my best to because we follow that framework, I try my best to map the topics that I picked" [8].

They discussed the importance of following a framework to select training. Their responses reflected the necessity to deliver relevant and effective training to businesses. For example, one participant said "I have to do is I review everything and see if it's suitable for like the X audience, because some of the stuff wouldn't necessarily say the right message that we want to convey. Because Nob4 it's not just tailored for education, it's tailored for, big banks, and loads of big, different types of institutions. So eventually, we hope to make our own bespoke content, we do have those capabilities. It's just finding the time right now [P3]. This response highlighted tailored training for businesses, to reflect relevant environments to that of the participant. In light of this, another participant discussed the need to select training with long standing reputation because it minimises unsystematic training. For example "I'm very heavy frameworks because if you're not careful you're going to be teaching things haphazard, so I pick out the framework because this framework developed by Organisations that have years before me" [P6].

A theme map of the content developer results is presented in Figure 16 Content Developer Theme MapThe theme map shows the relationship between themes via dotted lines. The themes are presented in a blue box, and corresponding subthemes are presented in a green box.

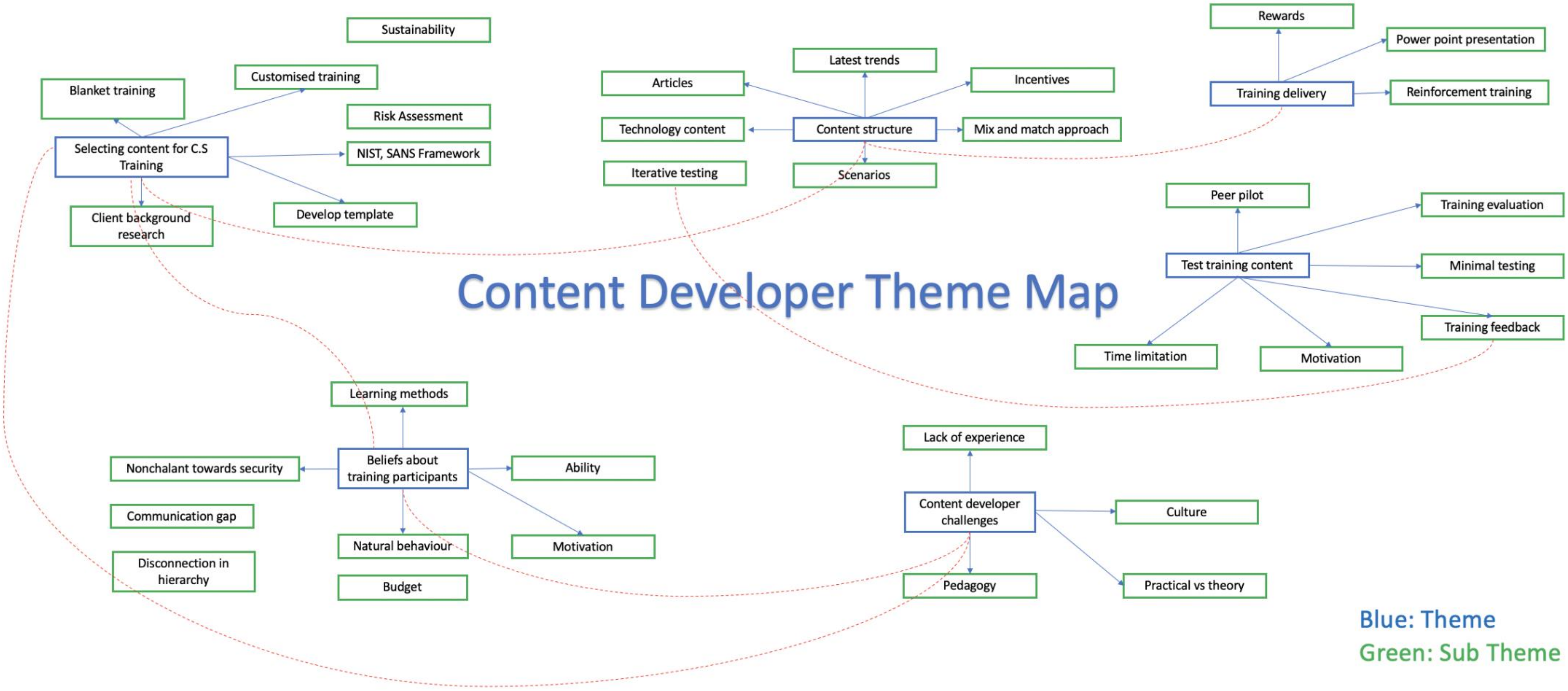


Figure 16 Content Developer Theme Map

Subtheme of Selecting content for Cyber Security Training-Risk Assessment

Following this, another sub-theme that was developed from this theme was Risk Assessment. This was prevalent in only three interviews and it shows that assessing risks associated with or relevant to clients are not assessed before or after delivery. In light of this, these three interviewers discussed how they research the industry threat landscape and assess what risks are relevant to the organisation they are developing training for. For example, one participant said “we research out there, they are vendors we partner with to deliver these. They are probably mostly delivered online… Then what we typically do is a risk assessment, of the landscape, within the organization. So pretty much kind of figuring out, what really are the risks? Are there high risks? [P8].

Another participant spoke about who develops training, they spoke about an intern student who pieces training together for their entire organisation. For example, “we've got an intern at the moment and he's developing us eight pieces of e-learning, 5 minute e-learning …We assess the courses and say yes this is a good one. This is not right. Let's put that one into the learning path” [P9].

Subtheme of Selecting content for Cyber Security Training-Personal knowledge

A developer discussed that selecting training comes from personal knowledge, or knowledge acquired from previous education. According to them, training is taken from various angles. For example, “My colleagues and I, we do a lot of reading and self-learning. So at the point of developing material, we may not have necessarily consulted anything, but I'm pretty sure subconsciously things have come from different angles. So, for instance, stuff I did at school like in my masters. I'm pretty sure a lot of things that I learned there I put them into practice” [P4].

They added that policies are not rigorous because they do not come from an academic background. For example, we don't have like a document detailing something and having citations behind that. “Like, it's not that that rigorous. But it doesn't have to be because we're not academics here” [P2]. This reflects the attitude developers have, for example, they believe research is solely for academia.

Subtheme of Selecting content for Cyber Security Training-Blanket training

In this section the sub theme ‘Blanket training’ is presented and discussed relating to the conducted interviews of content developers. The results showed that all the content developers select all-readymade training and restructure some elements to suit their intended audience. Only 3 out of 9 Content developers interviewed, occasionally develop customised training, this is as of when clients request this. Therefore, this sub theme is named ‘Blanket training’. One participant gave their challenges they experience, if they intend on tailoring training to each organisation such as, sustainability. They said “So, if we were writing bespoke content for every client, that wouldn't be a sustainable way of running an assess business, it would be a consultancy, but we're not consultancy. So, we would only gather training requirements if the customer was paying us for a bespoke piece of work” [P1]. Another participant gave a similar account, they differentiate between the need for having multi-use training and perhaps different content for another type of industry. For example, they said “So for instance, if I were to do the training for EFCC, I could probably use that same document for ICPC. They handle same financial crimes, so they literally do the same job. So I could probably use the same, the difference might be like 5% difference to material here, but I can't use the same for like health insurance scheme people. Because they're in a different industry. They have different risk that we face or different threats they’re exposed to [P4].

Subtheme of Selecting content for Cyber Security Training-Global training

Similar to this, some participants recognised that training is normally developed on a global scale, to reach a wide range of audience and it doesn’t reflect local settings of a business. For example, “So most materials pretty much are developed on a global scale, and not in a localised context so it effects how participants relate with trainers or read through the contents” [P5]. This same participant discussed that they develop bespoke training for clients by building on work they have done, or by extracting content from free sources. For example, they said “if it's for totally new organization or industry, its from scratch. But most times I rely on materials I've developed. Also, sometimes I look out for materials from ‘Critical license’ like free distributed license [P5]. Similarly, another participant discussed that the pre-made training they select, already has methods of delivery such as videos. For example, they said “we use a third party supplier called Nob4 and that comes with pre created content, things like training modules, videos” [P3]. On the other hand, content developers discussed challenges they perceive when they develop global training. For example, “You're planning training for employees that are in the Nigerian company and all your examples and images have white people, does that have a negative impact on the interests, it probably will” [P5].

Subtheme of Selecting content for Cyber Security Training) - Customised training

Considering the blanket training sub-theme, another sub-theme called ‘Customised training’ was deduced from the set of results. The results suggested that a few content developers custom training to meet the needs of its intended audience. One participant spoke about personal preferences, in terms of having a liking for customised training, as opposed to there being a factual reason or reason as to why customised training is suitable for cyber security. Or example, they said “I like things, being unique, but also because sometimes when you develop this training It's gotta be unique to your environment and not every environment is the same” [P8]. Another participant discussed how they try to accommodate business requirements from companies they offer training to, however, they have core modules in which they build work upon by liaising with companies administrator. For example, they said “Just as important to hear what people actually want to see. And because we have loads of clients, and most of the people, I often meet are administrators on calls, when they have something to tell me or we have been developed custom content for them as well. So we have our core modules, as I said, but when they want something that we don't have, I do work with them to see what they want” [P7]. Similarly, a third content developer mentioned that although they develop their own templates, they modify it suit whomever they intend to deliver training to. For instance, they said “so we developed our own templates and so we modified based on the client or a particular industry the person is in. But we had to develop our template from scratch before we can start using them to customize for customers” [P4].

Selecting content for Cyber Security Training Subtheme (Client background Research)

The content developers were asked if they gather user needs when they develop cyber training, this was to understand what drives their selection and delivery of training material.

One participant discussed that they assess the overall objective of training, followed by assessing maturity levels. For instance, they said “I asked them what they objective is what they're looking to get out of the training rights that defines the reason for training, for example compliance or legal reasons [P5]. This participant found that when they select training this, they identify some employee needs. For instance, they said “Also some clients tell you they need security for compliance. So that also drives how the training material will be developed” [P5]. Similarly, the second participant said “It’s typically based from research, industry research. But I also take into account the client needs as well, so that’s where talk about the risk based assessment” [P8].

The content developers who developed custom training, discussed some methods they take to gather requirements. For example, “There are two general ways I do it, so it's either I do my research on the firm, maybe I check their website and look for them, talk to one or two of the employees, or I could go in for an actual meeting with HR, and try to find out more about them and the idea is to build, to conduct like a surface skills gap analysis to see where they are. What they need to know as regards to cyber security and then we craft our content around their operations and where they are lacking” [P4]. Like this developer, others also conducted analysis by looking at industry and identify what security maturity levels are. They said “I Look at industry, what their position is. If I was different client. I’m going industry and build materials based on the industry. So before I jump in the training I ask about maturity level of the employees” [P5]. Lastly, they discussed how they evaluate how users best learn, what keeps training participants interested. For example, “You start with the need, why we've been asked to develop this piece of learning…you pull out your learning objectives. So what are we supposed to achieve here? We use blooms taxonomy to actually start making sure that we're with calling out reasonable learning objectives” [P4].

Another participant gave another perspective, they discussed assessing what the associated risks are to the client and proceed to access current content. For example, they said “what are the risks? So we look back at the risk register. Will look back at the why they needed this enhanced training and then we assess our current content and say is there any of this which is useful? [P9]. When the content developers were asked about research client needs, they identified that most training participants struggle to express their needs, so instead speak about general information. For example, “Mostly people would not know what to say, so they end up telling you know, common” [P5].

(Selecting content for Cyber Security Training) Sub theme: Training frequency

The content developers push the same training content to clients, one participant discussed how he gives the client access to choose the level of frequency, they want learning reminders. For example, they said “So they select how often they want them, but we send the same sort of nudges for everyone, but they can just select the frequency of it” [P2].

6.5.4 Testing training content

The content developers were asked what methods of testing they go through, to test training content before it is delivered to the training participants. The overall narrative shows that, content developers rarely test training material they develop, before they deliver it to clients.

One participant gave a multifaceted answer about the culture around testing in their company, and this highlights the attitudes and disposition this content developers feels towards testing. They found there was little to no reason to test training, as there is a level of trust, they put in the work they produce. For instance, they said "*I try to do one for myself and I still try to do on my colleagues. Depending on how much time we have sometimes because of how things get approved here You might have just a few days to get ready. We have a lot of trust within our team mates capability…we do not really scrutinize each others work like that, you know*" [P4]. The results showed that participants generally delivered training without testing training. Some participants explained this was due to the maturity level of the business, for example *"And being like, completely honest, we are not as mature in this area as we would like to be"* [P1].

Testing training content Subtheme - Peer Review

Similarly, some participants explained they conduct some peer reviews, but there is no actual test or validation for developed material. For example, "I didn't think I had to do that. Well, I've got some peer review, but not an actual pilot" [P2]. This disposition represents the majority of what the content developers said in the interviews, they generally either did not see a need to test training or there is a level of trust and confidence they share in their working capability, which may also represent a culture content developers share.

On the contrary, there were two participants that went through a review process of developed training. One of the participant pilots their training to departments within the organisation and based on the feedback they receive there is incremental finetuning of the training. For example, they said "we typically pilot online training with a couple of departments and get feedback and based on that I would improve certain things because again user feedback is always key" [P8]. This participant recognised the usefulness of user feedback. They went onto explain their process of getting training feedback from businesses they deliver to. They said in addition to going through content material with their manager or colleague, they gather live feedback from their training audience. For example, they said "I will review pilot with either my manager or a colleague of mine…and I would gather that feedback, eventually deliver it. When I'm done with the actual training to the live audience, I also gather their feedback and I use it to improve on the next that I'm going to give them" [P8]. Lastly, one participant discussed that the review process involves a colleague or manager, which will give feedback. For example, “Review pilot review with either my manager or a colleague of mine. You know to kind of go through it and give me some feedback on the content” [P8].

Testing training content Subtheme - Interviews

The second content developer had a different approach to testing content. They gave an account of how they conduct interviews to gather user requirements, and how they consider this in the training they develop. For example, they said “I've done about 30 interviews and I also tested it internally with all our employees. I analyse them afterwards, I prepared an Excel sheet with questions to all the employees within the company and I randomly selected X number of people to review all the modules…I took all the feedback and suggestions into consideration, it took a while to release the module” [P2]. This response shows a thorough methodology this content develop takes to test training, but it also highlights an issue of time that some content develops seemingly face. For example, “Depending on how much time we have sometimes because of how things get approved here, you might have just a few days to get ready” [P4]. Considering this, some content developers spoke about challenges they experience when they try to gather user feedback. For example, “frankly, I have been struggling for a long time. Even till now, I struggle with that, the only metrics are just attendance” [P6]. Another challenge the participant expressed was that, it was difficult to access every participant when training is delivered in a group. Instead, they propose a solution, by conducting general tests. For example “it's hard to access every individual when you do it in a group form. So the easiest way to know if each person is learning is to have a general test that everyone has to answer and submit their answers” [P4].

6.5.5 Training delivery

Most of the training delivered by awareness professionals are ‘shop bought’ (7.2.2.2) training. Some content developers assess training by looking at feedback, to provide what they think is most effective for training participant. They deliver training in a PowerPoint presentation style. For example, *“it could be PowerPoint presentations in person, so it all depends on what's effective, right? We try to gather statistics. I try to look at the feedback, I try to assess the situation and figure out. OK, what effective in this context, given the kind of budget we have”* [P8]. In addition to delivery style, the participants mentioned they assess the industry standards for training, and deliver training based on how they believe employees best receive information. For example, “*based on a couple of things, what I see is being done out there in the industry and also how I feel like users are actually receiving the information”* [P8]. They added that training is delivered in forms of posters and email distribution. For example, *it could be like in the form of like posters, infographics. It could be newsletters, sending emails like a blast of emails* [P8].

Subtheme of training delivery-Workshops

On the other hand, some participants discussed their process of sifting through training material, they discussed that when training is selected, it is broken down into workshops and different scenarios are created. For example, “So when we take this framework, we sort of break it down. We then give workshops and tasks that help students fully understand this framework. So, it's not just going to be take this framework and learn about it. No, it's gonna be create different scenarios [P6]. Interestingly, another participant discussed another technique they use, they discussed that they look at the threat landscape and select training based on prevalent risks. For instance, they said “For security awareness, I look at trends, security reports for previous years, I use Verizon report. I look at top trends, top breaches, how it worked and impact, use that to draw the baseline for content for general security awareness [P5].

Subtheme of training delivery Subtheme Language

One of the considerations when delivering training, is language. They acknowledge that uncommon terminology may confuse people, but if they can identify the best way to reach training participants through simple and engaging language, then they are more receptive. For example, “If the first thing you mention is firewalls, they are looking at you like What is it now? So if you can, you know talk to them in languages that are pretty simple fun and engaging manner then the other parties can be more receptive or what you're trying to teach” [P6].

Subtheme of training delivery Subtheme Mandatory training

The content developers spoke about mandatory training, it includes information about security risks. For example, “So, there's always what you called the mandatory training. Which just gives you what the basics of what you need to know in terms of the risk and outdated threats” [P8]. They also deliver reinforcement training, which goes into detail and focuses on specific subject areas. For example, “there is the reinforcement training. So, it pretty much reinforces those concepts that you learn, and then that goes into a bit more detail. It's now more selective and it's focused on specific topics” [P8].

One of the methods the content developers adopt to deliver training, is to send short messages and put posters across office walls. For example, “short stuff that could be sent via email he could put on the wall in the office, or you could use as wallpaper and so things like just simple things we try to do that” [P4]. They believe this will instil a secure behaviour culture in the organisation “It helps build a behaviour which becomes the organizational culture over time because that's the other end to it. When you do awareness we are building behaviour and yet your aim is to have a security culture at place in the organization" [P4]. This participant added that, they incorporate debates, training competitions and quizzes that result in rewards. They claim this helps training participants pay more attention. For example, "What we do sometimes we try to add rewards. So during our trainings will have competitions or quizzes, we have arguments like many debates and we randomly give rewards, it makes people to pay more attention because they don't want to do poorly on the quizzes they passed" [P4].

6.5.6 Training Evaluation

A theme from the results is 'Training evaluation'. The content developers were asked what training evaluation methods they use to verify training success, i.e. How are training objectives evaluated? The overall narrative around the theme showed that content developers have little to no measures in place to evaluate training success.

However, one participant expressed that they check if their employees change their passphrase after the completion of training modules. For example, "*we check whether someone changes their past passphrase, after completing our training module"* [P1]. They proceeded to describe a Likert survey they ask participants to complete and their scores whether they disagreed or not, would be an indication that training successfully fulfilled learning objectives. For example, they said, *"I'm regularly informed about the cybersecurity issues relevant to my job role… And then people are asked to rate whether they strongly disagree or strongly agree and this would be an indication of whether their training programme is doing what it's meant to do"* [P1]. For this participant, another method to check if training successfully fulfilled its learning objectives is by discerning if people have improved their behaviour, by checking if their passwords have been changed since instructed to. For example, *"ask them if they want to set another password or improve on that first password. If they say yes, then that's a free choice. You can infer from that, this person cares about security, and they're improving their behaviour. If they say no, then you can infer from that they don't care and they're doing it because they have to"* [P1].

Subtheme of Training Evaluation-Training Feedback

Some content developers collected training feedback from employees. The feedback generally focused on issues with training delivery, for example, they discussed that content developers speak too fast. For example, "I think one feedback I got this which is hard to implement, is that I talk too fast" [P5].

6.5.7 Content developer objectives

The content developers discussed their focus and objectives they aim to achieve when they develop training material. They mentioned that focus should be effective training, that will enhance behaviour change. For example, "what you want to be focusing on is training that is effective that will change behaviour" [P8]. Another way to define training objective is to write a business case and define what the objectives are. For example, *"standard way of doing this is we write up a business case. So we define what we're trying to achieve the objectives, your priorities, and solution requirements"* [P3]. They also mentioned if there is a gap in knowledge and participants are unaware of certain risks, this time frame is a good opportunity to train people. For example," *If you do realize that there is a gap and there are certain kind of risk, the person is unaware of, that's your entry point into helping the person understand … do you know about this and that?"* [P8].

One of the objectives for training, is make training participants see cyber security as a priority, they want to ensure everybody sees it as a joint responsibility. For example, "to make cyber more of a priority and try to get people on board. The main thing that we're trying to plug is it's everyone's responsibility" [P3].

Another objective is to focus on non-technical people, specifically people from legal teams and accounting departments. The purpose is to carry individuals along and ensure employees know what part they need to fulfil in the organisation. For example, "*I conduct cyber security awareness trainings and my focus is on people who are not tech savvy or who are not IT trained or educated. So for instance in an organisation I would ensure that everyone attends especially who are in the legal teams, those who in accounting and stuff like that. The idea is for everyone to get carried along so that everyone knows their roles to play in the organisation"* [P4]. In addition, another content developer specified that the target audience for training, could be one person, who will influence other people. For example, *"typically I don't wait to have a set of people or an audience to deliver training to. If it's just one person that one person is key, because if I change that person's behaviour, that person can influence other people. That's how I kind of see it"* [P8].

6.5.8 Beliefs about participants

This theme surmises the perceptions and beliefs content developers have concerning training participants. It also highlights, past events and feedback, which encompasses beliefs they hold towards training participants.

Subtheme of beliefs about participants - Fear

The content developers express perceptions they believe training participants have towards cyber security. The consensus across the interviews portrays various beliefs, ranging from a lack of understanding to fear, participant motivation, and human limitations such as concentration. One participant illustrated the ripple effect of fear, for example, "I would say because people are generally scared of what they don't know or they just discard it… And then you just shut their minds to it" [P6]. As well as that, participants expressed that people generally have a limited attention span for cyber security, and if the wrong message is sent, there is likelihood to disengage participants. For example, "If you just bombard people with training, everyone has a limited amount of concentration they can put into security. And if you fill it up with the wrong things, then when you need to talk to them about something important. They're already bored. So it's important not overload people" [P1].

Subtheme beliefs about participants - Motivation

Despite this, the content developers described assumptions about employee motivations, to adhere to cyber security. For example, one assumption was that employees had experienced a breach in the past. They said "Some are motivated because they have had a nasty experience in the past and they don't want to repeat that" [P8]. Similarly, they recognise a multifaceted motivation employees have when it comes to their personal reputation and the company too. For example, "The company to lose revenue if this happen the employee understands the larger risk so they are not like I want to use my flash drive. I don't want to be responsible for this issue" [P4].

The content developers assume different industries, for instance, industries with less regulations are non chalant to security, as they do not understand the business impact of their environment. They claim to solve this by providing training participants have different attitudes towards security. For example, "for industries that are not heavily regulated, they feel like why do I need to bother? So, at the end of the day, they don't understand the business impact because they don't have visibility into what's going on in their environment and how I try to solve that is by providing customers with some form of assessment" [P8]. They mentioned banks in particular, are regulated, hence they have regulatory bodies to ensure compliance.

For example, “banks are heavily regulated, so they don't have a choice but to just be compliant because they have regulation bodies that enforce those components that we enforce those compliance regulations and laws” [P8].

The content developers acknowledge they assume to know training participants knowledge and aptitude. They base training content on requirements Awareness professional provide upon requesting training. They developers later discovered that the training content was unsuitable for this target audience. For example, “As trainers we assume to know the knowledge of participants. We based the feedback or the input I was given by organizers. I had approached the training, in a particular way and then halfway down the line I found out that the knowledge level of participants way lower than expected” [P5].

The content developers described their assumptions towards the younger generation, they assumed they would like to do quizzes and games, for its competitive nature. However, upon delivering training, they found some hypothesis to be untrue. For example, “We used to initially think that the younger audience would be like quizzes or competitiveness of the games we do have during our sessions, so some assumptions may be flipped when you test things” [P4].

Subtheme beliefs about participants-SME Challenges

From the results, the content developers discussed challenges they believe SME’s experience. They discussed issues such as budget and relationships between seniors and employees.

The content developers mentioned that budget is an issue for businesses, and therefore they try to give an affordable bill, otherwise this could detract businesses from looking for training. For example, “it's tricky because you can't exactly give them such a high bill 'cause they would there be discouraged”. [P6]. As a result, their goal is to raise cyber security pioneers who will talk and campaign cyber security messages and from there start to monetize. For example, For us right now the goal is get pioneers and talk, preach, shouted message and then we can start to monetize it fully from then on” [P6].

One of the challenges identified is that, there are communication issues within businesses. For example, “there is a huge disconnect between management and executive level and the work security teams do in a lot of businesses. There is sort of lapse in communication" [P5]. This participant noted that in time past, they have encouraged businesses to not arbitrarily schedule training. For example, "we've also tried to encourage like the board, the management beforehand explained to the employees, don't just schedule a training" [P5].

6.5.9 Content structure

The content developers discussed how they structured training, some of them discussed the orientation of these structures and how they believe it benefits the training participants.

One of the participants mentioned that their preference for Power point presentations, is the motivation for this approach. They prefer to speak and present, rather than use a lot of words, to keep engagement. For example, "*I'm the kind of person that would prefer to have a lot more pictures on my PowerPoint slides and I speak to them. Rather than have a lot more words on it so that way you keep them engaged"* [P8]. It was identified in 7.2.5 that content developers believe the younger generation liked to do quizzes and games. This also transcends into how training is selected, as content developers take 'mix and match' approach to appeal to a younger audience. For example, "*So for that I try to find the mix and match, on the word content, but for more likely edgy audience. You know, like the young folks"* [P8].

One of the content developers mentioned that they structure training, in three 3 levels, they begin by drawing the training participant attention, followed by what they defined as the boring part, and lastly close it with interesting material. For example, *"I find ways to make the beginning of the content the content very interesting to draw attention. The boring parts in the middle and then close it with something interesting tell jokes in between and all that"* [P5]. In addition to this one participant said they structure training based on setting objectives they want participants to take from training. They offer training on two levels, employee level and at organisation level. For example, "*We actually have objectives by topic, so that we know that these are the things we want each participants to take home from this presentation. So we do it at both levels at both the individual level and then at the whole Organization level"* [P4].

As well discussing where content comes from, the developers spoke about how they structure this content into training presentations. Firstly, they select articles that speak on a security related issues, then they take screenshots to use in presentations. For example, "*things from articles… that talk about maybe BEC scams, latest trends. What storyline are* *they using?... I could take screenshots I engage with a scammer and use it in my presentation"* [P4].

Subtheme of content structure-Scenario based

The content developers discussed how they structure training using scenario-based training. Some of the scenarios, place the training participants in the context, and this prompts them to reflect and think what risks affect a particular department or group. For example, "We create scenarios, the assignments for students can be along the lines of, imagine that you are the head of HR, what are some of the industry businesses cyber security risk? how will you prompt them to find out what their risks are and what technologies will be put in place to mitigate those risks? So now they go back and they actually think. What are the risks that actually affect HR department, HR and admin, like insecure attachment?" [P8].

6.6 Discussion of Results from Training Selection

6.6.1 Training Selection

The content developers were asked how training is developed and selected. They often selected training from renown cyber security frameworks, such as National Institute of Standards and Technology (NIST) and Open Source Security Testing Methodology (OSSTMM). Some content developers would trial a plethora of training and select training on what they think works best. Their reasoning for this, is because existing training framework have existed for a long time and have a long-standing reputation. They believe following this method will minimise delivering haphazard training. In addition to cyber security frameworks, content developers selected training from acquired education and knowledge. This can prove to be problematic, because there is little to no way of verifying if this knowledge is scientifically or academically true, this means content developers could be developing false content and misleading people. The developers discussed that cyber security policies are not rigorous because they are not academics. This reflects the attitude developers have, for example, they believe research is solely for academia.

The developers shared that training is developed with the intention of dispersing training across various industries, countries and departments. They described that one of limitations of developing bespoke training for clients, is the issue of sustainability. They felt developing specific content for businesses would impact the efficiency of the business, and instead this method is best represented by cyber security consultants. However, in doing this they experience challenges when they disperse training intended for local businesses, to business on a global scale. They note that employee interaction with training may be negatively impacted when training participants cannot relate to people in the training. According to Bhatti and Aldossary (2021), they conducted a study on training effectiveness, social support and instrumentality on transfer of training. Findings of their study suggest that if training contents are not similar to the employees work setting, training transfer will decrease, and all resources and efforts allocated by the management will be wasted (Research in practice, 2012). For example, in Korpela's (2015) study to improve cyber security awareness and training programs with data analytics. They suggest cybersecurity education must be customised to give end users a learning experience that is in line with their regular job duties, time constraints, and learning preferences. Most importantly, their relationship with technology.

Some responses portray challenges awareness professionals contribute to how employees perceive cyber security and their interactions thereafter. They insight that employees may not fully understand the consequences of poor cyber practice. This exemplifies Safa et al. (2012) notion who suggested that employees may not be cognizant of the consequences of poor cyber practice. While the same training is sent across to clients, the developers discussed they give clients a choice of how frequent they want to receive nudges. This can be seen as a positive initiative, but this is problematic for businesses who do not know how nudge works or how it is meant to be educationally benefit them. Also, if awareness professionals have lapse attitudes towards security and are not motivated, they could easily decide not to send nudge reminders at all.

6.6.2 Testing Training Content

The content developers rarely tested training material before they deliver it to clients. Some of this was due to a culture of trust amongst developers. On the other hand, other developers said they have the desire to test training beforehand, but they feel their business is not as matured to have such procedures. However, testing is a paramount composite of design process in Information technology. For example, in System Analysis and Design (SAD) every designed system will go through a series of tests, to ensure quality control, ensure the products meets client requirements and it provides a means of evaluation and maintenance (Dennis et al., 2015). If applied to cyber security training, content developers may refer to client requirements to ensure training is aligned, and this may reduce distractions and disinterest. In light of this, two developers had a peer review process, which entailed piloting a training session to departments within the organisation and based on the feedback they receive, incrementally they fine tune training material. Rather than testing training, some developers carried out interviews with internal employees, and randomly selected them to review developed training models. However, their methodology is impacted by time limitations, for example, if there is an urgent need for training, they can be limited as to how much testing they can do.

The developers were asked if they collect or gather metrics of employee feedback and they shared, this was a work in progress. In fact, this was a challenge because they find it difficult to access every participant when training is delivered in a group. Instead, they measure attendance, i.e. people who attended and completed training. Patterson et al. (2011) recommend content developers to maintain communication, so they can collect data on when and why people fail and use that feedback to improve the program. While security awareness and training metrics can benefit a company by giving it a better grasp of the attitudes and behaviours of its users in relation to their activities, they are unable to give the company a fuller and more nuanced picture of its users' learning experiences (Korpela, 2015).

6.6.3 Training Delivery

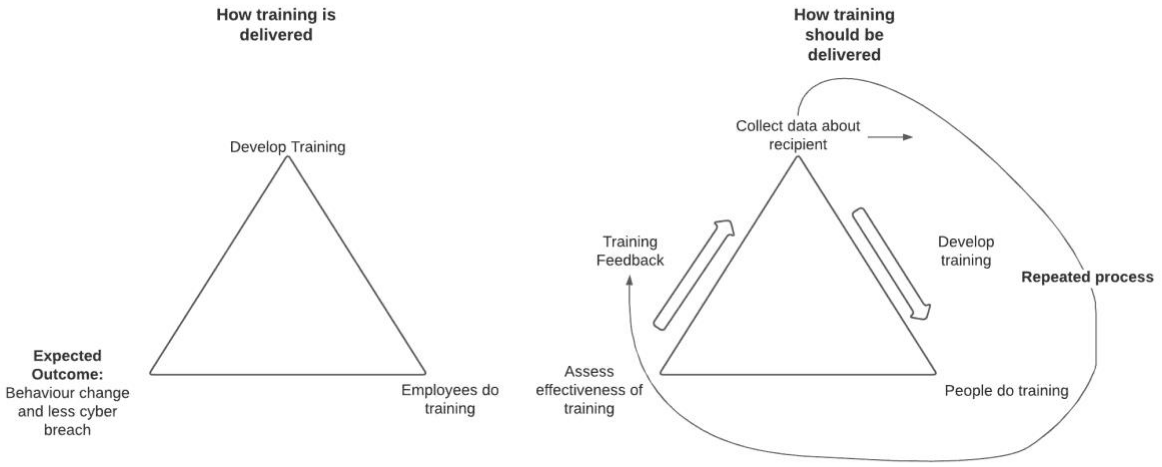

How training is delivered
Develop Training
Expected Outcome: Behaviour change and less cyber breach
Employees do training
How training should be delivered
Collect data about recipient
Training Feedback
Develop training
Repeated process
Assess effectiveness of training
People do training

Figure 17 Content Developer Training Development Process

6.6.3.1 How training is delivered

The first diagram represents the current state of how cyber training is delivered to businesses. It starts at the top of the triangle; content developers develop cyber training for businesses. This training is purchased by businesses in the hopes of training staff in preparedness of cyber breach. Their employees embark on training, whether it be an online course or video (Slusky, 2020). The final stage of training is the expected outcome, businesses expect instant behaviour change after training (Alshaikh, 2020). Traditionally, if employees are trained, and a breach happens, employees are the enemies (Mazzarolo, 2019).

6.6.3.2 How training should be delivered

The second diagram starts with collecting data about the learner. Knowles (1978) identified six characteristics of an adult learner, and one of them was that adults are self-autonomous and self-direct. He developed his point and suggested this ought to be acknowledged about adult learners. Specifically, they must get participants perspectives about what topics to cover and let them work on projects that reflect their interests. In doing so, the learners concerns, strengths and weaknesses are identified, and aims and objectives are aligned with employee needs (Beyer and Brummel, 2015). This in turn this can be addressed in the development and delivery of training. The next step is the learners undergoing the training they had input in. The training is assessed upon the established objectives and aims. The participants have opportunity to provide feedback about training, what they believe the training addressed and what they believe training failed to address. Training should not be seen as a one off, instead it should be a repeated process to ensure employee needs are met and training address cyber risks in businesses (Stefaniuk, 2020).

6.6.4 Beliefs about participants

The content developers discussed assumptions and perceptions they held about employees, some of these assumptions inform the selection of training materials and how training is delivered. For example, the developers believe training participants fear cyber security, and as a result they dismiss security. They acknowledge that human beings have a limited attention span, and if people are overwhelmed with incorrect information, it causes boredom and in turn disengagement (Bench and Lench, 2015). The developers assumed that the participants are motivated to adhere to security, when they have experienced a breach. They specifically discussed the differences in motivation and attitudes between different industries, such as the bank. For example, Haapamäki and Sihvonen (2019) discussed that firms in industries such as banks, business services, insurance, telecommunication, financial services, transportation and health care appear to be more proactive in providing voluntary disclosure of security-related activities (Gordon et al., 2006). In their responses they shared those industries that are not heavily regulated tend to have a lapse attitude, for example, they question why they need cyber security? Whereas, because banks are intrinsically secure, employees in the bank have no choice, but to be compliant because they are imposed to. This raises the question, what is the motivator for employees in banks, as opposed to employees working in a charity?

The developers acknowledge they presume knowledge about employees, however upon request, they also collect requirements from awareness professionals. One of the requirements in System Analysis Design (SAD) is to gather user requirements, these come from individuals who use the system. In this case the employee and awareness professionals (Wang et al., 2017). Although, this may be a productive methodology to gather user requirements, it shows there is a disconnect between what awareness professionals think employee's needs, and what employees need. Both content developers and awareness professionals assume what they think users should know, however neither group make any effort to investigate what user challenges or needs are. In the same vein, content developers develop training based on assumptions they think about employees, some of which they identify is not true. For example, they assumed that the younger training participants would like to do quizzes and games, for its competitive nature, but after some feedback it became apparent this was not true. The developers believe SMEs have a lower budget (Wong et al., 2018), so to maintain interest they give a reasonably cheap bill, otherwise this would detract SMEs from pursuing training. One of the ways content developers disperse knowledge across a business, is to raise training pioneers within the business to spread awareness to others in the business. However, Knowles (1978) highlights the importance andragogy; learning strategies that focus on the adult learner and how to engage them in their learning experiences. Akin to this, the literature suggests a good trainer must have a rapport; they must demonstrate good interpersonal skills when they interact with participants. Other characteristics include patience, flexibility, empathy, ability to nurture others, commitment to the job and the ability to be a team player (Trainer, n.d.). Given the importance of andragogy, it highlights the need for an encompassing trainer, however in the cyber security domain it raises the question, are these pioneers trained in adult learning?

6.7 Awareness Professional Results

Like content developers, the awareness professionals also had perceptions and beliefs they hold about employees that engage in training. In this section, the results from the interviews are presented. From this interview group, there was a total of 8 themes; Small business challenges, Business requirements, Beliefs about participants attitudes, Attitudes to cyber security, Training Selection, Problems with cyber content Culture and Motivation. These themes are presented in the corresponding theme map Figure 18Figure 18). Within the identified themes, subthemes can be identified in the *italic title text.*

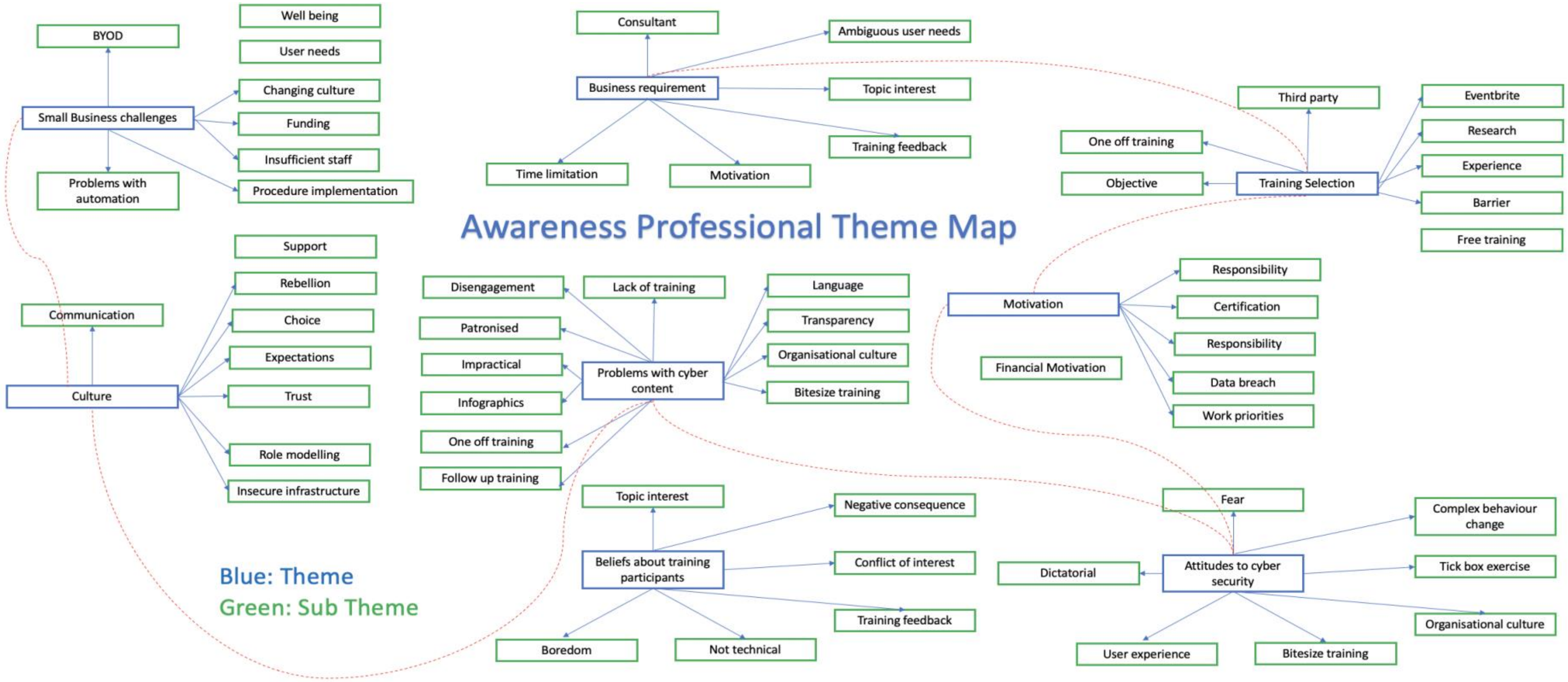


Figure 18 Awareness professional Theme Map

6.7.1 Small Business Challenges

The participants expressed challenges small businesses encounter when they seek for training, they pointed out finances and budgeting. On the other hand, some challenges are because of cultural problems within the workplace, and other challenges represented difficulty to change existing perceptions, so people see cyber security as their responsibility.

Subtheme of Small Business Challenges-Financial Challenges

The awareness professionals detailed some desire to seek for training, but some are hindered as a result of financial restrictions. For example, “I have a training budget that I could go off and do some learning myself. But the course that I wanted this year was too expensive” [P5]. The same participant expressed interest in training for senior staff, but the restrictions in budget means, there is little to no training expansion. For example, “there's a couple of senior sans courses that I'd like to do but they’re more than my annual budget” [P5].

Subtheme of Small Business Challenges-Behaviour Change Challenges

3 out of 8 content developers, identified challenges in changing employee behaviours. For example, they identified the challenge to change perception, to ensure people take responsibility. They said “That's the challenge, how do you make it so that people go yeah, we've got a responsibility. And I think if that was just drip, drip, drip, then the culture would be cybersecurity first” [P2].

Similarly, developers identify that training is not an automatic process, and in fact senior leadership have a responsibility to cascade the importance of security. For example, “Can't just like knee jerk change things all the time. So it's also taking that as a collective, and being able to use seniors as well to show why these topics are actually quite important” [P3].

6.7.2 Large Business vs SME’s

The participants highlighted that, big businesses have flexibility and larger budgets to select relevant and apt training for their business. For example, *“when you actually try and get cyber essentials, it can be hard for the small company to put in place the procedures that is required, compared to a bigger company that provide all of their machines and has more control”* [P2]. In light of, this comparison, one participant noted that small businesses have the liberty to discuss work related issues anytime, as opposed to rigidity. For example, they said *“I think the pros that we have is that, because we are small, we can chat about it, rather than it bring a huge memo flying around a large building that everyone has to look at”* [P6].

The participants noted that consultants and business coaches are available for marketing and business growth, however they note this is not regulated as a service in cyber security. For example, *"looking at the small to medium businesses. I think there are plenty of consultants and business coaches out there will tell you how to do sales, marketing, but they're not really offering to come in and be your cybersecurity consultant"* [P3]. They also discuss that small businesses have a limited flexibility in selecting bespoke training. They associated this with a limited skill set. Does this mean that small businesses have a lack of experienced Awareness professionals?For example, "*the smaller business that you are, the less likely you are to be able to make something bespoke because you just don't have the skill set"* [P7].

6.7.3 Bring Your Own Device (BYOD)

One of the challenges experienced, was the issue of BYOD. One particular participant identified this as a challenge, as they expressed implementation difficulty. For example, *"This challenged around personal devices as well. Because how much can we as a company insist on certain practices that can affect personal devices that then affect the company?"* [P2].

6.7.4 Business Requirements

The awareness professionals detailed what requirements to ensure training is successful and in turn a positive behaviour change is produced. They discuss some techniques they use to gather a sense of what their employees feel. For example, one participant said, *"So using this polling in a way will help give a sense to check what people feel and where they struggle. And when we do those, it's one every two weeks, two to three weeks"* [P1]. Another Awareness professional mentioned 'needs analysis' to gather requirements. For example, *"user needs analysis and training needs analysis is really important"* [P3].

One the business requirements identified was the need to have a consultant, to give guidance and recommendations. They said *"what would be great would be for a consultant to come in, look at our systems and say, this is great or actually, you need to improve here. And this is how you do it"* [P5]. One of the challenges they identified is around changing present operations to automated systems. For example, *"the only problem for us was we were always everything was always on paper. So it's been quite a challenge to try and change things from paper to computers* [P6].

6.7.5 User Needs

The results showed that the recipients of training, also have requirements, as well as the organisation as a whole.

They specifically noted that employees may not learn anything, if the awareness professional delivering the message is bothersome. For example, *"if I'm annoying people where they feel frustrated, they're not learning anything"* [P1]. The awareness professionals were asked why they think current cyber security training does not change behaviour, and one responded that *"it has to be fulfilling a need"* [P2]. On the contrary, they also identified that some employees may be oblivious to their own needs *"if I was to go to somebody and ask them, what they wanted to really sure, I'm not entirely sure they would be able to articulate it in a way that in the most helpful way"* [P1].

The awareness professionals note that the premise for successful training and behaviour change, is for people to have an initial interest. For example, "*some people love TED Talks. Some people love watching YouTube videos at length, like at night and learning something new. But in both of those cases, they are learning something they were already interested in"* [P3]. In addition to this, they recognise there are necessities that need to be considered for a successful training campaign. For example, training design. However, they also talk about the difficulties to convey training objectives that the recipients want to hear. They said *"if you're going to make a good speech, which is basically what strong training… you have to, design that with the reader or the listener in mind. Because it's not about the information that you want to convey is about information that they want to hear. And that is a very, very difficult thing to do"* [P3]. According to one participant, they gather user requirements based on key factors, such as what they need to know. For example, "*the requirements gathering process is based on what do we think they need to know? And how is it relevant to their job"* [P5].

Considering this, the awareness professionals note that employees feel acknowledged and heard when concerns are raised and addressed, it makes them receptive to training. They also discussed adopting webinars as a delivery mechanism, instead of PowerPoint presentation. For example, "*it feels like we're listening to them, it feels like we've actually thought about their needs. And it makes them more receptive to taking on the points that we raise with them, particularly when we're able to have conversations and do it in webinar format, rather than just throwing a PowerPoint or an e-learning"* [P5]. As well as delivery mechanisms, they discussed the way training clauses and questions are framed, and an onus is placed on its importance. For example, *“When you get a question, that's kind of like an A4 question. You're kind of bored after the second line. So I think that's really important as well, the way you know, the way the questions are presented”* [P6].

Continuing from user needs, one awareness professional discussed the outcomes of phishing simulation as a mode of training, and they highlight that people feel attacked and affects their well being. For example, *“so they will get a random email…so what that has done is created people to complain about it, they feel that they're getting got at, or it's not good for their, and so forth. So, the consideration for the user need is really important”* [P1]. On the other hand, one Awareness professional highlighted the frequency of training sessions, the company engages in. They described this was every six months, and it lasts approximately an hour. For example, *“then every six months or sometimes every year if we miss a session, we do a catch up for an hour with the entire team. We go through all the IT cybersecurity and GDPR make sure everybody will be up to speed”* [P3]. They also added that, this session is an opportunity to raise concerns or issue, however they note that employees fail to express any issues. For example, “*is an opportunity to stay late to have any questions, they never do”* [P3].

6.7.6 Belief about participant attitudes

This theme consolidates beliefs and assumptions awareness professionals simulate about employees that partake in training. They discuss topics like negative reinforcements and how these deter people away from engaging with cyber security, conflict of interest and mixed perceptions.

One Awareness professional discussed that people tend to remember negative consequences. For example, *“There is a chance that people remember negative consequences. So try not to engage it. They don't want to rock the boat, so they don't really want to engage because if they do, they might get it wrong type of attitude”* [P1]. This itself, could create fear, rather than motivation, people may feel fear because of the consequences, and this could cause people to avoid security altogether. This same participant went onto discuss that training participants may consume information from the organisation they work in, as well as from external sources. Depending on how the training content and delivery is structured, the participant can interpret different messages, and have a conflict of interest. For example, *“there is this built up perception of what it is, how they should act, perhaps whether it's useful, it's questionable. And then not only in an organisation, they also hear about one of these things externally and have messages externally, which may be in slight conflict or* *contradiction"* [P1]. One of the perceptions the awareness professionals highlight is the fact that training participants perceive themselves as non-technical. They discuss that this is rooted in the language. For example, *"people have this perception that they're not technical enough, because we build security with a language and a perception that it's technical"* [P1]. They add that, training participants fail to see past fraud, as the only crime and so have a mixed understanding of the subject matter. For example, *"the only thing people see about security is through fraud which is about scams and breaches. And so they have this really mie landscape of what it is and how they can take part"* [P1]. When the awareness professionals were asked why they thought training participants disengage from training, they discussed issues with the training content, for example language and length of text.

The awareness professionals mentioned that if the training message is not interesting, or the message is too complex, there is a likelihood this would cause disengagement. For example, *"If the message is not interesting or original to them, the message has been too complex or too filled with jargon. I think, if you don't make it, and if you don't make it understandable and relevant, they're going to leave it alone"* [P5]. This participant added that people generally do not understand cyber security, and the complex training doesn't aid the objective. For example, *"And I think the reason that it's challenging with Security Awareness and information security in general, is people don't understand it, we're not helping people. By making things reallycated"* [P5]. They highlighted that people would become disengaged if training content contains too many description, and this will often lead to boredom. For example *"I think also, if it's got too many words in it, people get bored"* [P6]. They also highlighted that initiating cyber security training induces negative attitudes from employees. For example, *"you need to do this training, it can automatically elicit an eye roll from people, depending on the culture of the organisation"* [P5].

In another light, another participant noted that the initial premise for a motivated training candidate, centres around initial genuine interest in the topic, coupled by placing a demand on training participants to complete training. For example, *"be availability time, interest in the subject, seeing how it's relevant to them, it would have for them to come along, it would have to be mandated"* [P5].

Subtheme of Beliefs about Participants attitudes-Fear

One of the beliefs about training participants, is that they generally have a fear of not being able to understanding cyber security. While, those that do understand it, can have a nonchalant attitude. For example, "I do think there's a fear of lack of knowledge, what you don't know... I think there's a fear of not being able to understand stuff. .And then on the flip side of that, those that are technological sometimes can have a cavalier attitude” [P2].

6.7.7 Attitudes to cyber security

This theme discusses the various attitudes the awareness professionals share towards Cyber Security Awareness and Training. There were mixed attitudes, some professionals had positive attitudes and discussed ways to engage staff and ensure security is mandated in the work place. On the other hand, other Awareness professionals demonstrated some lapse attitudes to the subject area.

One awareness professional showed positive attitudes towards security through employment selection. For example, one of the premises for employing staff is their attitudes to embracing new information, i.e. cyber security. However, if the candidate feels contrary to this, there is little opportunity for employment. For example, *"One of the things that as an innovative start-up, that we require of our team of individuals, and to me, is the ability to, to embrace new information and engage in active research, and lifelong, lifelong learning. And if someone isn't prepared to do that on cybersecurity, and it's necessary, then they're probably not a good fit for the company (P2].* The awareness professionals noted that most businesses weigh the probability of a cyber breach occurring, to inform their security decision. For example, *"it's very easy to look at Cyber security, as is there a probability of this, impacting us? And so we're going to begin loosely manage the risk and say it probably won't happen to us. I'm not saying that's an active decision, but I think that is that is reality"* [P2].

On the contrary, some of the awareness professionals, who did not represent positive attitudes, they described cyber security as being a tick box exercise to fulfil client's needs. For example, *"it's a tick box exercise, an exercise in satisfying regulators and client's want to know what our security posture is, rather than being an effective change at all"* [P5]. The same awareness professional, discussed that if they learn too much about the technology, then there will be a disconnect with the user experience. For example, *"But the reason that that serious techies are not great at awareness is because they know too much"* [P5].

Sub theme of Attitudes to cyber security-Complex behaviour change

This sub theme was derived from 'Attitudes to cyber security. One of the awareness professionals identified the complex nature of behaviour change and noted that behaviour change is not achieved through annual training. For example*, "you don't change behaviour with a one shot only, or you don't even change behaviour with an annual refresher" [P5].*

6.7.8 Organisational Culture

One of the key themes that transpired from the interviews, was ‘Workplace Culture’. The awareness professionals discussed everyday activities, thoughts and feelings they imbibe in within the workplace. The awareness professionals discuss a culture of embracing questions, if employees had any uncertainty. For example, *“If you don’t understand it just come and ask me, and if I don't understand it, we can sit down, work it out, and, find the best answer for it”* [P6]. They also described the level of free awareness information they receive within the community. For example, *“because of the community we were in, we kind of get sent quite a lot of information, around that kind of stuff. So it's easily shareable”* [P6]. The same participant also described an empathetic approach to how they see cyber security in the workplace, they mention that whatever security task an employee has to do, then they are more than willing to also commit to it. They said *“I'm not one of those sorts of managers, that is a manager and not one of the people.. Anything a member of staff can do, I can do”* [P6]. Another participant gave a similar stance, they described the liberty senior leaders have to admonish security messages, but it is less represented in reality. For example, *“it's really easy for a very senior leader to stand in front of the camera and say, This is really important. It's less easy for them to actually carry that through, and act upon it themselves”* [P5]. When this participant was asked about workplace challenges that affect behaviour towards cyber security, this participant highlighted the influence of culture within the workplace. They said *“I think that's because there's not a culture to show that it matters yet”* [P5]. In light of this, the awareness professionals highlight influence they personally have on employees, but everybody on a larger scale, through actions employees observe. They said *“If you're role modelling bad behaviour, it's not just the impact of you as an individual, it's everybody within your sphere of influence is therefore negatively impacted as well”* [P5]. When asked what procedures are in place, if an employee does not follow cyber security policies or training measures, one of the awareness professionals discussed that there is a HR process to go through, but ultimately the company is important than an uncompliant employee. For example, *“from a legislative point of view, we go through normal HR procedures, but from an operational point of view and security point of view, the company is more important than an individual who can't take on their training”* [P2]. This shows an angle of Organisational culture.

Sub theme of Organisational Culture-Personal Choice

The results also showed there is an expectation from awareness professionals to employees, that they should express concerns or requests they may have for training. The expectation is that when employees find this training, they ought to gauge the benefits of the training and partake if they see benefits in doing so. For example, *"I would expect the team individuals to come to me and say, I really need this training, because we need to do this as a company. Or if its free training, for them to judge their time, and the importance and value of that training, and then just get on with it"* [P6].

They add that, training should be a liberal activity and people should not be forced to do training. For example, *"So have one of them come to me and say, we need cybersecurity training, and here's the free training. And that would have been how that worked. I think if you're starting to force people to do something and say they have no choice at all, I think they're going to go against it. You know, it should all be about choice"* [P4]. This shows there is belief that training is not necessary, and it is seen an activity the employees desires to learn, rather than training employees should know to a secure member of staff. It also shows, the expectation that training should be free, rather than an outsourced service they need to be a secure company.

Another representation of workplace culture through personal choice, is discussed by the awareness professionals, as they highlight that implementing a dictatorial scheme would prove challenging. For example, they said *"it's very hard for a company to operate in what I would call quite a sort of dictatorial, Central, enforced way on what essentially a private device"* [P2]. The participants also highlighted disparities between different industries, such as the bank. They explain how banks are intrinsically secure by nature, and therefore there is an existing nature of secure culture, as opposed to other industries. For example, they said *"Because you have be secured as a bank, it's part of the DNA. If you're an estate agent. You don't have that same sort of imperative around it. If you're an estate agent, you don't think about information security, it's not the same thing. If you're freaked out about banks, you have a very real risk of losing actual cash, or digital. So it's easier to that culture is already aligned for it"* [P5].

Sub theme of Organisational Culture-Support and encourage use of cyber security

The awareness professionals detail ways they support and encourage their staff and in turn implore a cyber security culture in the workplace.

One of the ways they encourage a security culture is by providing a video to answer inquiries, every quarter. For example, “we'll provide either a video or some answer to their questions, or create two, we do it in quarters. So next quarter, we'll answer some of those questions” [P1]. Another awareness professional, adopts the use of videos to encourage staff to be security compliant. They instead, use senior members of staff to create security campaigns, however they note it is not always positively received. For example, “the CEO, the chief risk officer, the senior board members, they've all been very happy to stand on video and put out messages for me saying, yay, the layer that actually manages all the different projects, not quite as engaged, and therefore it doesn't necessarily play through to being done in various different spaces” [P5].

Another strategy used, is to instil security in people of influence across franchises to influence other members of staff. They do this, because of the ratio of awareness professionals outweigh, that of staff. For example, “we do have a culture group and such policy where they will go out and because there is different franchise, the X is huge, 76,000 people, so I can't affect everybody. So, we use the people who have influence in those areas and we have a monthly meeting about what we're doing to keep them updated” [P1]. However, how many of these people are qualified

The awareness professionals described how cyber security information is passed across the business. Due to the limited awareness professionals in their organisation, information channels are also limited. For example, “And like I said, because you've only got, like me and two other paid members of staff that is so easy to pass that information on” [P6]. In addition to this, they find ways to inform staff and keep them up to date, by printing training materials and asking training feedback. They said “I've got a X worker, for example, I'll find things and print them off for her… I support her, probably more, and ask her kind of how she found it” [P6].

The awareness professionals also highlight the importance of language, they recognise that if language is not properly assessed and appropriately used, then it has a way of influencing what people do with that information and the consequential behaviour thereafter. This highlights how language can culturally inform people’s behaviour. For example, “So one of the things I think is really important is the making sure that people in security realise the effect of the words that they use, and how it influences what other people actually do, and the behaviour that it then create" [P1].

As well as the language used across the workplace, awareness professionals note the importance of treatment towards training participants. They note that if employees are treated as children there is a likelihood that will introduce barriers and challenges. For example, "When you start treating your employees like children, then they start getting quite defensive, like, Oh, we don't need to do this. We know what we're doing… but if you if you treat them like adults, then they will normally react by adults, generally speaking. That's not exclusively true" [P3].

Subtheme of Organisational Culture-Trust

One of the cultures within the workplace is trust. The participants discussed that people are over-trusting, however the cyber security world teaches people the contrary i.e. be defensive and untrusting. For example, "People are too trusting… But how bad is that in society that you have to assume that everybody around you is evil? It drives me nuts. But in the cyber security world, you have to teach people and train people to act like unsuitable people, which is just inevitable" [P3]. As well as trusting within the workplace, another awareness professional discussed that people should trust their own individual instincts. This also represents a culture of trusting individual instinct within the workplace. They said "encouraging people to trust their own instincts, which is where the self efficacy theory comes in. You got to encourage people to trust their judgement, then they will trust their judgement" [P5].

6.7.9 Training Selection

This theme represents the process and approach Awareness professionals typically take when they search for training.

Subtheme of Training selection-Research

One participant discussed their outlook to select training, it involves multiple options such as Industry standards and Academia. For example, "I tend to take a lead from sort of commercial research, so I'll tend to use something like the DVIR…my leadership tends to rely on things like Gartner and Harvard Business Review and those kinds of things rather than academic research" [P5]. Similar to this outlook, another participant highlighted research they embark to keep informed about cyber threats. For example, "I keep myself updated with what's going on SANs, the register and ZDNet, see what threats are coming through" [P3]. Another participant said, their sole source for training selection is through research. They associate this to their background and to previous work experience. For example, "it's mainly based off research and that's mainly because of my background, and where I come from, and what I've done previously" [P1].

Subtheme of Training Selection-Open source

On the other hand, some other participants received training material, as opposed to searched or enquired about it. One of the participants gave an account of the information they received from an open network group, who sent training material during the global lockdown. For example, "I think Eventbrite, send us lots of things. We're, community action network, they send lots of information, especially around COVID stuff, changing guidelines" [P6]. They also said they gather information from trusted sites, and training content from companies they have previously worked with. For example, "from recognised sites, normally it's people we've done things with before. So it's just them sending us, updates and things" [P6]. They also said cyber material is given to them, as opposed to looking for it. They said "So, you end up hearing about things rather than having to search for them, so it falls in my lap, rather than me having to sit there and think, okay, you know, what do we do next?" [P6].

Subtheme of Training Selection-Shop bought training

This theme was derived from 'Training selection', and it presents the thoughts and perceptions awareness professionals have about shop bought or 'off the shelf' training. The general narrative from the results shows that, businesses tend to purchase off the shelf training. One participant discussed issues with shop-bought training and stated that it was financially laborious and the reality of what you buy differentiates to the advertised product. This participant said "I have never been a fan of off the shelf products, I find they are overpriced. There's too much marketing hype behind them, and what you actually buy is not what you bought" [P3]. They went onto say that although, it may serve as a tick-box exercise to certify accreditation, it does not inform new learning, nor is relevant to the clients business or user needs. For example, "let's say I bought the US it was like Norton cyber security training package for £250. But if I take people through that package, at the end, I can say they have all completed the Norton cyber security package 2021. And that's a nice little box ticking exercise. However, when I'm doing that training, 90% of what I'm teaching people I know is completely irrelevant and ridiculous" [P3]. They also spoke about these trainings being for free. For example, "so a lot of the courses and stuff we do, we're looking for free, quite often they're not paid for" [P6].

Subtheme of Training Selection-Disengagement

The awareness professionals also discussed that shop bought training causes disengagement. They note there are human limitations as to how much information can be retained. They question how participants, trained using unengaging materials, could possibly retain important security information. For example, "I have seen a couple of these off the shelf products, these online training videos. I struggled to stay awake watching some of these online training videos and there's my job" [P3]. Another participant mentioned that encouraging engagement for unmandated training is challenging. For example: "Getting people to engage with something that isn't mandatory is quite difficult" [P5].

Subtheme of Training Selection-Training Frequency

This sub theme was derived from Training selection, and it represents the rate in which training occurs in participant work environment. The awareness professionals said training generally occurred once a year. For example, "For cybersecurity realistically, it would be one off" [P5]. Another participant discussed the impact of the global lockdown and how it changed the training frequency. They said "It's six monthly sometimes but during the pandemic, it became an annual thing" [P3]. Another participant follows that industry says, which is a minimum of twice a year. They also signpost security messages to remind people of security habits. For example, "So I think some best practices recommend like twice a year minimum of twice a year. I think ISO27001. The simple reason is because you need to refresh people that we advise people as well to do like a monthly email blast or to have like stickers in the office… that reminds people of security habits" [P4]. Another participant mentioned their in-house training is mandated at the start of employment, usually within a month of recruitment. For example, "there's a one time in house-built course that you take when you join the company in the first 30 days" [P5].This participant also said, "So actual training is once a year. But we send out communications, reminding people about behaviours every week, and we do a quarterly newsletter, where everything all of those comes together and talk about headline topics" [P5].They also mentioned that training should not be seen as a one off, they said "instead of just seeing security as like a one off. I do it induction for every member of staff who joins the company" [P3].

Subtheme of Training Selection-Training Evaluation

The awareness professionals were asked about what training evaluation methods they have in place, to measure training objectives and successes. The general consensus, from the results showed that participating businesses have little to no methods of evaluating training. One Awareness professional discussed that they did not have any training evaluation process in place. The only measures they can view, are the number of people engaging and viewing their social posts and videos after presentations. For example, "Currently not. We're having a proof of concept, through an innovation project to do that more systematically… all we can really see is engagement with people sharing our posts, or viewing our videos or... But we don't measure that in any systematic way" [P1].

Another participant said their only measure is knowing who completed the training. They are unable to identify duration on each question. For example, "So for example, with the mandatory training, all I have is did they complete it? I don't know how long they spent on each question. I don't know whether they completed it in five minutes or half an hour. I don't have that kind of data" [P5]. The participants also mentioned there are limited ways to measure training objectives, because they are third party vendors. For example, "we do not have a way to measure ourselves because we are third party" [P4]. One participant said they would seek for training evaluation, if an employee returned back from training, feeling like they did not learn a lot of content. This also reflects attitudes to training evaluation i.e. it is only necessary of when training participants feel training was informative. For example, "I think if it was a webinar that went on for a couple of hours, and the support worker come away feeling that they hadn't really learned anything. I think I'd probably actually, contact the providers of it, do they do any feedback on their, evaluation on their courses or anything?" [P6]. The same participant also discussed that persuading participants who found training unbeneficial to complete training evaluation forms, can prove difficult, leaving people questioning what the purpose of training is even for. For example, “it's kind of quite hard, and I think to tell my staff who found it, bad that training evaluation forms pretty good, but I can't say boring… it's kind of like, what was that even about? What was the aim of it?” [P6].

A different process to other participants was a participant who described training success by assessing phishing simulations; identify employees who click on phishing emails. For example, “The only thing we can measure is through fishing is, that's a bit more obvious, because we can see the types of emails that they click on what they're more likely to click” [P1]. The same participant mentioned that their training platform offers trigger questions, which they define as refresher tests. For example, “we have a feature called refresher tests, and the refresher tests, basically, trigger knowledge check questions after a certain amount of time” [P1]. They mentioned that these refresher tests come after six weeks of training, and they focus on what the training participant remembered. For example, “someone might do some training. And then six weeks later, they might get a refresher test, which says, that training you do, can you still remember these things” [P1].

6.7.10 Training Feedback

Some of the participants discussed the challenges they experienced with gathering user feedback. They expressed that it was generally a difficult task because they had not experienced a breach, for example, “*That's a very, very difficult thing to measure. Because we've never had a breach to date”* [P3]. It was also noted there is a limited capacity to accomplish evaluation in their business. For example, *“I tried to, and the capacity for doing so given the technology I have in place is quite limited”* [P5]. This shows a lapsed attitude towards receiving employee feedback, it could be seen that employee feedback is only relevant if there is a breach.

6.7.11 Motivation

The awareness professionals were asked what motivates them to look for security training adhere to security policies, even after training. They were asked what are the driving factors that motivate and external motivations, i.e. factors that directly impact them as an individual or business or factors that affect clientele relationships for instance.They speak about attending training and attaining accreditations, because they’re free, and their job responsibility as drivers is to seek training. They mentioned that as a s a small business finance can be difficult and so they feel inclined to advocate for free training. For example, *"for a small company, if it's free, we probably push the door. And cyber essentials was funded, which was great"* [P2].

They highlighted external factors that implore them to search for cyber security training and adopt policies in the workplace. They described various business relationships that involve data handling; however, this is not necessarily transpired when handling personal data. For example, *"we have to go through with local authorities, we work with FDA through GDPR, and data impact, data protection, impact assessment. So, it made absolute sense for us to be on the curve ahead of cybersecurity, even though we're not, we're not particularly providing security for personal data"* [P2]. The same participant describes what seems like a haphazard countermeasure, they take the cyber security route when they deal with external parties, but also recognise the risk they pose to themselves by not adhering or implementing security in their business. For example, *"But we also recognise that if we get hit by us by a cyber-attack, and we're not doing what we need to be doing, then that could be the end of the business"* [P2]. In addition to this, the participants highlight the importance of obtaining certifications, to show the community they are cyber accredited. This shows the weight of external influence on businesses, how it changes their disposition towards cyber security. For example, *"I think for a community organisation, it's really good if you do have certificates, from other places saying, you are aware of cybersecurity"* [P6].

As part of external motivation, the awareness professionals perceived cyber security accreditation as a source of support to their customers, and a way to show sustainability. The results somewhat showed that some awareness professionals view cyber security training or accreditation as business empowerment to show clients they are cyber secure, rather than actual training objectives. For example, *"cyber security often something that we would look at in terms of operational support to customers, and how we make sure that we, stay on a sustainable track"* [P2]. On the other hand, one of the participants discussed an internal factor that appeals to them to adhere to security, which is their job responsibility. For example*, "I have a responsibility to the company and the staff to be up to speed on all these things. Because how can I make decisions otherwise?"* [P6].

One of the participants discussed that IT is imposed on people and there are expectations for people to simply use and adhere to security policies, but they note there are other priorities employees have on the job. For example, *"IT support is the most worked job, I worked within the NHS, it was very apparent to me how technology was imposed on people.*

And that it was expected that it could just be used" [P1]. They discussed the varsity in people's jobs, and they highlighted that different sector demand a range of attributes from employees, for example, what is being demanded of in the IT sector is different to the NHS, and therefore people have different motivations. For example, *"But it isn't like they don't have other things going on people, especially in the NHS are trying to save somebody else's life. They're not thinking about their authentication journey, or how they log in, or their passwords, because they are literally trying to save somebody else's life"* [P1].

Subtheme of Motivation-Financial motivation

The participants also spoke about financial motivation, they discussed that financial limitations impact the level of outsourced security they can achieve. Typically, they would negate certifications because it comes at a price. They said "I would say that certification comes at a price, and it just wouldn't be on our lead unless there was an outcome that we needed" [P1]. However, if the certification would enhance a greater customer base, then they would obtain it. For example, "if, the only way to get our local authority to buy our product was to have cyber essentials plus also potentials. And the only way to get those things was to pay £1000, then because it will have to be certified, then we would do it" [P1].

6.7.12 Problems with Cyber Security Training Content

The awareness professionals gave several accounts of the problems they experience with security training. They discussed issues with the design of training, highlighted content issues and, presented what they believed training should look like. One of the participants who buy 'off-shelf' training mentioned the awareness package they use, does not fulfil its description. For example, *"NCSC puts out, lots of guidance. And they do things in a way they classed as an infographic. But it isn't really an infographic. It's, it looks like too much information on a page"* [P2]. This participant also said training, was more than regurgitating information from a PowerPoint presentation, they described that awareness professionals need to adopt a level of honesty and transparency, to encourage people to speak about the subject area. They said, *"it's not just reading from a PowerPoint, there's a level of being open and transparent yourself and honesty that makes a lot of people feel comfortable to have that conversation"* [P2].

On the flip side, the awareness professionals discuss challenges they experience when they deliver training. They mentioned factors that training participants may not acknowledge when they deliver training, such as listening and reflecting on what participants are saying while delivering a topic that makes them feel uncomfortable. For example, "*I think* *that one of the things that is forgotten is the ability to listen and reflect, it's actually quite hard. And that ability to listen, reflect, and facilitate in the moment while keeping the conversation going when people are feeling uncomfortable"* [P3].

The awareness professionals provide their view of how they believe training should look like. Some of which are based on comparative experiences between different training packages. One of the participants spoke about training following a simple approach but should rely on training participants knowledge. For example, *"it has to be really, simple message. And it relies on an innate knowledge of the subject matter"* [P5]. The participant added that training needs to be practical, for example, instructing people to do things that hinders fulfilling a task would negate secure behaviour, as opposed to encourage it. They said *"It has to be workable. So you can't just say, don't click on links, they might be malicious. That's a crappy message because everyone has to click on links every day in their emails as part of their daily job. So it's not an actionable message. So it will encourage people to disengage if they can't actually act on what you say"* [P4].

In terms of training content, the Awareness professionals highlighted information overload within the training they had experienced in the past. For example, *"But it's always been intriguing to me actually, how much of that is really read? That people take away from it, because there's just so much information all at once, that it's hard to break down"* [P1]. This same participant associates the financial limitations small businesses experience, to limited options in seeking professional cyber support. For example, *and it's actually quite difficult for people to find their roots through because people who own small businesses won't have a security expert"* [P1]. Continuing from information overload, the Awareness professionals gave their experience when they completed the same training the employees did. They questioned how much information was retained, they questioned whether or not they applied adequate time for optimum learning and concluded by saying the training did not change their overall business practice. For example, *"did the training recently. It was okay, I'm not sure how much I learned from it to be honest. But then, time is limited. So did I invest the right amount of my time into it? I'm not entirely sure how much I learned from it, to be honest. And I don't think it's actually changed our practice very much"* [P2].

The awareness professionals identify another challenge; it is the fear appeal content developers use in the design of training. They claim that most cyber training vendors, take a fear appeal approach. For example, *"it's very easy to, just scare people into submission and that's generally the approach that a lot of vendors take is"* [P5]. They add that, cyber professionals should take a step back when designing training, on the contrary they feel IT technicians are unable of doing this. For example, *“You have to be able to pull back far enough. And I think sometimes it's hard for fully fledged technicians to do that* [P3]. Having said that, they suggest cyber security training should involve people who are not fully cognizant of security risks, so professionals can remember what it feels like to be a recipient of training. For example, *“I think there's something to be said, for involving people in security awareness as a discipline, who are not necessarily deeply technical for that reason, so that you can remember what it's like to not be an expert”* [P5].

Subtheme of Problems with Cyber Security Training Content (Follow up training)

The consensus from the results represented a ‘one-off’ training culture. The awareness professionals were asked if they do follow-up training, and they typically did not, unless their customers were affected. This shows the relationship between advocating training and external motivation, for instance, awareness professionals seek training when it’s in the interest of their customers, or if the awareness professional’s business can benefit from it. For example, “We don't at the moment tend to follow up, the only time we would follow up on training and engagement would be if it was an area that directly affected our customers” [P2].

6.8 Chapter Summary

This chapter identifies the methodology for participant recruitment in study 2. It discusses analysis methods and highlights the strength of the chosen methodology. Pursuant to this, the results from study 2 are presented, focusing on the highlighted themes. The results presented methods content developers typically take when designing training for businesses, assumptions and perceptions they have about employees and a theme map to demonstrate the key themes from the results. The next part presents results from awareness professionals and employees, following a corresponding theme map for each group. The last part of the chapter is a discussion pertaining to each research group

Chapter 7 Training Selection Study 2 Interview Discussion

7.1 Discussion of Results from Awareness professional

7.1.1 Small business challenges

The results showed that small businesses are unable to find training of their choice, because of financial limitations. The literature confirms this, as 73% of large businesses have had cyber security training, in comparison 37% of SMEs (Statista, 2021). The results show that some awareness professionals have a desire to do external training to increase knowledge, it shows admiration to increase skills and insight into cyber security. In this chapter the subthemes can be identified in the *italic title text,* this is to highlight that it is a subtheme and not a theme.

7.1.2 Training Evaluation

Training evaluation is a measurement technique that examines the extent to which training programs meet the goals intended. The evaluation measured used depends on the goals and includes evaluation of training content and design, changes in learners, and organisational payoffs. The awareness professionals were asked what training evaluation method they use to measure program goals. The narrative showed that they did not have evaluation techniques. On the contrary, one awareness professional had a proof of concept for mandatory training, they could only see whether or not employees had completed training. On one occasion, they discussed they would contact the training administrators for training evaluation if an employee felt the training was not beneficial. This reflects a lapse attitude some awareness professionals have towards cyber security as a whole and then employees and Cyber security. For example, they take it as a matter of urgency only when there is a compliant, but in general, there is no sense of urgency to measure training success. As there is no way to measure training goals or success, this could discount the purpose of training in itself and therefore become arbitrary. They added that these employees, who find training boring or hard, also feel reluctant to complete training feedback forms.

7.1.3 Training Needs

The literature discussed that employees need to be ready, they define learner readiness as “the extent to which individuals are prepared to enter and participant in training” Holton et al (2007, p.276). A study that measured learner readiness in terms of retention and motivation to retrieve and apply such knowledge, found that learning transfer is at a higher level when trainees are confident to retain the knowledge. In the results, the awareness professionals point out that employees who have a positive attitude and willingness to learn, generally have an initial interest in the subject. This suggests that a component of motivation is genuine interest. Could this suggest that one of ways to motivate employees to learn cyber security is to have a genuine interest. This leads to the question, where does a genuine interest come from?

The results showed that employees may not learn anything tangible if the awareness professional delivering the message is bothersome, e.g., irritating (Reeves and Delfabbro, 2021). Gates (2000) found that an appropriate use of emotional expression and suppression was believed by teachers to be an important tool to facilitate student learning (e.g. showing enthusiasm as a tool to enhance student motivation for a subject area: masking disappointment in order to show faith in students) .This may contribute to how employees perceive and engage with cyber security training, they may either be irritated by the training delivery or feel encouraged through emotional expression from the training facilitator. Another need they identified is that cyber security training should be designed with the user in mind, they add that training information should convey information users want to hear. For example, Walker and Kramer (2004) discussed that awareness professionals need to know enough information about the end users, before conveying training information. This idea supports Knowles (1987) principles for adult learning, he proposes that adults should be involved in establishing learning objectives. The adult's input does not have to be the sole, determinative or final basis for defining objectives, but he notes it is vital for them to have input into training objectives. As well as defining learning objectives, one of the cardinal principles of andragogy is mutual planning. This is where the learner is involved in planning what the learning will cover. However, when the awareness professionals were asked how they define employee needs, they shared that they generally did not check employees training needs. They shared the fact that objectives are not defined at the beginning of training, and they do not speak to employees to identify what they want to see in training. Instead, awareness professionals choose training based on what they think employees need to know. Selecting training that does not address employee challenges, may be seen as arbitrary, and this in itself could disengage employees (Hultman, 2020).

One awareness professional confirms Knowles (1987) principles of adult learning, he states that when learners are involved in the conversations about training delivery, they are more receptive. The results support this principle, as awareness professionals found that when they involved employees in conversations about training delivery. For example, employees discussed that training should be delivered in a webinar form instead of PowerPoint presentations. The awareness professionals described the positive reception and engagement employees have with training and they also said employees were more receptive to taking training points. On the contrary, awareness professionals gave accounts where they have not involved employees in training planning, and instead, training has had adverse effects. For example, one business implemented a phishing simulation as a mode of training, so this meant the manager would simulate phishing emails from the training package and employees would have to decipher whether they were legitimate emails or indeed a phishing email. However, the awareness professionals found that employees feel attacked, and it affected their well-being.

7.1.4 Beliefs about participant attitudes

The awareness professionals had perceptions and beliefs they held about employees, when it comes to cyber security. They perceived those employees believe cyber security is for technical people, for example, only technical people can understand cyber security terminology. In addition to this, they add that employees receive information from multiple sources, and this can cause a conflict of understanding of cyber security. For example, whenever the topic of cyber security is raised people automatically associate it with fraud and financial scam, but they do not acknowledge cyber security on a wider scale. They were asked their opinions as to why they felt employees disengage from training, and they discussed issues with training content, for example choice of language and length of text. A common theme from the results are issues with training contents, most especially the choice of language. They described that if a training message is not interesting, or the message is too complex or filled with jargon, it will cause disengagement and people will get bored and tend to leave it. They added that people generally do not understand cyber security, and complex training doesn’t aid learning (Renaud and Weir, 2016). The results are supported by Knowles (1978) who discussed that learning ought to be connected to people's life experience, by drawing out participants experience and knowledge which is relevant to the topic. The awareness professionals believe that employees want to be treated as adults and if they are treated so, they generally will react as adults, but when treated as children, employees will get defensive. This highlights the importance of understanding adult learning, and what it entails to deliver training to adults.

7.1.5 Organisational Culture

The awareness professionals discussed the cyber security culture within their business, some of which represented positive culture, and others contrary. They acknowledged that it is easy for senior staff to orchestrate cyber security, but it is difficult for them to follow through. This shows there are disparities between what is expected is employees and what senior staff do. Could it be that employees see this disparity, and choose to negate security as a result?

In other organisations there is a culture of 'personal choice', that is, training should be a personal choice, it should not be enforced on people. The expectation is that when employees find training suitable to them, they should identify training benefits and decide if they want to participants. But awareness professionals also argue that when employees have been asked to share concerns about cyber security, they never do. This seems somewhat contradictory because, if there is an expectation for employees to raise concern, it no longer makes it a personal choice whether or not they want to learn. This shows there is a belief that training is not necessary and is seen as an activity employees desire to learn, rather than training employees to be equipped to do the job.

One of the ways awareness professionals solidify cyber security into their organisation culture, is through managerial support. Managerial support has been identified as a key environmental variable affecting transfer (Ford et al., 1992). Some businesses were intentional with the level of support they offer employees, for example, they use senior members of staff to create campaigns. Another strategy is to instil security into influential people across the business, who would cascade this to others in the business. While this may seem beneficial to businesses, the method questions the authenticity of the security message, it questions the motivation the appointed people have to 'train' or 'influence' others. Eraut et al. (2001) established that people learn both positive and negative models, so if any reason, the appointed 'trainers' are not motivated to 'train' people and they happen to have negative perceptions about security, the negative attitudes could also be a source of learning for employees.

A subtheme that was developed from Organisational Culture, is trust. Trust was a prominent factor that represent how most businesses operate. They argue that society is taught to trust, but cyber security preaches the opposite. In addition, they add that people should trust their instincts, they influence self-efficacy, so people trust their own judgement.

7.1.6 Training Selection

The awareness professionals discussed the process in which they go about selecting training for their business. The typical procedure either entailed free training being sent from open sources or awareness professionals purchasing shop bought training. The businesses who purchased shop bought training was often because it was a tick box exercise to assist in accumulating accreditation. This represents some of the attitudes they feel towards cyber security, for example, it is seen as a catalyst to achieve a certificate for business expansion, and not for genuine awareness or training.

Knowles (1978) established principles for adult learning, which incorporates employees in defining objectives. However, if businesses are purchasing shop bought training, that suggests employees are not involved in defining training objectives. This proves problematic for employee learning, because shop bought training was developed for another business, and it does not directly address their needs. This may cause disengagement because training is not tailored to business needs, nor does it address employee needs. One awareness professional partook of the shop bought training and mentioned the difficulty to remain focused. This drives several questions, for example, why is there an expectation for employees to learn cyber security, when managers struggle to optimally pay attention to same training?

A different perspective was observed by awareness professionals who discussed that disengagement comes from training not being unmandated. They argued that if training is unmandated there is a tendency for people to be disengaged. However, the literature says otherwise, Reeve et al. (2003) gave undergraduates ‘action choices’, how to allocate their time or ‘option choices’ for example which puzzle to solve. Their study found that, action choices have a stronger impact on the sense of psychological freedom and volition and this in turn places a role in employees’ intrinsic motivation. Patall et al. (2021) contributed to this point and argued before choice can be expected to translate into autonomy satisfaction, it needs to be accompanied by additional autonomy supportive acts of instruction, for instance take employee’s perspective. This shows that awareness professionals have some expectations and beliefs about employees, that are unsupported by the literature, some of which are discussed in 7.4.6.

A subtheme that was developed from Training selection is 'Training frequency'. Training often occurred once a year in businesses which was is typically when people are employed, some twice a year and others had training as of when a breach occurred. Some businesses often training twice a year, but were affected due to the global lockdown, and reduced training to once a year. Psychologists have highlighted those human beings have both short term and long-term memory (Zlornik, 2019). Short term memory can only hold limited information for a limited time, and since training happens at such a low frequency it means little to no information is retained over time, and training gradually becomes a historic event.

Subtheme of Training Selection-Training Evaluation

The consensus is that awareness professionals have little to no methods to evaluate training. Generally, they can access data about who completed training, but there are no indications as to what topics employees were disinterested in or what topics appealed to them. There was a lapse attitude to evaluating training success, for example, the participants said they would go back to the training vendor if employees felt they had not learned anything. Although, they make the effort to contact the vendor if questions come from employees, the sequence of actions seem haphazard. It shows that Awareness professionals, only care about employee learning if the employees actively voice out their thoughts. However, the results show not all businesses share an open space culture, where they can conveniently share thoughts and challenges about cyber security. This may limit employees who may not feel comfortable enough to voice opinions in their work environment. Clardy (2005) argued that employees should evaluate how well their learning outcomes were met, the adequacy of their learning as well as their progress with the material. This shows that expecting employees to share training evaluation without providing the opportunity to, can be seen unpractical and unsuitable.

7.1.7 Motivation

There are two types of motivation the awareness professional depict. They were asked what motivates them to search for training, they generally said it was because of internal and external factors. They were externally motivated because they handle customer data and are concerned what their reputation would become if there was a breach. However, some are aware of the risks they post to their business by having a haphazard approach. On the other hand, some are internally motivated because cyber security is inherent to their jobs, for example, they are responsible for cyber security. In both scenarios, awareness professionals have a tangible motivation, it either boosts business recognition in society or maintains or upholds perceptions of their business.

In addition to this, they discussed financial motivation, and the results showed that businesses are generally motivated to outsource security if there is budget available for this and if it directly benefited their business. But they would typically negate certifications that would boost business credibility if it came as a price. This shows businesses who may have a genuine interest to achieve cyber security accreditations may be a deficit because they cannot afford it.

7.1.8 Problems with Cyber Security Training Content

The awareness professionals discussed that shop bought training, does not fulfil its description. The training content is impractical and become disengaging, for example, content that instruct people not to click links just because they are malicious. They argue this is impractical because clicking links are integral to their job. In addition to this, the results showed that small businesses are financially burdened, so there is no luxury of having a security expert, and therefore they resort to shop bought training. There were comparisons between the financial freedom and flexibility in large businesses and small businesses. Awareness professionals expressed that small businesses are financially restrained, and often at times, the manager covers multifaceted roles including training cyber security because they do not have funds to invite a cyber security expert to conduct training, whereas larger businesses can invite a security expert to assist a business' risk posture. Allen et al. (2015) supports this, as they found large businesses typically employ a chief security officer who has formal training as an information security analyst to address legal and compliance issues.

7.1.9 Training investment

The role of the transfer of knowledge has been widely recognised in Professional Development (PD) where practitioners consistently conclude that the return on many training investments is low. Also, organisational investments in training are too often wasted but also due to a lack of understanding trainee's characteristics at the pre-training stage (Chang & Chiang, 2013). Overall, in the cyber security context 1 in 9 businesses (11%) have provided cyber security training to non-cyber employees in the last year. These training sessions are not always focused exclusively on cyber security, and they often incorporate other aspects like the General Data Protection Regulations (GDPR). The training is typically mandatory, but in 3 in 10 cases (30%) in the private sector, it is not (Pedley et al., 2020). Although there is a basic level of knowledge in training, there is a lack of cyber security PD that could contribute to the desired behaviour towards cyber security. This wider staff training is more likely to be internally developed than externally developed. Only in half of the cases (48%) businesses are provided with training delivered by external organisations. Whereas training designed for management boards is relatively rare, accounting for just 39 percent of the cases where businesses are providing cyber security training to any non-specialist staff. This equates to just 4 percent of all businesses.

7.2 Thematic analysis of Employee Interviews

The employees that receive training within organisations, were interviewed to identify their perceptions and attitudes towards security, they were asked where their influence and motivation comes from, they were asked what levels of support is available in their business and their expectations from cyber security training. Themes deduced from the study are presented in a theme map Figure 19.

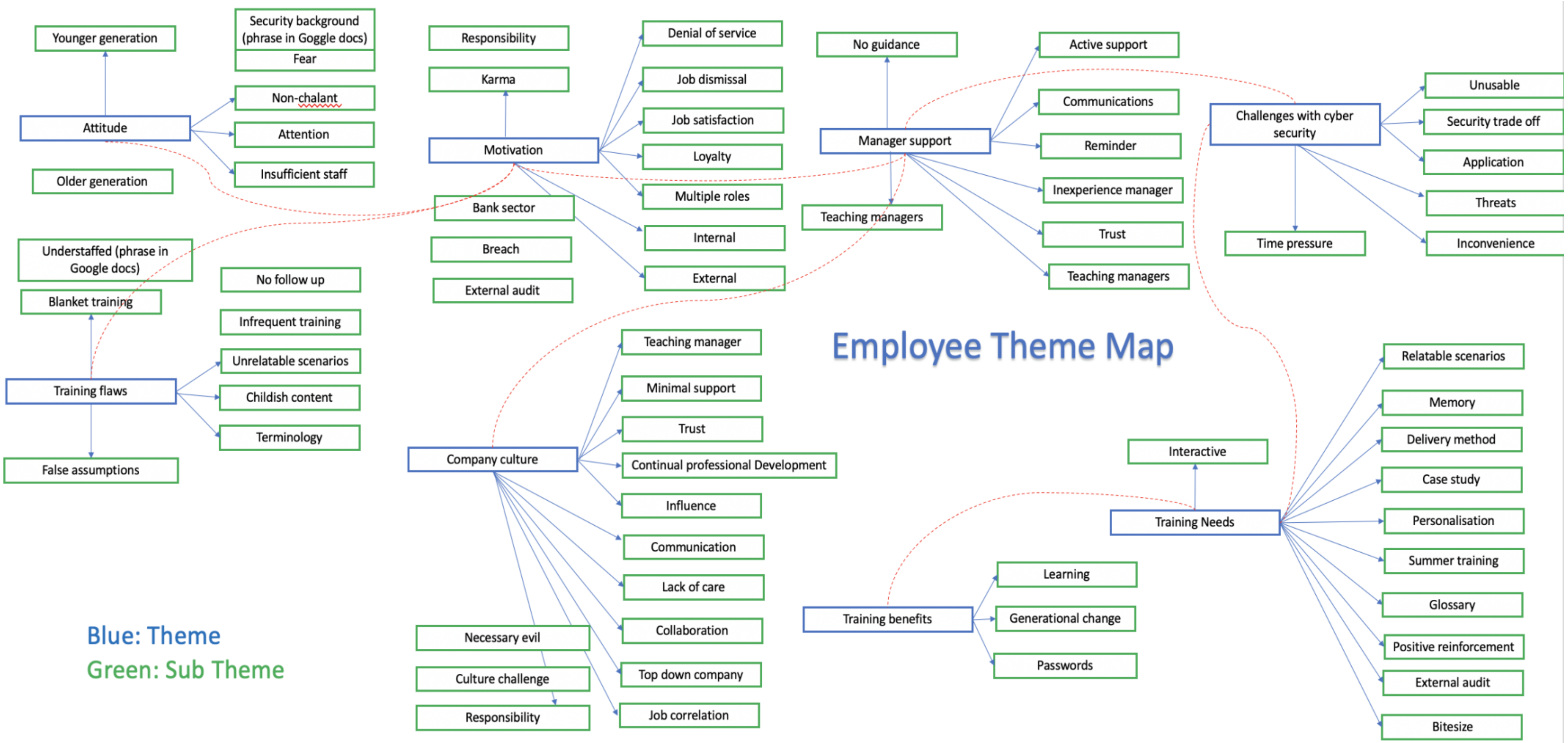


Figure 19 Employee theme map

7.2.1 Motivation

The participants discussed where their source of motivations comes from. The consensus of the interviews showed that employees are motivated by internal and external motivations and these contribute to perceptions of security, and consequentially interactions with security.

In terms of internal motivation, the participant explained they feel motivated because they do not want to be the cause of a breach, especially because it could lead to losing one's job. They said, *"I think the only motivation is like the fear of like a breach and like what if I need something and then I lost my job"* [P1]. This participant shows an element of personal motivation, as they also mentioned they do not want their personal data to be leaked out. For instance*, "I don't want to be the one who leeks something. I don't want my data to be leaked out"* [P1]. Another participant said similar; however they noted that data loss is not the end of the world, but in the same vein they wouldn't want their own personal data to be leaked. For example, *"maybe it's not the end of the world, but in an ideal world I don't want to have like lots of things like with my own being leaked"* [P2]. This participant added, they fear a breach and the leading consequences of losing their job. On the other hand, the employees discussed internal motivation and typified this by giving internal workplace examples. For example, *"We have internal audits with external audits, so there's reasons why things need to be in place. So no, I never feel the need to rush things"* [P11]. In addition to this, they discussed that their motivation intertwines, with the fact they don't want the business to experience a beach, but also, they specifically do not want people to know they instigated it. This shows that though they might care but the business, but it is contingent on their own reputation. For example, "*Well, because I don't want the X to have some like massive like security data breach and everyone to know it was me that clicked on the email That's my motivation Like I'd rather, but I wasn't that person"* [P12].

Some of the participants discussed that an element of work loyalty plays into how serious they take security. For example, *"there is a definitely a sense of loyalty in all sorts of ways because I've worked for the X for a long time*" [P12]. Another participant discussed they had been employed for a number of years, and how they feel indoctrinated into a corroborate mindset. For example, *"I've worked for the university for years, so maybe I'm just indoctrinated into the kind of like the corporate way of thinking of It"* [P12]. Another participant gave a different perspective of where their motivation comes from. They discussed there is a genuine interest in learning cyber security, so this solidified their interest. For example, *"It's important because I'm passionate about it I enjoy, you know, learning about cyber security, learning the tips and tricks and things that the hackers are doing"* [P3]. Lastly, one of the participated described a trade-off experience, when discerning between choosing cyber security and what is socially acceptable. For example, "*sometimes you can have a trade-off between what's morally right and what is socially right"* [P2].

7.2.2 Training needs

The employees were asked about their experience with previous training packages they had completed in the past. They began to describe what they felt better suited their work environment, they described elements of training they felt made them lose attention and they explained what would aid learning cyber security training. This theme is called 'Training needs.

Subtheme of Training Needs-Personalisation

The employees discussed personalisation in training, as a factor that aids learning. They discussed ways in which training should personalise training to match their department. For example, I think "the personalized to the department relevant training might be a better approach" [P9]. This participant added, there should be investments made to identify user needs and identify what is relevant, and tailor training to focus on the learners. For example, "It would be great if there was some time invested in actually going through the department. Check what's really relevant to them and actually look at real threats tailor made to the department" [P9]. The employees discussed relatable training, as an important factor that aids learning training. They spoke about scenario-based training, for instance, what could potentially happen if they experienced the scenario in the real world. For example, "I would probably prefer something like much more specific to my role and also it could be scenario based, kind of like these common scenarios you might come up against, like common pitfalls and maybe more baked in so" [P2]. They also discussed, to use different examples and case studies for repeated training, so it doesn't come across boring. They said "if it's something a bit different, like maybe like the actual content is the same but it's sort of presented in a different way, maybe you'd get better engagement from people would like feel a bit less bored by it" [P5].

In addition to the issue of personalisation, one participant discussed that training language and content need to specifically relate to daily work tasks, otherwise it becomes ambiguous. For example, "I guess the people that write the training or the people you know I can see they've really tried to put it in like plain language and everything, but if that's not what you do for your job, if you're not really involved in IT stuff and like mostly I'm just using my Computer mostly for emails and word documents and spreadsheets Actually all of that like web based stuff is like a bit of a mystery in a way as to how it all works” [P12].One participant discussed learning aids, content developers could consider when developing training for their business. They mentioned learning attributes, such as a Glossary. For example, “Maybe like some sort of glossary of terms or something, so that if there's a term…you could go and check like exactly what that means, or maybe some kind of case studies or sort of like examples to sort of illustrate that, rather than just explaining” [P12].

When the participants were asked if their managers seek to find what their training needs are, or challenges they experienced with cyber security, they often said this was not the norm in their business. One participant discussed that potential challenges would be discussed when an appraisal happens. For example, “So when you get in the appraisal will go throughout what my training needs are and what I've done” [P11]. Another participant gave a similar account; however, they pointed out that though the manager checks to see if there are any problems in general, there is an expectation from the employees to share any challenges they experience. For example, “My line manager checks in with me to see if I have any problems generally, but she's not at any point specifically asked if I have any cyber security related issues It's more just, she trusts me If I'm having an issue or something to bring it to her” [P8].

Sub theme of Training Needs-Memory

The participant discussed memory issues, as a factor to be considered in training needs. They mentioned they have poor memory, and so questioned how much content is retained months after the training. For example, “The question is would you remember this is one of the occasions in eight month’s time especially for me cause generally have quite like a poor memory for things” [P2]. They added that, perhaps an interactive training would be beneficial to making training engaging. For example, “I don't know how much actually gets retained I don't know if maybe something a bit more interactive would be beneficial”. [P8]. The participant generally spoke about their likes and dislikes from previous training they had completed in the past. They gave time suggestions as to when training is most effective for them to engage in. For example, “It depends on the time of the year. I think training is much better received over summer or over downtime” [P9]. They also spoke about negative reinforcements, according to them they felt it does not work. For example, “I don't think negative reinforcement training ever works in anything really” [P3]. On the other hand, one of the participants suggested training should be condensed into smaller specific chunks. They said “Training should be like more bite size chunks. More like specific chunks” [P2]. The participants discuss frustration that comes with security, they mention that security comes with a level of frustration, they question how much of this frustration is considered. For example, “I will say that there is never a level of too secure, but there's always a level of security to frustration, right? So, you can make things as secure as you want, but how frustrating is it for your users? [P3].

7.2.3 Training flaws

The employees described flaws they experienced with previous training they had done in the past. They discussed flaws such the training content and delivery style. One the flaws the participants mentioned, is that training can be frustrating, especially around passwords, so people take shortcuts instead because security is so strict. For example, *"you can't make it so frustrating for your user that they just don't want to do the job, or they'll save it in their browser passwords Or they'll make decisions that are negative against the security because the security has been so strict"* [P3]. The participants also said, cyber security training can be simple theoretically, but difficult in practice. For example, "*Feels like black and white in some quite simple theory space to do, whereas like other stuff is difficult in theory and It's difficult in practice"* [P2].

Subtheme of Training Flaws-Infrequent training

When the employees were asked how often they had cyber security training, the answer was generally once a year, or as of when recruited to join the company. For example, "So normally we have it once a year, so I had a couple of months ago" [P2]. The participant compared, privacy and ethics training, they regularly have, to cyber security training they have one off. They note the difficultly to remember a one-off training in comparison to a repeated training like privacy. For example, I didn't know how long it would take for me to just remember it like in a natural way, like in the same way I remember like the kind of privacy and like human ethics stuff that I must do is a researcher because that's literally been like years and years of training" [P2].

Subtheme of Training flaws-Blanket training

One of the sub themes that was developed from 'Training flaws' is 'Blanket training'. The participants discuss that training is sent to multiple other staff, and there is no relevant or relationship between the content and their work environment. The participant mentioned that training is written for several people, they note that each individual has a different level of knowledge and capability. For example, you have to write training for X people. I don't know how many we are people and with all different levels of knowledge and capability [P9]. Another participant said similar, they discussed that training is blanket and the same content is sent to every staff. For example, "It's just a blanket thing that sent out to staff" [P12]. For example, "The other bits, that kind of really specific to our company and like really technical and like seem to apply to another country. How do I remember that like how is that everything it impacts me in that I kind of figure out say?" [P2]. It was mentioned that training encompasses other modules, and therefore it makes it difficult to decipher what parts of the training relate to security. For example, "it's like so big. I think I'd probably like maybe remember like 3 out of 10 'cause it covers like so many different things and it's difficult to know what's the cybersecurity portion bit" [P2].

Subtheme of Training flaws (Training delivery)

The participants attributed the delivery of training, to the training flaws. They described that the training delivery is not adult-friendly and missed a real-life example. They said "The format of it, the delivery of it. I find it a bit too kiddy for my liking. Yeah, didn't learn anything new. Very basic. Very kiddy like and lacked real example" [P9]. They added that cyber security training presents information that is irrelevant to the recipient of the training. For example, "What's the point of me telling something that is irrelevant to our department, to somebody in a different department that will never have to do deal with like encrypted reports" [P9]. Does unrelated training turn people away from cyber security? Another flaw described they did not understand how specific cyber attacks happen in their workplace, and this is coupled with the terminology used to describe it. For example, "But I guess sometimes it's like the terminology that's used, and I don't entirely understand how it works, like how a cyber attack on the X" [P12]. They discussed that striking a balance between what they think people know and knowledge areas they believe are not as cognizant, is a difficult task to accomplish. For example, "If you assumed that everybody knew nothing, the training would probably be like way too detailed and boring for a lot of people that did already understand those things So it's a difficult balance" [P12].

7.2.4 Training benefits

The participants also discussed the benefits they identified when they complete training. They spoke about disseminating knowledge across to family members. For example, *"It's just so important to say it's affected me and I tried to pass that on for my children as well"* [P11]. Another participant mentioned that recent training reinforces training information in their minds. For example, *"Obviously done this cyber security training quite recently as well so that like really sort of reinforces it in your head"* [P12]. In addition, it was mentioned that training highlights knowledge gaps, that participants wouldn't ordinarily see. For example, "*It kind of shows stuff like maybe I wouldn't notice so I didn't even know that was something we were supposed to be doing. So it does help me learn"* [P2].

7.2.5 Manager support

The participants were asked whether Awareness professionals encourage and support security in the work place. They were asked how much of an impact manager support have on their decision making. Their responses distinguished two separate approaches, that Awareness professionals may adopt, they are either active support or lack of support.

Subtheme of Manager Support-Active support

The employees discussed ways in which their Awareness professionals support them to adhere to security and actively use it in daily tasks. One participant said, their manager sends warnings of risks they should be alert about. For example, "I think recently there's been so many communications from the X about the need to be careful with these things" [P12]. They recognise the importance of hierarchy and leadership, they claim that setting the example from senior members of staff assists in dispersing this across the business. For example, "it's setting that example at the top. I think that definitely helps in every part of any department" [P11]. This participant added that, setting the expectations of the business and showcasing what is important and priority helps create a consensus for everybody within the business. For example, "if they're set that expectation or that model, if that's the kind of person they are now saying this is important and prioritizing, then I think yeah, that definitely sets the agenda for everybody" [P11]. Another method of active support is that some Awareness professionals would email employees to remind them of outstanding training they need to complete. For example, "Yeah, so that like my line manager would email everybody that she manages and say, make sure that you've do this training [P12].

Subtheme of Manager Support-Modelling behaviour

The participants also described that Awareness professionals who model secure behaviour, influence ow they approach cyber security. One participant gave an account, that whenever they have asked their manager questions, they are encouraged to follow the correct policy. The manager goes as far to find answers from their compliance, to ensure there are no shortcuts and cyber security is appropriately adhered to. For example, “So when I've gone to a manager with these questions just to check and get that audit trail he's never told me to cut corners, he will always like point me to a specific part of the policy or he'll be, well, I'm gonna ask somebody from compliance or he would say this is what we do in this situation So I think having that reassurance from the manager that compliance matters is really important” [P2]. In addition to this, they mentioned that when they see how important security is to their manager, it influences them to also spend time on security. They said “It just shows it's important to him and so I think all of that really helps. Knowing that is important and that people are going into spend like the time on it” [P2].

Subtheme of Manager Support-Lack of manager support

As well as active support, the participants also discussed a lack of manager support towards cyber security. The interviews showed that some Awareness professionals generally trust their staff to complete training, and so they do not follow up on training or potential challenges employees may have. They discussed that training is seen as a tick box exercise and once it is complete, it is assumed that participants do not need further support. For example, “I think managers trust us to do the right thing, in terms of ticking boxes they send us to that cyber security training and they assume that everything is fine” [P9]. One the participants discussed one of their daily tasks, which includes collecting bank details. However, they stated that they implemented their own method of collecting these details securely, as their manager did not suggest security policies they should follow. For example, “So I've been asking the X to send me the bank details in an encrypted Excel file and to send the password on a separate email UM, but if I hadn't necessarily known to do that in the first place, my line manager should have suggested that I do that That sort of thing” [P8].The participants mentioned they have never experienced their manager send specific material to look at. They described material comes centrally and not within the team. For example, “I've never seen anything come from my manager to look at things specifically, it's all kind of dealt with centrally and not within the team” [P2]. Another participant mentioned there are prompts to do training, but there is little to no attempt to follow up with training. For example, “We get prompted to do the training, but it's not followed up ever” [P12]. On the other hand, one participant says it is the managers responsibility to liaise with employees, especially if dealing with sensitive data. They said “I think the responsibility of your line manager to check in with you if there's specially if you're handling anything particularly sensitive to make sure that you are being careful with it” [P8].

7.2.6 Organisational Culture

The participants discussed various activities they partake in, and they also discussed norms and values the company imbibes which compromises the organisational culture. Some participants discussed positive and negative cultures within the workplace and demonstrate how these are representative of the business.

Subtheme of Organisational Culture-Positive Culture

One of the participants discussed that employees communicate on Teams, and potential threats to the business are shared. This is where people can express concerns and discuss if there are shared risks amongst individuals. For example, “So we took we do a chat on teams so for the team as jobs would be working at home. So like this morning I said tell if you've seen this, I took a snippet of that something I got this morning that I wasn't sure about and I was like, have you seen this? Have you got one of these? And so we kind of keep in touch that way and I would just bring something up anyway” [P11]. The same participant said they felt there was generally a good collaborative working culture across their departments, especially the finance team. For example, “I think we have a good culture of working together in not only just our team but I think the wider finance team” [P11]. Similar was said by another participant, who discussed there is a culture difference in how people perceive and interact with security, based on their industry, like the financial institutions. For example, “It depends on the industry, so I think that there are some people in certain industries where they're very cautious and very protected and go through a lot of cyber security training like, the financial institutions and things of that nature” [P3]. Some participants discussed activities they partake in; these activities contribute to the overall culture of the business. One of the activities, include going the extra mile to ensure traffic coming from external parties are secure to be opened. For example, “If it looks dodgy, I would probably get on the phone and say ah is everything OK your end up just to be safe” [P9].

The participants suggested there is a secure culture in their workplace, for example, they expressed they would go through multiple layers of security. For example, “I don’t care if I have to go through two hoops” [P9]. As part of this secure culture, this participant said their company generally share a culture of not clicking on links. They said “We don’t like links, we don't like clicking on clicks" [P9]. To add, the participants discussed what enables a positive security culture in the workplace, they said the business ought to be in a good place, and this consequentially cascades to employees too. For example, "I think then like everybody benefits if like the organization is in a good place, then as staff you benefit from that" [P12]. Another participant mentioned that positive culture, comes from managers at the top. For example, "It's setting that example at the top. I think that definitely helps in every part of any department" [P11].

Subtheme of Organisational Culture-Negative Culture

On the contrary, some participants spoke about negative cultures within the work palace. For instance, one participant, discussed that they have been better at IT, than managers, in every job they have occupied, and in fact they teach managers. For example, "I have not had a role where a manager has been better with IT, than me. Usually I'm the one teaching them" [P9]. Similar was said by another participant, they described that although not intrinsic to their job, they are the ones informing managers of security risks. They explained that from previous experience, awareness professionals are not as knowledgeable as the employees are. For example, I'm the one informing the managers at the moment. Not as part of my job, but from experience. Usually, the managers are not as technical savvy as we are" [P9].

Subtheme of Organisational Culture-Culture challenges

The participant discussed challenges they believe exist when it comes to security culture in the workplace. For example, "I think the part of trying to get people to care about the business, whatever it may be, and that's sometimes a challenge today" [P3]. When participants were asked what challenges they experience with security, one mentioned the difficulty comes from knowing the right procedure to adopt in what part of the business. They explained there are different expectations in different parts of the business. For example, "I think my biggest challenge is maybe like knowing what to do when and like knowing the exact right procedure, and sometimes it feels like different parts of the business have like different norms and different expectations" [P2].

Subtheme of Organisational Culture-Responsibility

A subtheme that was developed from Organisational Culture is 'Responsibility'. The employees who imbibed in a positive security culture associated this with cyber security being a key responsibility to their role. One employee said, they did not experience a trade-off, because cyber security is their job. For example, "I mean for me my job is cyber security, so there's not really any trade off for me. It's just another day" [P3]. In another company, there is a culture of shared responsibility, however they also acknowledge this may not happen in reality. For example, "that's why it's kind of like everybody's responsibility to do it. But I know that there's times when that doesn't happen all the time, like in practice" [P2]. Another participant mentioned that security is a shared responsibility, so they encourage that employees should have the company's interest at heart. For example, "Well, I think we all play a part on it, so we need common sense, so it comes a bit to the individual to protect themselves and have the best interest of the company" [P9]. This links to internal motivation 7.6.1, employees are internally motivated because they have the company's best interest at heart and therefore, they feel a sense of responsibility to be cyber secure.

In addition to this, the participants identified a shared responsibility culture in the company, and they describe that these behaviours are inclusive to personal life. This participant worked in the financial team. For example, I think, we all have a responsibility. We all own responsibility and the X is very good about that cause they've just put out a few online modules that we have to do, but we all have to be vigilant as to what we're doing and even when we're at home in our personal life, whenever we get an email, we have to be aware of things up [P11]. On the other hand, one employee who trained staff gave a counter response to responsibility. They explained the level of encouragement and emphasis placed on staff, however employees did exactly what was being negated. So instead, they believe they should not take responsibility over staff. For example, "I staffed I provide training to staff. You cannot imagine how many times I've told people please do not do this. We have an audit we need to do this to abide to the framework and then people go into exactly what we told them not to do so and how should I be accountable for them not listening?" [P9]. Likewise, one participant said responsibility for cyber security comes from line managers, as they should give extra precautionary care for sensitive data. For example, "I think the responsibility of your line manager to check in with you if there's specially if you're handling anything particularly sensitive to make sure that you are being careful with it" [P8].

Sub theme of Organisational Culture-Cyber necessity

Another subtheme from Organisational culture, is ‘Cyber necessity’. One employee acknowledged that while security may slow down performance, it is necessity that must happen. For example, “It does slow us down, but it's a necessary evil” [P9]. Similar to this, they said cyber security is a minor annoyance but does not prohibit work. In fact, they accept that security is there for a reason. For example, “So to me it's a minor annoyance and not prohibit my work. It is. I accept that it's there for a reason” [P11].

7.2.7 Attitudes

The employees discussed attitudes they have regarding cyber security. The attitudes generally reflect non-chalant attitudes and positive attitudes, after a cyber security breach. They described that businesses are understaffed, and organisations fail to recruit new staff. They added that employees have repeated the same job over several years and are burnout. For example, *“They are tired, overwhelmed. They are understaffed departments, are understaffed people. They don't recruit. People keep get retired or redundant. And then there's no recruitment drive. And people have been doing the same job for 10-15 years*”. They are a bit more burnout [P9]. They associated this with businesses never experiencing a significant cyber security issue in the past. For example, *“Maybe because they never had any issues in the past*” [P9].

Subtheme of Attitudes-Lack of care

The participant highlighted that there is a work determination which is to complete jobs very quickly and therefore people simply do not care about security. For example, "They want to do their job fast and they just don't care" [P9]. The same participant explained that cyber security is annoying because it requires additional time to think. For example, "I think sometimes it feels annoying because it's like a time thinking" [P2]. In addition to this, another participant specified that certain industries have a culture of lapse attitudes towards security, and if people do not feel directly affected there is a likelihood there is no care. For example, "But I also think that there's industries where, people just don't care. It's not my stuff It's not my data, it's not my computer" [P3]. The employees highlighted that the reason for the lapse in attitudes, at times comes from a place of fear. For example, "Some people are genuinely afraid of tech" [P9]. Some participants acknowledged that cyber security happens, but they questioned how serious it is. They compared a cyber breach, to the events happening in the world, and compare its severity. For example, "the real impact of these privacy breaches, if it happens, everything that's happening in the world, is that really the end of the world? Like is it really that massive threat to business that we think is?" [P2]. They added that visiting untrusted sites are the norms in their business. For example, "This type of stuff probably happens all the time…visiting untrusted site [P2]. This also reflects a poor security culture within this organisation.

Subtheme of Attitudes-Attention after breach

The results showed that employees attention levels increased after they experienced a breach. One participant recounted an event where they experienced a breach, they highlighted that having their personal data stolen stirs up concern and consideration to how important cyber security is. For example, "So my eBay had got hacked and I had no idea like how, why or where… So maybe somebody's got my home address, my phone number, and my passwords I don't know if they've got like my age or like photos of me …so that's when I think how important is it? [P2]. The participant highlighted that until a breach happens, people tend to have a relaxed attitude. For example, "So until it becomes an issue, I think people are relaxed and the other day they were all relaxed and me running like a headless chicken and then we had the problem and then everybody like, oh OK, we're going to be careful this now" [P9]. One participant mentioned that if a breach happened, only then would training attendance be checked to verify if training had been adhered to. For example, "I guess unless something went wrong and that's when I think they would find out that like it had been followed"

*[*P7]. They added that at times a breach needs to happen to see the consequences. For example, “I think you have to sometimes see the consequences first hand and also know that you’re liable to experience consequences” [P2]. One participant who experienced a breach said, people will recognise the impact of breach as of when it happens to them. For example, “People only realise or when, the penny needs to drop” [P9].

Subtheme of Attitudes-Younger generation

The employees discussed there is a disparity in attitudes towards cyber security, in different generations. They mentioned that the younger generation are more risk cognizant, and they understand better. One participant spoke from her perspective as a young person, and described that because she grew up with technology, she can conveniently use it. For example, “So I sort of understand it's just something I kind of get on with it I grew up with the Internet as being a thing so. I think it helps that I'm a bit younger” [P8]. Another participant highlighted that, older participants are more likely to click unsafe links out of curiosity, but younger people tend to thoroughly think about the risks. For example, “especially with the emails with the dodgy link setting, we would perhaps think a bit more before we click it, whereas someone who maybe my parents’ generation or a bit older order would be like oh what's this and just open it and then get a virus” [P8].

Subtheme of Attitudes-Older generation

The participant comparatively discussed, the older generation and the younger generation. They claimed that younger people understand risks more. For example, “I suppose sometimes there's a risk that if people don't understand… the younger generation I just think they're a bit savvier with all of that stuff and they sort of understand it better” [P12]. One of the employees discussed an older colleague, who is resistant to IT, for instance they do not see the need for a computer. For example, “I do have some colleagues that really struggle with IT and very resistant to IT. Even you know like I have been a teacher for years, I don't need the computer” [P9]. This participant added that older employees who shared this mindset are beginning to retire. For example, “those kind of stuff I have that kind of mentality in in the department, although we most of them every retired now” [P9]. Some older participants had attitudes, that supported what the younger generation said. For instance, some had attitudes where they felt they could never understand cyber security, and only younger people can. For example, “I kind of followed the rules, but some of it is like a little bit of a mystery to me, but I know what kind of what the risks are, but I think you know the younger generation are like very much more like switched on to all of that” [P12].

7.2.8 Small business challenge

The employees discussed small business challenges, some of this centred budget issues. One employee said, in comparison to larger businesses, smaller businesses are usually at a larger risk, because of limited financial allocation for cyber security. For example, "*Smaller companies also tend to be bigger targets because they don't have the security budget that a large company does, so they will inherently be less secure because they can't afford to buy that fancy firewall"* [P3]. This participant added that, large businesses are heavily targeted, and so they have regular training for their employees. For example, *"large corporation tends to have a much bigger target on them, they're going to have a cyber security team They're going to have you know, regular interval training with those people"* [P3]. Similar to this, small businesses also have a mentality that they are exempt from cyber breach. For example, *"I think a lot of times the smaller businesses don't think that their a target yet"* [P3]. They added that, small businesses make use of who is available, for instance, the manager, is the same person who conducts cyber security training. For example, "*In smaller to medium businesses, I find that a lot of times the security person in the company has to use the manager, to educate because a lot of times it's just one guy that is running cyber security and the only way to make that scale is to use other resources that you have, such as the people manage"* [P3]. In the same vein, the employees highlighted that people running small businesses simply do not know enough about cyber security to conduct training. For example, "*I think a lot of times you know, depending on how small the business is, a lot of times the people that are running the business just don't know enough about cyber security to do training"* [P3]. Another participant discussed they need a compliance tool, but this is limited due to costs and budget. For example, *"I just had like some kind of compliant tool that I knew I could do this with, but I can't because it's like a cost"* [P2].

7.2.9 Employee Result Summary

This Chapter discussed the results from the Interviews; Study 2 of the research. In summary, the employees lack of manager support was unexpected. For the employees a form of motivation comes from internal drivers, for instance, primarily motivated by the thought of losing their jobs and potential 'name and shame' if they were the source of a breach. Employees' perceptions and attitudes originate from previous jobs, organisational culture and positive and negative modelling. The level of attentiveness and earnestness employees exhibit come after they experience a breach, it further increases their motivation for cyber security. The employees show an interest to training, when it is relevant, relates to personal work environment and when it is easily consumable.

7.3 Discussion of Results from Employee

7.3.1 Motivation

The employee's motivation generally come from internal motivation. Employees do not want to be the cause of a breach, and they are incentivised by their jobs to adhere to security. They discussed from an empathic perspective, that they wouldn't want their personal data to be at risk of a cyber breach, so this motivates them to intensify their security vigilance. For example, Boerman et al. (2021) explored motivations for online privacy protection behaviour and discussed that, people are concerned about their online privacy, they worry about possible misuse of their personal information and express the desire to have more control over their personal information line (Gomez, 2009). Similar to this, they described a cross-polynisation between personal motivation and internal motivation, for example, though employees were internally motivated to the business, they were also personally motivated because they did not want the embarrassment or the shame of introducing a breach into the business. However, this is dissimilar to Ferreira et al. (2018) who claimed that if adult learners do no perceive that a learning event will add value or satisfaction, they are unlikely to be motivated to commit. Although some employees followed this notion, they displayed non-chalant attitudes to data loss and data leaks, for example, they questioned the seriousness of a breach, but in the same vein despite the idea of their data being at loss. This illustrates the motivation employees have towards cyber security, there is a heightened level of motivation if their data is at risk, but somewhat nonchalant to risk to the business. This could mean that the ideology that employees lack cyber security awareness is false, it could mean employees are indeed aware but are not motivated to adhere to security, because it is not their own personal data at risk.

7.3.2 Training needs

The employees discussed that one of reasons for disengagement is the lack of personalisation in training. They described that training should be personalised; it should incorporate language and scenarios that specifically relate to daily work tasks (Verbert, 2012). This typifies Taatgen (2021) notion as they support that training effectiveness is dependent on if content reflects and is identical to the actual job task. For example, if the training programme is about the safe use of modern technologies, and these technologies are not available in the rea educational setting, the training transfer will slow down (Bhatti & Aldossary, 2021). It is therefore always advisable that training contents should be familiar with the actual educational setting to maximise the rate of transfer. Bhatti et al (2013) observed that when trainees found training content similar to the real educational settings, they would show more confidence and actively participate in the training activities. The employees shared that awareness professionals typically do not investigate what their cyber security training needs are, what challenges they experience with security or what feedback they have to share about previous training. Rogers (1969) developed guidelines for awareness professionals, and it encourages them to elicit and clarify the purposes of the individuals in the class, as well as other general purposes of the group. On the contrary, the results shows that awareness professionals expect and trust employees to share cyber security related issues. One of the training considerations from the employees is memory. As the literature establishes each person’s working memory capacity variers from one individual to the other (Robert et al., 2009). Given memory limitation, employees questioned how much content will be retained after months of training, couple with the fact that training is infrequently delivered. The employees discussed that training is most receptive during the summer period or over downtime. They also mentioned that negative reinforcement does not negate poor cyber security behaviour. They suggested one of the easiest ways to consume information is if information is broken into small bite size. Similar to this, NCSC (2019) design training courses which spread from minutes to over several days. This suggests that employees are likely to consume information if presented in smaller chunks over a period, rather than one off training.

7.3.3 Training flaws

The employees described flaws they experienced with training. They generally felt cyber security could be frustrating, and at times they have had to deter away from security to quickly finish job tasks (Pham et al. 2017). They felt cyber security can be binary and straightforward in some regards, but in some cases, it is difficult to practicalise theory from training into reality. Like awareness professionals, employees also explained training happens as a one off, mostly when recruited to join the company. They note the difficulty to remember content from one-off training, in comparison to repeated training like privacy and ethics. One of the challenges they experience with training is that it often encompasses other training modules, so it makes it difficult to identify exactly what parts are cyber security related. The results show that training delivery is not adult-friendly. They described that training is sent to various other departments, and there is no correlation between training content and their work environment. They added that training is blanket, and there is no differentiation in training for people with different levels of knowledge and capability. The success of training is partly contingent on meeting training participant needs. Taylor (2013) noted that awareness professionals should recognise that adults want their learning to be problem-oriented, personalised and appropriate to their need for direction and personal responsibility. The results show otherwise, it shows that training is blanket and covers multiple departments and industries, without addressing personalised security issues or concerns of that of the participant or business.

7.3.4 Manager Support

The awareness professionals showed active support to employees, by sending cautions they should be aware of. The results showed that employees tend to adhere to security when there is an observable example set from awareness professionals and other senior members of staff (Srinidhi et al., 2015). They also mentioned that businesses should set expectations of employees, and in doing so everybody is aware of what expectations are. This supported in the literature, as managerial support has been identified as a key environmental variable affecting transfer (Ford et al., 1992) and is likely to be of central importance in creating a 'transfer friendly' environment (Axtell et al., 1997). The employees discussed the impact of positive modelling. Some awareness professionals go the extra mile to find answers to questions or concerns employees have. When employees observe the level of urgency security concerns are dealt with, it motivates them to learn cyber security and adopt principles in the workplace. Positive modelling not only impacts employees within the workplace, it also transcends into personal spheres, with some employees now teaching their family members about cyber security. For example, Eruat et al. (2001) examined the impact of the manager on learning in the workplace, they identified that negative models could be a source of learning as well as positive models, and often are elements of both. This shows that employees are observing senior staff, and their models of behaviour could influence how employees perceive and then engage with cyber security. In the same vein, the employees described a lapse of positive attitudes from Awareness professionals. Some employees explained that existing practices in their workplace, such as collecting bank details have no procedure or method of ensuring safety of data collection or storage. As a result of this, some employees adopted and implemented methods they were once taught in previous jobs and transferred this into their new job. Some employees had never experienced a manager encourage, support or send information about risks they should be aware of.

7.3.5 Organisational Culture

There was a display of positive and negative cultures in the businesses interviewed. Some of the positive cultures included going through extra layers of security. The employees shared a positive culture of security, as they discussed regardless of how busy they might be, they would never cut corners, because security is integral. They continue to share this secure culture as they work from home. This shows that security is an essential part to their business operations, they ensure security is still at the forefront of employee minds, despite working from home. They discussed that culture is impacted by the state of the organisation, for example, if a business is in a good place, it automatically cascades to the employees. The results show that employees believed there was a disparity in culture difference from one industry to another. For example, they said financial institutions like banks are intrinsically protected and partake in more training. In the same vein, they discussed negative cultures within the workplace. They discussed that Awareness professionals are not typically as knowledge as employees. Some went as far to describe that they teach and inform Awareness professionals of risks, and in fact their manager does not support or influence them to learn cyber security. This shows that some Awareness professionals may not actually be as trained or educated to fulfil the role of an Awareness professional. If employees can spot negative attitudes and cultures depicted from senior staff, who should be cascading positive security messages across the business, it could influence them to also overlook security, since their managers also do. The positive attitudes towards cyber security, came from employees who have experienced a breach in the past, and consequently recognise the risks imposed on businesses. They share a culture of risk acknowledgement; they accept cyber security may take extra time, but also acknowledge the deeper consequences of a breach. This shows that the desire to be secure comes as result of a breach. Does this mean, employees need to experience a breach to be security conscious?

7.3.6 Attitudes

The employees described other employees who have been employed for years, and say organisations fail to recruit new staff because there is no recruitment drive. They add that these employees are overwhelmed and burnout, and due to doing the same job over several years they are unmotivated to change or adopt new policies, like security. They associated this with the fact that, perhaps because they have never had security issues in the past. The results showed that people prioritise work to complete tasks as quickly, and as a result people do not care about security. In addition, they questioned the seriousness of a breach, they questioned if the impact of a breach would really cause any damage. They also compared a cyber breach, to the events happening in the world. This shows that some employees have reservations about security and its impact. The results also showed that employees were more attentive to cyber risks after they experienced a breach. They described that experiencing a breach, raises attention for personal data and how these are being used. This shows that people are motivated for personal reasons, unless it directly affects them people are generally lapse towards security.

The employees identified disparities between the older staff and younger staff. The results showed that the younger generation were more cognizant and aware of cyber risks, and not only this they displayed positive attitudes towards cyber security. On the other hand, the older staff did not understand the risks they personally pose to the business, and they felt only younger employees could learn cyber security. This shows that the older generation have a dismissive attitude to cyber security, and feel only a certain group can understand it, e.g., the younger generation.

7.3.7 Small business challenge

The results showed that small businesses believe they are inherently more at risk, than large businesses. This is because small businesses have limited financial freedom to buy physical security (Antipova, 2021). The employees believe large businesses are targeted more, so they have regular training for staff (Zimmerman, 2014). This shows that some small businesses realise the risks posed on them, but there is little to nothing they can do because of financial limitations. In addition to this, small businesses use managers as awareness professionals and they associate this with, financial limitations. Large businesses may have the freedom to seek for professional help, but small businesses are limited because of finances. For many reasons, this could be problematic, if haphazard awareness professionals are not as skilled or knowledgeable as employees, then this can easily be identified, and employees can choose to disengage. To buttress this, the results show employees felt small businesses do not know enough to conduct cyber security training.

7.4 Concluding Discussion

This research identified that cyber security training may not encapsulate fundamental factors and theories pertinent to learning, more specifically adult learning. In this Chapter, the research questions are revisited alongside how the research addressed each question.

There were three research questions:

1. How do content developers cyber training select, devise, and deliver cyber security training?
2. How does the procurement and delivery of cyber training affect how people receive, retain and apply cyber knowledge in the workplace?
3. How does organisational culture affect how cyber training is perceived in the workplace?

There were proposed aims:

1. To identify the procedures and processes content developers take to create and deliver cyber training.
2. To identify what factors, affect users from learning and changing behaviour.
3. To identify if any communication between content developers, end users or awareness professionals.
4. To understand challenges SMEs, have with cyber training.

Three groups involved in the development of training, the request for training and the experience of cyber security training were: content developers, awareness professionals and employees. The overall results suggest that content developers develop training based on assumptions and belief systems they hold about businesses and employees therein. The results show that employee challenges and apprehensions are coupled with the complexity of training design, content, and delivery.

7.4.1 Content Developers

Research question 1: How do content developers of cyber training select, devise, and deliver cyber security training?

The results show that content developers select training by taking a mix and match approach, as they sift through various reputable training packages such as NIST and OSSTMM, to choose what they think best addresses clients. When they identify suitable training, they readapt training packages and deliver this to multiple clients, making this a 'blanket' training, e.g., it covers a wide range of target audience. One of the reasons for this approach is for sustainability purposes; content developers suggest investigating employee needs would mean they are consultants, and it would cause business efficiency problems. In the same vein, the developers acknowledge the problem challenge by using blanket training for all clients, they identify that this method doesn't reflect the local settings of that client. In addition to this, training is developed with previous knowledge and experience in past jobs and education. While some of this information may be apt and relevant, this method questions the authenticity of the information, for example, if information from past jobs is relative to that job, it minimises its relevance in the current job and training is ineffective. When developers deliver training they measure attendance, but little to no metrics to gather employee feedback about training. For example, employees would complete training, but there is no opportunity to share their experience, and what they propose for future changes and development in the next training. However, Patterson et al. (2011) recommends that content developers should keep lines of communication open, in so doing, they can also collect data on when and why people may have had a disinterest and what they think should change in future training packages.

The content developers in both Nigeria and the UK discuss that SMEs are financially limited to search for customised training, because of this they use 'off the shelf' training, as opposed to customised training, which may directly address employee needs and cyber security challenges in the workplace. The developers identified disparities in motivation and attitudes between different industries, such as the bank. The employees within the Finance department confirmed this, they discussed they were intrinsically secure and aware of risks, because of the nature of their job. In addition to this, they perceived that employees generally have a limited attention span for cyber security, and if the wrong campaign message is sent, then people will disengage with training.

One content developer conducts interview with awareness professionals to gather employee needs and what challenges they experience with cyber security. After developing and conducting training, they found that employees had lower knowledge, than what was discussed by the awareness professional. This shows there is a disconnect between what awareness professionals think employees are struggling with and what needs are, as to what employees actually need. This has a ripple effect on the success of cyber security training. For example, Bhatti and Aldossary (2021) suggest that training contents are critical for higher level of training transfer due to the fact that when trainees observe training contents are similar to their setting, they feel confident in transferring the learned skills and devise such teaching strategies that are compatible with the training contents. On the other hand, if training contents are not similar to their work setting, training transfer will decrease, and all resources and efforts allocated by the management will be wasted. The developers assume that younger employees like quizzes and games, however upon delivering training they found this was untrue. This shows that developers develop training based on perceptions and ideologies they hold about employees, they fail to address uncertainties and perceptions they hold with awareness professionals and with employees themselves. This means that training developer is of arbitrary substance because it does not fulfil the requirements or suggestions early education scholar suggest, such as Rogers (1969).

Finally, the developers discussed that small businesses are financially restricted, so they reduce bills to maintain interest, otherwise businesses lose an interest in cyber security. If businesses, see cyber security as contingent to budget, it means they do not really see the value or need for cyber security in and of itself. As a result, developers raise cyber security pioneers in the clients' organisations, who will talk about cyber security. This may seem like a plausible idea to content developers, but it raises the questions, are these pioneers trained in adult learning? Are they motivated to do this additional job?

7.4.2 Awareness Professionals

The awareness professionals demonstrated both positive and negative attitudes towards cyber security. Their interest for cyber security were generally around internal motivation, for example, factors that directly impact them. For example, they described cyber security as tick box exercise for business rating and accreditations. This shows the interest is contingent on a result that impacts and benefits their business goals. They discussed that if employees find training, they think will benefit them, there is an expectation employees should find this training and raise it with Awareness professionals. Culture was a prominent factor that affected how employees perceive cyber security. The Awareness professionals discussed that cyber security has not positively been modelled in businesses, and as a result, there is no security culture in businesses.

The awareness professionals discussed various methods they use to select training, some of which is through research. The professionals who followed this method used cyber security in previous jobs and contributes to attitudes and perceptions to cyber security. The professionals have an expectation from employees; they should look for training and complete it. This shows there is a belief that training is not a business standard or requirements, it is seen as an activity employees desire to learn, rather than an intended training from awareness professionals. In addition to this, it shows that Awareness professionals expect training should be free, hence why there is an expectation for employee to find training and complete it, rather than a paid outsourced service. On the other hand, awareness professionals were sent training programs and information, through local authorities, word of mouth and Eventbrite. The professionals rarely actively looked for cyber security training, as they often see it as a tick box exercise, and search for it when it directly affects business deals, contracts and how potential clients may view them. They often went for 'off the shelf' training as it was financially feasible. The professionals note that 'off the shelf' training causes disengagement because of the lack of engagement and relevance to the target audience. If awareness professionals, have identified these challenges, then why are 'off the shelf' training still being conducted to employees, when there is an understanding of its shortcomings?

The awareness professionals did not outline training objectives, and there was little to no procedure or methods to evaluate training effectiveness or success. In the exception, where employees returned feeling like training was unbeneficial, only then would awareness professionals contact cyber training developers. This also represents a poor security culture, for example, professionals only speak to training developers, if there is an issue. This shows there is no real interest to evaluate training or gather employee feedback about training. This solidifies the point that, professionals see training as a tick box exercise for internal benefits, and not because they want to address real security challenges in the organisation. security. External motivation implored awareness professionals to search for cyber security training. They described business relationships they have with clients, that require handling personal data and working with local authorities. The professionals had a haphazard approach for security risks, they acknowledged they were not as secure as they could be and recognise some of the consequences that could beseech their business. The results from Study 1b Chapter 5 also show that professionals were driven by external motivation, it is an integral factor that drives professionals to adopt cyber security.

7.4.3 Employees

The interviews with the employees answered two research questions out of three. They are:

1. How does the procurement and delivery of cyber training affect how people receive, retain, and apply cyber knowledge in the workplace?
2. How does organisational culture affect how cyber training is perceived in the workplace?

The first research question looked at how the selection and delivery of cyber training impact how employees receive, retain and transfer knowledge in the workplace. The employees discussed that training is not memorable because of its complicated language, and its lack of relevance of examples and scenarios. This correlates to what the content developers shared, as they described that training is designed for multi-use by several businesses. For example, training could be developed with no particular client in mind, however, it can be distributed to businesses handling personal data like a university as well as a charity who does not handle personal data. As a result, employees identified little to no correlation between training content and their work environment. Consequently, employees would lose interest and disengage in training because it is irrelevant and does not address specific problems they encounter.

The second research question looked at how organisational culture affects the perception of security in the workplace. The results showed that both negative and positive modelling (Eraut, 2001) can form a culture in the workplace. For example, some employees were more knowledgeable about cyber risks than managers and this culture expanded across the business, as employees did not witness the seriousness of security in their managers, and in turn, believed cyber security is unimportant. Similar to this, some of the employees described a culture of communication where employees can freely express challenges or errors they encounter and resolve them through collaborative work. Other employees added that a positive security culture comes from a hierarchy, i.e., managers and claim that if they observe managers and peers behaving securely, it will influence them to also behave securely. This could mean that employees are motivated through the organisational culture of cyber security in the workplace. For example, as employees observe a positive security culture, it could internally motivate them to behave securely. So not only through job satisfaction or the fear of losing their job, but through the organisational culture of security. That is, employees, observe and learn the organisational culture of their environment and it impacts their perception, in terms of whether it is worth note-taking and adhering to. This shows that organisational culture has leverage on the perception employees have about cyber security culture.

The employees discussed that they would not cut corners to finish a task quickly, and some would go through extra layers of security to ensure activities were securely performed. However, these participants worked in the Finance department, IT or had experienced a breach in the past. This confirms one of the beliefs the Content developers have about employees, which was people who work in finance and IT are generally aware and informed about risks and act accordingly. On the other hand, employees from other industries, such a charity shops and academics generally prioritised work over security.

In comparison to the awareness professionals, employees were driven towards cyber security as a result of internal motivation. Their motivation did not come handling personal data it came from the fact that employees did not want to lose their jobs, as well as this, they do not want their personal data at risk. The awareness professionals discussed autonomy, i.e., employees should actively search for security training they think is relevant. The employees discussed the impact of positive modelling, for example, if they identify managers and senior staff encourage the use of security, this could also heighten an interest for the topic. However, when employees have an onus to search for training, rather than managers search for training and deliver, employees could perceive cyber as unimportant as it is portrayed as personal development, as opposed to an all-rounded development, for both individual and business.

The employees discussed issues with recruitment. They mentioned that employees who feel burnout and overwhelmed by security, have been doing the same job for several years and there is motivation adapt change. The results showed that organisational culture, flaws in training content, motivation and busy work schedules are major factors that affect learning cyber security.

7.5 Chapter Summary

In this Chapter, the results from each interview group (content developer, employee and awareness professional) were presented and discussed. The Chapter started with the methods in which content developers select and develop training, the results show they often take a mix and match approach, by selecting training they assume clients may benefit from. The results show that employees have little to no say about training objectives or topics that need addressing, it also showed that training is rarely evaluated. For example, employees are not able to share their experiences and what they found beneficial or less beneficial. The content developers have a plethora of beliefs about businesses and their employees, the results show content developers are driven by these beliefs, some of which counter reality and therefore false training is developed. This Chapter discussed challenges awareness professional had in the workplace, one of them were financial challenges which was a common theme across SMEs. This limitation meant that training is 'off shelf' and it causes disengagement because the material is irrelevant. Akin to the content developers, the professionals have little to no way of measuring training success. This Chapter also discussed employee results, it highlighted employee needs, their source of motivation and training limitations, the influence of managers and organisational culture. Each of the results was followed up by a discussion relating to the literature in Chapter 2. Lastly, the chapter presents how the research questions are answered through the analysis of the results.

Chapter 8 Proposed Solution to Designing a training package

8.1 Chapter Introduction

In this section, a set of recommendations for content developers, awareness professionals and employees are suggested. The recommendations are developed based on the results and discussions from Study 1b and Study 2.

8.1.1 Content Developer Recommendation

The results showed that content developers lacked training in Education and Training for Adult Learning. The content developers discussed that they select training based on open-source information, for example, they may research the latest trends and from this begin to cherry-pick what content they want to include in training. All the developers either followed this pattern or sifted through various training until they found one, they believed to be suitable. The reason for this haphazard method could be that the literature does not provide recommendations or suggestions as to how content developers should select or develop training.

8.1.1.1 Recommendation 1: Gather User Requirements (Software Development Life Cycle)- SDLC

The results showed that employees have challenges about understanding cyber security, negative attitudes based on shared culture in the workplace and perceptions centred around fear or past experiences. However, developers do not establish these factors or what the dynamics of the client environment is, so they blindly develop training without understanding the target audience needs. To rectify this, Knowles (1978) suggests learners should establish training objectives, and equally be involved in building training. This should be enhanced by adopting the Software Development Life Cycle (SDLC). The SDLC model describes each step of a software development project, from planning to maintenance (Scroggins, 2014). Although the SDLC is a systems engineering, information systems and software engineering model (Motta et al., 2018), this research suggests it may be applied to cyber security training development. There are various models connect to this process, each of which has a wide range of duties and operations. For example, identification of requirements, architecture, and design, testing and production and maintenance of the application (Mohino et al., 2019). In the requirements phase, the project manager works closely with the customer to gather all the information like what the customer wants to build, who the users will be, the purpose of the product and allocation of the correct resources (Arrey, 2019). Requirements gathered can be in the form of use cases, customer natural language documents, diagrams and flowcharts (Sharma et al., 2014). In addition to this method, one of the ways to gather user requirements is to conduct confidential open-ended interviews, to establish what the organisational cultures are and what challenges employees perceive and experience with training material. A focus group could also be conducted to observe where the influences come from, and to gather a sense of what the organisational culture is to cyber security training. Krueger and Casey (2000, p.25) discuss that focus groups further encourage participants to give genuine information unwittingly through its interactive mechanism, which increases validity. However, a focus group could also hinder employees from being completely honest and feel pressure to give scripted answers. A confidential open-ended interview will allow content developers to delve in on deeper responses to answers, and this would provide a clear picture of the target audience. Rather than adopting a survey to gather business and user challenges, interviews are recommended. This is because surveys limit the depth of information that can be collected, and, surveys are rigid, which means interviewers are unable to probe certain responses. For example, Sebastian, (2021) conducted an exploratory survey on the perceptions regarding the inclusion of security and privacy by design, and one of the questions were 'Does your company require you to document security requirements along with Functional requirements in the Business requirement document?'. While this is a good question, a survey gives the employee a Boolean response, i.e., yes or no. A subset of algebra called Boolean, often known as Boolean logic, is used to formulate true or false propositions (Warshall, 1962). This means the participant may only answer yes or no, and therefore unable to further describe why their answer is yes or no. On the other hand, if the interviewee responded with a 'No', an open-ended interview will enable the interviewer to ask, 'why' their response is 'No' and further investigate if there are conditions surrounding the participants response. In cyber security training surveys for evaluation and feedback appear to be the sole way to get information about users' learning experiences. Korpela (2015) investigated ways to improve cyber security awareness and training programs with data analytics, and discussed that survey's has the drawback that, in most cases, only engaged end users respond to it, leaving the unconnected and disengaged end users. Security awareness and training metrics can aid an organisation by giving it a better grasp of the attitudes and behaviours of its users in the context of their activities, but they are unable to give it a fuller and more nuanced understanding of how those users learn (McIlwraith, 2021).

In addition to this, the content developers should interview awareness professionals to identify from their perspective what challenges they perceive employees have with cyber security. Any disparities from the groups, should be addressed in a separate interview or discussion with the groups. For example, the results showed that awareness professionals believed that employees are driven by fear and have a nonchalant attitude. Though in some regards the assumptions are correct, there are contingent factors to these attitudes. For instance, the results showed that some nonchalant attitudes are as a result of believing they are exempt from a breach and flawed training content that does not represent the business or issues they experience. However, the awareness professionals believe the attitudes come from employees wanting to quickly complete a task. Conducting an interview will highlight disparities between assumptions and beliefs awareness professionals have about employees, and what employees actually experience, in doing so awareness professionals will understand employees more, and employees will feel valued when their opinions are heard and acknowledged. However, this is a time-consuming process because the content developer would need to schedule these interviews with businesses, and this may be subject to availability. In addition to this, there are financial factors, that could prohibit the flexibility of conducting the interviews. For example, if the content developer schedules interviews with businesses residing in another city, and they want to continue interviews based on initial findings. The distance between the content developer and the business, could be a hindrance, especially, if the business is unavailable for follow-up interviews. On the other hand, the content developer could conduct a video interview, and does not need to consider aspects like travel, distance or safety (Gray et al., 2020). Depending on how the participant is positioned in front of the camera, the interviewer can see and observe the subject fully or partially and understand facial expressions, body language, and to some extent other non-verbal cues. However, there are some restrictions that require attention. For video interviews, dependable gear is needed, including a steady internet connection and a high-quality camera (Saarijärvi and Bratt, 2021).

8.1.1.2 Recommendation 2: Evaluation

The results showed that content developers rarely design training with evaluation. The recommendation is to develop evaluation techniques to identify if training successfully established its objectives. A recommended model is the Context, Input, Process and Product Evaluation Model (CIPP) the model starts by assessing the target audience and their needs, the next step identified the stakeholders and cultural context of the business, and the third stage includes process evaluation and this is where the program is assessed with the focus on continuous improvement. The final stage is the process evaluation provides opportunities to periodically evaluate how well and appropriately the project is being carried out. Product evaluation detects and rates anticipated and unintended project outcomes. significant (Zhang et al., 2011). A variety of procedures, according to Stufflebeam and Shinkfield (2007), should be utilised to evaluate a wide range of results. By doing this, the various findings may be cross-checked. For example, case studies, hearings, focus groups, document retrieval and analysis, analysis of photographic records, achievement tests, rating scales, trend analysis of longitudinal data, longitudinal or cross-sectional cohort comparisons, and comparisons of project costs and outcomes are just a few of the many techniques that can be used to evaluate products. In doing this, there is a constant evaluation to ensure parties of the training are content and that training content achieves its aims (Stufflebeam, 2003). However, if after product evaluation training appears to be ineffective, the Incremental Software Life Cycle Model (ISLC) may be adopted. The model emphasises an initial, basic implementation that then gradually adds more complexity and a wider feature set until the final system is finished. The term "incremental development" is also frequently and interchangeably used when describing the iterative technique to describe the incremental changes made during the design and implementation of each new iteration (Alshamrani and Bahattab, 2015). Regarding cyber security training, the iterative process would produce a new version of training, after testing and implementation. At each iteration, design modifications are made, and new functional capabilities are added (Adenowo and Adenowo, 2013).

8.1.1.3 Recommendation 3: Develop relevant training.

One of the characteristics of adult learning is ‘adults are relevancy oriented’ (Knowles, 1978). That is, adults must identify a reason for learning something. Learning must be applied to their work or other responsibilities to be of value to them. Therefore, instructors must identify objectives (Lieb, 2005) for adult participants before the course begins. This means that theories and concepts must be related to a setting familiar to participants. For example, if an employee is handling money in a firm, the training should present a similar environment. This need can be fulfilled by letting participants choose projects that reflect their interests (Collins, 2004). The content developers develop training based on what they think clients need to know and not what they need to know. The third recommendation is to develop relevant training for each client they deliver training to. Based on Knowles (1978) principles, if training objectives ought to be outlined for a particular client, this means objectives would change from business to business. For example, a care home facility may need certain training about General Data Protection Regulation (GDPR) (Dewsbury and Dewsbury, 2017), as they handle client records, whereas a financial firm may need certain training of money laundry, fraud or business email compromise (BEC) (Zweighaft, 2017). Therefore, content developers should develop bespoke training for each client, rather than the blanket training they use for all clients.

8.1.1.4 Recommendation 4: Understanding by Design (UbD)

A plethora of methods and tools can be put into practice to sustain a developer's professional development, one of which is Understanding by Design (UbD). UbD is described as an approach to designing curriculum to allow instructors to focus on the desired learning outcomes and provide structure for student learning (Wiggins, 2011). Wiggins (2011) argue that backward design is focused primarily on student learning and understanding, rather than the learning process. When teachers are designing lessons, units, or courses, they often focus on the activities and instruction rather than the outputs of the instruction.

One of the benefits of UbD is its ability to continue the developer's professional development (Brown, 2004) and ensure students' understanding (Wiggins, 2011). The main point of UbD is to focus on all learners and pay attention to their learning preferences by mitigating learning that happens incidentally. While doing this, the conducted training is made in good design and instructional priorities are determined. These aims can be used as a tool for both increasing students' academic achievement and sustaining teachers' development throughout their professional lives (Wiggins, 2005). Similarly, in a cyber security training context if training aims are to train users on what to look for in a suspected phishing email, the training should tailor learning preferences for participants. For example, a live demonstration or a hands-on task. It is reasonable to draw insight from this domain as it addresses training and knowledge sustainability in the school environment, which is a challenge this research has identified with cyber security training.

8.2 Awareness professional

8.2.1 Manager support

The results showed that managers rarely support employees to use cyber secure methods of working, instead there is a haphazard approach if there is a breach. This is supported by Odlyzko, (2019) who researched the importance of cyber security and mentioned that a security breach is addressed when it happens, rather than prepare for when it happens. The first recommendation is that awareness professionals should actively support employees, through regular meetings with groups and individuals, actively send relevant information to employees and set the atmosphere for group training Rogers (1969). In structuring a workplace environment that promotes the value of intrinsic motivators, leaders must first understand which intrinsic motivators drive the individuals in their department (Itri et al., 2019). Eraut et al. (2001) examined the impact of the manager on learning in the workplace, and they discussed that the key person is the local manager whose management of people and role in establishing a climate favourable to learning, in which people seek advice and help each other learn quite naturally, is critical for those who are managed. They added that negative models could be a source of learning as well as positive models and often are elements of both. Managerial support (for example, encouraging trainees to use new skills and tolerating mistakes when they are practising them) has been identified as a key environmental variable affecting transfer (Ford et al., 1992) and is likely to be of central importance in creating a “transfer friendly” environment (Axtell et al., 1997). Similarly, Marx (1982) suggests that during the initial phases of transfer, when more errors are likely to occur, reinforcement from managers may be particularly critical in helping trainees to maintain the new skills. To create relevant information security policies and to inspire people to abide by them, managerial attention is required. Managers should place emphasis on outlining policies and those policies are assessed for non-compliance, whereas lessening the importance of rewards (Boss et al., 2009).

8.2.1.1 Budget

The awareness professionals discussed that finances are limited, so in the exception of one professional who have found training for themselves have to sacrifice this because there is simply limited budget. The overall attitudes of the awareness professionals suggest, cyber security is a one-off exercise (Stefaniuk, 2020) and there is little to no need for cyber security in the long run, this could explain why there is no allocated budget for security because there is no security culture. Therefore, a suggestion would be to address this attitude, so awareness professionals see the need for security and perhaps apply for SME funding available by local councils and government bodies. In addition to this, the awareness professionals should communicate these finance needs with management and finance directors, to ensure security is part of business expenditure.

8.3 Employees

Metalidou et al. (2014) suggest users are unintentional threats, because of human errors they deposit into an organisation. However, the results show that some employees had a positive attitude to security, they refused to cut corners, and, in some cases, they were the ones teaching and informing Awareness professionals of risks and threats. The recommendation is for employees to feel confident to share challenges they experience with security (Li et al., 2019). However, this is contingent on awareness professionals to provide this space and encourage such culture in the workplace.

8.4 Chapter Summary

In this Chapter, there is a proposed solution to address the challenges each interview group expressed. The Chapter starts by highlighting that content developers take mix and match approach when selecting and developing training for clients. Consequently, solutions to address this such as Software Development Life Cycle (SDLC) and training testing were proposed. The next solution addressed awareness professionals centring support and budget, and lastly, employees were supported with advice to share concerns they feel about cyber security.

Chapter 9 Conclusion

This Chapter will conclude the thesis by summarising the key research findings concerning the research aims and questions and discussing the value and contribution thereof. It will also review the limitations of the study and propose opportunities for future research. The thesis initiated its aims in Chapter 2 Literature Review. This Chapter demonstrates how each aim was achieved in the research. The first aim is to:

1. To identify the procedures and processes content developers take to create and deliver cyber training.

The results indicate that content developers sift through a range of reputable open-source training material to assess what they assume will best fit. The material is then repurposed and packaged for intended clients. Further findings show that content developers rarely test training, nor does it go through any quality control to ensure it meets client needs and concerns. The second aim is:

2. To identify what factors, affect users from learning and changing behaviour.

The results indicate that employees engage with various job tasks which require time, focus and attention, however, this limits their interest and attention to training. They added that manager support through positive behaviour modelling is a factor that impacts behaviour. Further findings show that organisational culture, internal motivation and training design affect employees learning security training and in the long-term changing behaviour. The third aim is:

3. To identify any communication between content developers, end users or awareness professionals.

The results indicate that awareness professionals seek training without discussing it with employees, so therefore their needs are not highlighted or heard. Content developers also develop training based on assumptions, without defining learning objectives with awareness professionals or employees. Further findings show that employees are rarely opportune to share concerns about cyber security training, or challenges they experience with it. This shows there is a gap in communication between each of these groups, as content develops develop what they think people should know, but this differs from the recipients' reality. The final aim is:

4. To understand challenges SMEs, have with cyber training.

The results indicate that SMEs are financially limited to select bespoke training that would specifically address their own business needs. Further findings show that SMEs believe cyber security training is for larger businesses because they have more assets, and so there is a general distaste for cyber security. Findings also show that training is often irrelevant and covers topics that do not apply to SME settings, this could be because SMEs are financially limited and opt for what is available rather than what is suitable.

9.1 Research contribution

In this research the concept of cyber security content developers is explored. While other researchers may have investigated how content developers contribute to the employees learning experience, to the knowledge of this research, this is not a heavily researched topic. This is supported by the fact that in the literature there are no objective definitions of who they are or what they do. This research highlights an essential domain which is the selection and development of training, and findings show that this area is rarely evaluated. Akin to this, the research highlights disparities between how training should be selected (Knowles, 2014; Rogers, 1969) and how training is selected.

Previous research has tended to focus on flaws within human nature and labelling users as unintentional threats (Khan et al., 2021), rather than identifying psychological factors that may impact learning, like individual working memory, short and long-term memory, and motivation. This research contributes to the body of knowledge by adding factors like manager support, peer influence, organisational culture and training design (7.2), which seem to all impact the perception, attitude and motivation toward learning cyber security training. In light of this, the research shifts away from blaming users, to focusing on user-centred design (UCD) (Gulliksen et al., 2003). For example, active user involvement, both and continuously throughout the entire development and process of specifying what delivery style is used, what training material is incorporated and what involvement learners have in the development of training Chammas et al., 2015). One of the benefits of UCD is that it gives designers focus on the users and their needs in each phase of the design process. Adopting this method, alongside andragogy (Knowles, 1978) would effectively develop a rapport between content developers, awareness professionals and employees. It would in turn develop an impactful training for employees, because of the mutual understanding and communication between each andragogic step.

The research contributed by identifying a link between these three groups: content developers, awareness professionals and employees. Though this may go without saying, the current research does not identify these three groups as needed participants for successful training material. Furthermore, the research also highlights a disconnect between these groups, as it highlights there is little to no communication and there no measure to ensure each group's needs are met. This research bridges this gap by developing a research based framework for designing bespoke training packages for businesses (Chapter 8 Proposed Solution to Designing a training package). The framework builds on work from (Knowles, 2014; Rogers, 1969; Mujtaba, 2004) as it incorporates involving learners in the development of training and it provides methods in which awareness professionals should ensure a positive training experience.

9.2 Project Limitations

As indicated in Original Research Question 3.1.1 the project encountered certain limitations which altered the overall research methodology and the approach taken to acquire results. The original project plan was a wider project with the Dorset Growth Hub, and it aimed to capture preliminary habits and behaviours towards cyber security and Information Assurance. The project was cancelled, however, the literature review process produced useful foundational knowledge about perception, habits and attitudes. The research project took its initiative by informally interviewing 4 SME owners. The interviews centred findings on the foundational knowledge acquired from the literature review process, for example, questions around attitudes, rewards and punishments and social influence.

In Chapter 4 a larger project arose and allowed the opportunity to collect data for the research. The original project aimed to conduct a webinar and use a Randomised Controlled Trial (RCT) to examine the impact and value of an innovative behavioural change treatment focused on cyber and data management learning and video delivery techniques. The research question was 'Does the deployment of a cyber game with nudge learning increase the cyber and data knowledge resilience in SMEs?'. However, this changed due to COVID-19 and instead looked at productivity at work during COVID-19, by conducting a survey and interview after completing a training video. One of the limitations of the reformed project is that COVID-19 impacted the data sample size from 300 to 67. This meant that only descriptive analysis could be conducted, and no inferential analysis could not be conducted because of a low sample size. In addition, the interviews were not solely related to the research, which meant there were specific research questions.

In Study 2 (6.1.1.1) there were challenges in recruiting content developers in the UK. This could suggest that content developers are scarce in the UK and supports the fact that there are no objective definitions of what a cyber security content developer is. As a result, a recruitment flyer was designed to help recruit potential participants. This was shared globally across social media like Twitter and LinkedIn, and received a successful response rate, as content developers from Nigeria reached out to participate.

In the same vein, when recruiting awareness professionals, participants from Study 1b were invited, however, due to COVID-19 they responded to say that participating was not a business priority. One of the ways to mitigate this limitation was to Google search businesses in 'Silicon Valley'. Although two business owners responded, it did not lead to an interview. The next approach was to design another recruitment flyer for awareness professionals and employees. The flyer was distributed across Heads of Departments at Bournemouth University. This had success, however, after 6 employee interviews, the themes appeared to be similar. For example, the participants that came from both HR and Finance, shared similar security behaviours i.e., they were both behaving securely due to handling student records and finances.

In terms of data analysis in Figure 13 the data was analysed by typing the code label beside the data in an electronic version of the dataset formatted into a two-column table (Braun and Clark, 2006). While there a several ways to code data, this method was time consuming as it required manual coding and analysis to derive the themes. To add to this, there could be a potential that other vital factors that attribute to learning were missed, because transcribing, coding and analysing are manual processes. The results showed there were some disparities between the younger generation's beliefs and attitudes, in comparison to the older generation. For example, the younger generation identified that the older generation seems to have a lapsed attitude to security, whereas the younger generation generally has a positive security outlook because of the daily use of technology. This point was briefly highlighted in (7.2

Thematic analysis of Employee Interviews), however taking a software program approach would have assisted the coding process.

9.3 Future work

Building on study 1a of the research, future work would entail the recruitment of an increased sample size. To achieve this, a survey would be conducted on Prolific, an online platform that launches studies and recruits trusted participants. In so doing, inferential analysis can be conducted, instead of only descriptive analysis.

Future work would merge parts of study 1a (the cancelled cyber game) to study 2 (the interview). This is due to commonalities between studies, for example, in both studies, attention, and memory were highlighted factors that contribute to motivation for learning cyber security training. The future work would merge the cyber game (which was cancelled due to COVID-19) and the interview element in the study and this would involve employees participating in a cyber game while their eyes are tracked using an eye-tracking machine. The purpose of this would be to identify and measure, where their eyes go to during the cyber game, whether it is on the screen or off the screen, or if their eyes gaze on one part of the game longer than another area (Dalmaijer, 2014). The employees would have a follow up interview to further investigate what their thoughts were during the training, and question why they had more gaze on a particular part of the training, than another. Adopting this would create representative and accurate data which allows the research to better understand students and design meaningful experiences for them (Sharma et al., 2020).

As highlighted in 9.2 (Project Limitations), most of the recruited employees came from either HR or the Finance team. While they gave informative responses, after 6 interviews there was data saturation, where similar themes were highlighted across the interviews. In future work, the sample demographics would expand beyond one department, to several industry types like the hospital, charity shops, and the police unit. This would highlight a range of different challenges, needs, motivations, and attitudes towards cyber security. This would give the analysis a robust output, as different responses can be compared based on demographics and location. This was not highlighted in this research.

In 9.2 (Project Limitationss), it was mentioned the data was analysed by typing the code label beside the data in an electronic version of the dataset formatted into a two-column table. However, there is a likelihood that key themes were missed due to manual coding and analysis. In future work, the analysis would take a different approach by using NVivo. NVivo saves researchers from time-consuming transcription and boosts the accuracy and speed of the analysis process (Zamawe, 2015). In future work, NVivo would organise demographic data, for example, age and gender. This would take the analysis further by ascribing certain responses to certain gender and ages, this way a higher level of comparison can be made about demographics from different departments.

The thesis answered the research questions, however, the research identified there are still unanswered questions that future work would aim to address. For example, a common theme across this research is organisational culture, and the Literature Review Chapter 2 proposes there is no universal definition of what this is. One of the future directions would be to research what components compose of organisational culture and identify how and if it can be measured. Additionally, the results demonstrated that employees are influenced by what their managers portray as a norm, which in turn is culture (Abid et al., 2014). One of the future research questions would investigate 'how managerial influence impact organisation culture? In future work, if NVivo is adopted, there could be more research on the disparities between the older generation and the younger generation learning cyber security. For example, the participants that highlight a difference in attitude and approach from an older employee and a younger employee, could further engage in subsequent interviews so they can share observations and experiences. In doing so, the use of personas would demonstrate how these strategies can be applied. Ki-Aries and Faily (2017) suggest current security awareness strategies fall short of this need of designing for the user. An opportunity to investigate Human Computer Interaction (HCI) strategies that could be implemented into a security awareness approach is provided as a way to close this gap. To address this future work would propose to answer, 'how does gender differences impact adult learning'?

References

Abid Alvi, H., Hanif, M., Adil, M.S., Ahmed, R.R. and Vveinhardt, J., 2014. Impact of Organizational Culture on Organizational Commitment and Job satisfaction. *European Journal of Business and Management. New York, NY: International institute for Science, Technology and Education (IISTE), Vol. 6, no. 27, 2014*.

Adams, M. and Makramalla, M., 2015. Cybersecurity skills training: an attacker-centric gamified approach. Technology Innovation Management Review, 5 (1).

Adenowo, A.A. and Adenowo, B.A., 2013. Software Engineering Methodologies: A Review of the Waterfall Model and Object-oriented Approach. *International Journal of Scientific & Engineering Research*, *4*(7), pp.427-434.

Alahmad, M., 2020. Strengths and weaknesses of cognitive theory. Budapest International Research and Critics Institute-Journal, 3(3), pp.1584-1593.

Alami, H., Gagnon, M.P., Ahmed, M.A.A. and Fortin, J.P., 2019. Digital health: Cybersecurity is a value creation lever, not only a source of expenditure. Health Policy and Technology, 8(4), pp.319-321.

Allen, J.H., Crabb, G., Curtis, P.D., Fitzpatrick, B., Mehravari, N. and Tobar, D., 2015. Structuring the chief information security officer organization. CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States.

Alsalamah, A. and Callinan, C., 2021. Adaptation of Kirkpatrick’s Four-Level Model of Training Criteria to Evaluate Training Programmes for Headteachers. Education Sciences, 11(3), p.116.

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

Alshamrani, A. and Bahattab, A., 2015. A Comparison between three SDLC Models Waterfall Model, Spiral Model, and Incremental/Iterative Model. *International Journal of Computer Science Issues (IJCSI)*, *12*(1), p.106.

Ameen, N., Tarhini, A., Shah, M.H., Madichie, N., Paul, J. and Choudrie, J., 2021. Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Computers in Human Behavior, 114, p.106531.

Andersen, P.H. (2005), “Relationship marketing and brand involvement of professionals through web-enhanced brand communities: the case of Coloplast”, Industrial Marketing Management, Vol. 34 No. 1, pp. 39-51.

Arrey, D.A., 2019. *Exploring the Integration of Security into Software Development Life Cycle (SDLC) Methodology* (Doctoral dissertation, Colorado Technical University).

Association for Psychological Science - APS. 2009. Learning Styles Debunked: There is No Evidence Supporting Auditory and Visual Learning, Psychologists Say. [online] Available at: <https://www.psychologicalscience.org/news/releases/learning-styles-debunked-there-is-no-evidence-supporting-auditory-and-visual-learning-psychologists-say.html> [Accessed 24 November 2021].

Axtell, C., Maitlis, S. and Yearta, S., 1997. Predicting Immediate and Longer-term Transfer of Training. Personnel Review, 26(3), pp.201-213.

B. Guttman and E. A. Roback, An Introduction to Computer Security: The NIST handbook. DIANE Publishing, 1995.

Baldwin, T. T. & Karl, K. A. (1987). The Development and Empirical Test of a Measure for Assessing Motivation to Learn in Management Education. Pp. 117-l 21 in F. Hoy (Ed.), Proceedings of the 47th Annual Meeting of The Academy of Management. New Orleans, LA.

Baldwin, T. T., Magjuka, R. J. St Loher, B. T. (1991). The Perils of Participation: Effects of Choice of Training on Trainee Motivation and Learning. Personnel Psychology, 44: 51-65.

Baldwin, T.T. and Ford, J.K., 1988. Transfer of training: A Review and Directions for Future Research. Personnel Psychology, 41(1), pp.63-105.

Baldwin, T.T., Magjuka, R.J. and Loher, B.T., 1991. The Perils of Participation: Effects of Choice of Training on Trainee Motivation and Learning. Personnel Psychology, 44(1), pp.51-65.

Bandura, A. (1986). Social Foundations of Thought and Action. Englewood Cliơs, NJ: Prentice-Hall.

Bandura, A. (2004). Health Promotion by Social Cognitive Means. *Health Education & Behavior*, *31*(2), 143-164.

Bandara, I., Ioras, F. and Maher, K., 2014. Cyber Security Concerns in e-Learning Education.

Beautement, A., Becker, I., Parkin, S., Krol, K. and Sasse, A., 2016. Productive security: A Scalable Methodology for Analysing Employee Security Behaviours. In Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016) (pp. 253-270).

Bedi, A., 2004. An Andragogical Approach to Teaching Styles. Education for Primary Care, 15(1), pp.93-97.

Bell, K., Fahmy, E. and Gordon, D., 2016. Quantitative Conversations: The Importance of Developing Rapport in Standardised Interviewing. Quality & quantity, 50(1), pp.193-212.

Bench, S.W. and Lench, H.C., 2013. On the Function of Boredom. Behavioral Sciences, 3(3), pp.459-472.

Beyer, R.E. and Brummel, B., 2015. Implementing effective cyber security training for end users of computer networks. Society for Human Resource Management and Society for Industrial and Organizational Psychology.

Bhatti, M.a. and Aldossary, M.a., 2021. Faculty Development through Training Effectiveness: Role of Training Contents, Social Support and Instrumentality. Eurasian Journal of Educational Research, 96(96), pp.170-181.

Bhatti, M.A., Battour, M.M., Sundram, V.P.K. and Othman, A.A., 2013. Transfer of training: does it truly happen? An examination of support, instrumentality, retention and learner readiness on the transfer motivation and transfer of training. European Journal of Training and Development, 37(3), pp.273-297.

Boerman, S.C., Kruikemeier, S. and Zuiderveen Borgesius, F.J., 2021. Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), pp.953-977.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W., 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), pp.151-164.

Bowers, B., Cohen, L.W., Elliot, A.E., Grabowski, D.C., Fishman, N.W., Sharkey, S.S., Zimmerman, S., Horn, S.D. and Kemper, P., 2013. Creating and Supporting a Mixed Methods Health Services Research Team. *Health Services Research*, *48*(6pt2), pp.2157-2180.

Brau, B., 2020. Constructivism. The Students' Guide to Learning Design and Research.

Breed, A., Fouché, N., Brink, N., Coetzee, M., Erasmus, C., Kapp, S., Pilon, S., Wierenga, R. and van Huyssteen, G., 2021. Content Developers as Stakeholders in the Blended Learning Ecosystem: The Virtual Institute for Afrikaans Language Education Portal as a Case Study. In Re-Envisioning and Restructuring Blended Learning for Underprivileged Communities (pp. 124-142). IGI Global.

Brookes, D.R., 2019. Shame vs. Guilt: Is there a difference?

Brooks, D.J., 2022. Intrusion Detection Systems in Physical Security. In The Handbook of Security (pp. 681-703). Palgrave Macmillan, Cham.

Bruhn, M., Schoenmueller, V. and Schäfer, D.B. (2012), “Are social media replacing traditional media in terms of brand equity creation?”, Management Research Review, Vol. 35 No. 9, pp. 770-790.

Bruner, J.S., 1961. The act of discovery. Harvard educational review.

C. Ruiter, R.A. and Kok, G., 2005. Saying is not (always) doing: Cigarette warning labels are useless. The European Journal of Public Health, 15(3), pp.329-329.

Camp, M.D., 2011. *The power of teacher-student relationships in determining student success*. University of Missouri-Kansas City.

Čeleda, P., Čegan, J., Vykopal, J. and Tovarňák, D., 2015. Kypo–a platform for cyber defence exercises. M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization.

Celestin, B.N. and Yufen, S., 2018. The Influence of Pre-training Factors on Motivation to Transfer Learning at the Post Training Stage. Human Resource Research, 2(1), pp.1-17.

Chammas, A., Quaresma, M. and Mont’Alvão, C., 2015. A closer look on the User Centred design. *Procedia Manufacturing*, *3*, pp.5397-5404.

Chan, S., 2010. Applications of Andragogy in multi-disciplined Teaching and Learning. Journal of Adult Education, 39(2), pp.25-35.

Charmaz, K., 2000. Grounded theory: Objectivist and Constructivist methods. Handbook of Qualitative Research, 2, pp.509-535.

Chene, A. (1983). The concept of Autonomy in Adult Education: A Philosophical Discussion. Adult Education Quarterly, 34, 1, 38-47.

Choudhury, G.B. and Sharma, V., 2019. Review and Comparison of Various Training Effectiveness Evaluation Models for R & D Organization performance. PM World Journal, VIII (II). Retrieved from https://pmworldlibrary. net/wp-content/uploads/2019/02/pmwj79-Feb2019-Choudhury-Sharma-comparison-of-training-effectiveness-models-for-rd. pdf.

Chung, Y., 2013. Trainee Readiness for Diversity Training. Journal of Diversity Management (JDM), 8(2), pp.77-84.

Clardy, A., 2005. Andragogy: Adult Learning and Education at Its Best? Online Submission.

Collins, J., 2004. Education Techniques for Lifelong Learning: Principles of Adult Learning. *Radiographics*, *24*(5), pp.1483-1489.

Colquitt, J.A., LePine, J.A. and Noe, R.A. (2000), “Towards and Integration Theory of Training Motivation: A Meta-analytic Path Analysis of 20 years of Research”, Journal of Applied Psychology, Vol. 85 No. 5, pp. 678-707.

Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D., 2007. A Video Game for Cyber Security Training and Awareness. Computers & Security, 26(1), pp.63-72.

Conner, M. and Norman, P., 2015. EBOOK: Predicting and Changing Health Behaviour: Research and Practice with Social Cognition Models. McGraw-hill education (UK).

Coventry, L., Briggs, P., Blythe, J. and Tran, M., 2014. Using behavioural insights to improve the public’s use of cyber security best practices. Gov. UK report.

Coventry, L., Briggs, P., Blythe, J. and Tran, M., 2014. Using behavioural insights to improve the public’s use of cyber security best practices. Gov. UK report.

Cram, W.A., Proudfoot, J.G. and D'Arcy, J., 2021. When enough is enough: Investigating the antecedents and consequences of information security fatigue. Information Systems Journal, 31(4), pp.521-549.

Cram, W.A., Proudfoot, J.G. and D'Arcy, J., 2021. When enough is enough: Investigating the antecedents and consequences of information security fatigue. Information Systems Journal, 31(4), pp.521-549.

Crawley, K., 2020. Cybersecurity budgets explained: how much do companies spend on cybersecurity?. [online] Available at: <https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget> [Accessed 5 November 2021].

Çubukçu, C. and Aktürk, C., 2020. The rise of distance education during covid-19 pandemic and the related data threats: a study about zoom. Igd Univ Jour Soc Sci,(Ek2), pp.127-143.

Dalkey, N. and Helmer, O., 1963. An experimental application of the Delphi method to the use of experts. Management science, 9(3), pp.458-467.

Dalmaijer, E., 2014. Is the low-cost EyeTribe eye tracker any good for research? (No. e585v1). PeerJ PrePrints.

Dantas, L.A. and Cunha, A., 2020. An Integrative Debate on Learning Styles and the Learning Process. *Social Sciences & Humanities Open*, *2*(1), p.100017.

Daswani, N. and Elbayadi, M., 2021. The Marriott Breach. In Big Breaches (pp. 55-74). Apress, Berkeley, CA.

De Crescenzo, S. (2016, September 5). A new kind of Policy to Safeguard Small Business Finances: New insurance may protect companies from cybersecurity losses. San Diego Business Journal, 37(36), 18. Retrieved from https://search.proquest.com/docview/1818681665?accountid=28902

De Jaegher, H., 2020. Seeing and inviting participation in autistic interactions. Transcultural Psychiatry, p.13634615211009627.

De Vicente Mohino, J., Bermejo Higuera, J., Bermejo Higuera, J.R. and Sicilia Montalvo, J.A., 2019. The application of a new secure Software Development Life Cycle (S-SDLC) with Agile Methodologies. *Electronics*, *8* (11), p.1218.

Decker, P.J. (1982), "The enhancement of Behaviour modelling training of supervisory skills by the inclusion of retention processes", Personnel Psychology, Vol. 32, pp. 323-32.

DeJonckheere, M. and Vaughn, L.M., 2019. Semistructured interviewing in primary care research: a balance of relationship and rigour. Family medicine and community health, 7(2).

Dennis, A., Wixom, B. and Tegarden, D., 2015. Systems Analysis and Design: An Object-Oriented Approach with UML. John Wiley & Sons.

Dewsbury, G. and Dewsbury, D., 2017. Securing IT infrastructure in the care home. *Nursing And Residential Care*, *19*(12), pp.672-674.

Dolan, P., Hallsworth, M., Halpern, D., King, D. and Vlaev, I., 2010. MINDSPACE: Influencing Behaviour for Public Policy.

Duhachek, A., Agrawal, N. and Han, D., 2012. Guilt versus Shame: Coping, Fluency, and Framing in the Effectiveness of Responsible Drinking Messages. Journal of Marketing Research, 49(6), pp.928-941.

Dupuis, M. and Renaud, K., 2021. Scoping the Ethical principles of Cybersecurity Fear appeals. Ethics and Information Technology, 23(3), pp.265-284.

Ec.europa.eu. 2021. Glossary: Vocational education and training (VET) - Statistics Explained. [online] Available at: <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Vocational_education_and_training_(VET)> [Accessed 23 January 2022].

Ertan, A., Crossland, G., Heath, C., Denny, D. and Jensen, R., 2020. Cyber security Behaviour in Organisations. arXiv preprint arXiv:2004.11768.

Eseryel, D., 2002. Approaches to Evaluation of Training: Theory & Practice. Journal of Educational Technology & Society, 5(2), pp.93-98.

Fabro, M., Gorski, E., Spiers, N., Diedrich, J. and Kuipers, D., 2016. Recommended Practice: Improving Industrial Control System Cybersecurity with Defence-in-depth strategies. DHS Industrial Control Systems Cyber Emergency Response Team.

Faily, S. and Fléchais, I., 2010. Designing and Aligning e-Science Security Culture with design. Information Management & Computer Security

Ference, E.A., 1982. Human-Ressources Development: Toward a Definition of Training. Cornell Hotel and Restaurant Administration Quarterly, 23(3), pp.25-31.

Ferreira, D., MacLean, G. and Center, G.E., 2018. Andragogy in the 21st century: Applying the assumptions of Adult Learning Online. Language Research Bulletin, 32(1).

Fogg, B.J., 2002. Persuasive technology: Using Computers to Change What we Think and do. Ubiquity, 2002(December), p.2.

Ford, J.K., Quinones, M., Sego, D. and Sorra, J. (1992), “Factors Affecting the Opportunity to perform trained tasks on the job”, Personnel Psychology, Vol. 45, pp. 511-27.

Friborg, O. and Rosenvinge, J.H., 2013. A comparison of open-ended and closed questions in the prediction of mental health. Quality & Quantity, 47(3), pp.1397-1411.

Furman, S., Theofanos, M.F., Choong, Y.Y. and Stanton, B., 2011. Basing cybersecurity training on user perceptions. IEEE Security & Privacy, 10(2), pp.40-49.

Furnell, S. and Vasileiou, I., 2017. Security education and awareness: just let them burn?. Network Security, 2017(12), pp.5-9.

Furnell, S. and Thomson, K.L., 2009. Recognising and addressing 'security fatigue'. Computer Fraud & Security, 2009(11), pp.7-11.

Georgiadou, A., Mouzakitis, S. and Askounis, D., 2021. Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal, pp.1-20.

Gervais, J., 2020. Beware Of These Coronavirus Scams. [online] Us.norton.com. Available at: <https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html> [Accessed 1 September 2020].

Ghazvini, A. and Shukur, Z., 2016. Awareness Training Transfer and Information Security Content Development for Healthcare Industry. International Journal of Advanced Computer Science and Applications, 7(5), pp.361-370.

Goldstein, I. L. (1991). Training in work organizations. In M. D. Dunnette & L. M. Hough (Eds.), Handbook of Industrial and Organizational Psychology (2nd ed.; pp. 507–620). Palo Alto, CA: Consulting Psychologists Press.

Gomez, Joshua, Travis Pinnick, and Ashkan Soltani. "KnowPrivacy." (2009).

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Sohail, T., 2006. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. Journal of Accounting and Public Policy, 25(5), pp.503-530.

Gray, L.M., Wong-Wylie, G., Rempel, G.R. and Cook, K., 2020. Expanding qualitative research interviewing strategies: Zoom video communications. *The Qualitative Report*, *25*(5), pp.1292-1301.

Hamblin, A.C., 1974. Evaluation and Control of Training. Industrial Training International, 9(5), pp.154-6.

Hash, J. and Wilson, M., 2012. Building an information technology security awareness and training program. National Institute of Standards and Technology (NIST), pp.800-50.

Hense, J., & Mandl, H. (2014). Learning in or with Games? In Digital systems for open access to formal and informal learning (pp. 181–193). Springer.

Herath, T. and Rao, H.R., 2009. Encouraging Information Security Behaviours in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), pp.154-165.

Herold, R. (2005). Managing and Information Security and Privacy Awareness and Training Program. Boca Raton, FL, Auerbach Publications.

Holmlund, L., Hellman, T., Engblom, M., Kwak, L., Sandman, L., Törnkvist, L. and Björk Brämberg, E., 2022. Coordination of return-to-work for employees on sick leave due to common mental disorders: facilitators and barriers. Disability and Rehabilitation, 44(13), pp.3113-3121.

Holton III, E.F., 1996. The flawed four-level evaluation model. Human resource development quarterly, 7(1), pp.5-21.

Hommel, B., Chapman, C.S., Cisek, P., Neyedli, H.F., Song, J.H. and Welsh, T.N., 2019. No one knows what attention is. Attention, Perception, & Psychophysics, 81(7), pp.2288-2303.

Hoomans, J., 2015. 35,000 decisions: The great choices of strategic leaders. Leading Edge Journal.

Huang, K. and Pearlson, K., 2019, January. For what technology can't fix: Building a model of organizational cybersecurity culture. In Proceedings of the 52nd Hawaii International Conference on System Sciences.

Huang, K. and Pearlson, K., 2019, January. For what technology can't fix: Building a model of organizational cybersecurity culture. In Proceedings of the 52nd Hawaii International Conference on System Sciences.a

Huczynski, A. and Lewis, J. (1980), "An empirical study into the learning transfer process in management training", Journal of Management Studies, Vol. 17, pp. 227-40.

Hughey, A.W. and Mussnug, K.J., 1997. Designing effective employee training programmes. Training for Quality.

Information Security Forum (ISF).: The Standard of Good Practice for Information Security, Security Standard. 2007

Hultman, K., 2020. Building a Culture of Employee Optimization. *Organization Development Journal*, *38*(2).

Ismail, W.B.W. and Yusof, M., 2018. Mitigation strategies for unintentional insider threats on information leaks. International Journal of Security and Its Applications, 12(1), pp.37-46.

Itri, J.N., Bruno, M.A., Lalwani, N., Munden, R.F. and Tappouni, R., 2019. The incentive dilemma: Intrinsic motivation and workplace performance. Journal of the American College of Radiology, 16(1), pp.39-44.

Kahn, W.A., 2015. The ostrich effect: Solving destructive patterns at work. Routledge.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., and Wei, K. K. 2003. "An Integrative Study of Information Systems Security Effec tiveness," International J

Karmowska, G. and Marciniak, M., 2015. Small and medium-sized enterprises in European union.

Katsikas, S.K., 2000. Health care management and Information Systems Security: Awareness, Training or Education?. International Journal of Medical Informatics, 60(2), pp.129-135.

Katz, I. and Assor, A., 2003. Is autonomy important for non-western students? Examining autonomy as a universal human propensity. In 84th annual meeting of the American Educational Research Association, Chicago.

Kaufman, R. and Keller, J.M., 1994. Levels of evaluation: Beyond Kirkpatrick. Human Resource Development Quarterly, 5(4), pp.371-80.

Khan, N., J Houghton, R. and Sharples, S., 2021. Understanding factors that influence unintentional insider threat: A Framework to Counteract Unintentional risks. Cognition, Technology & Work, pp.1-29.

Khan, N., J Houghton, R. and Sharples, S., 2022. Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks. Cognition, Technology & Work, 24(3), pp.393-421.

Kho, N. (2008), “B2B gets social media”, EContent, Vol. 31 No. 3, pp. 26-30.

Ki-Aries, D. and Faily, S., 2017. Persona-centred Information Security Awareness. Computers & Security, 70, pp.663-674.

Knowles, M.S. (1984). Adult Learning: Theory and Practice. In L. Nadler (ed.), The Handbook of Human Resource Development. New York: John Wiley and Sons. Pages 6.1-6.23

Knowles, M.S. (1987). Adult learning. In R.L. Craig (ed.), Training and Development Handbook. New York: McGraw Hill. Pages 168-179 (3rd ed.).

Knowles, M.S., 1978. Andragogy: Adult learning theory in perspective. Community College Review, 5(3), pp.9-20.

Knowles, M.S., Holton III, E.F. and Swanson, R.A., 2014. The adult learner: The definitive classic in adult education and human resource development. Routledge.

Kolb, A.Y., 2013. The Kolb learning style inventory–version 4.0. a comprehensive guide to the theory, psychometrics, research on validity and educational applications. *Kaunakakai, HI: Experience Based Learning Systems*.

Korpela, K., 2015. Improving cyber security awareness and training programs with data analytics. Information Security Journal: A Global Perspective, 24(1-3), pp.72-77.

Kortjan, N. and von Solms, R., 2013. A cyber security awareness and education framework for South Africa (Doctoral dissertation, Nelson Mandela Metropolitan University).

Kostadinov, D., 2018. The components of a successful security awareness program. InforSec Institute.

Kreuter, M.W. and McClure, S.M., 2004. The role of culture in health communication. Annual review of public health, 25(1), pp.439-455.

Krueger, R.A. and Casey, M.A. (2000), Focus Groups: A Practical Guide for Applied Research, Sage Publications, Los Angeles

Lai, A., 2022. Data security and privacy policies. [online] Otter.ai. Available at: <https://help.otter.ai/hc/en-us/articles/360048258953-Data-security-and-privacy-policies> [Accessed 29 March 2022].

Larson, K., Grudens-Schuck, N. and Allen, B. L., 2004. Methodology brief: Can you call it a focus group?

Leary, M.R., 2022. Emotional responses to interpersonal rejection. *Dialogues in clinical neuroscience*.

Leberman, S. and McDonald, L., 2016. *The transfer of learning: Participants' perspectives of adult education and training*. CRC Press.

Lewis, B.A., Marcus, B.H., Pate, R.R. and Dunn, A.L., 2002. Psychosocial Mediators of Physical Activity Behaviour Among Adults and Children. American Journal of Preventive Medicine, 23(2), pp.26-35.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X., 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour. *International Journal of Information Management*, *45*, pp.13-24.

Lieb, S., 1991. Principles of Adult Learning, Phoenix, AZ: Vision–South Mountain Community College. Retrieved September, 24, p.2014. Behaviour Analyst, 36(2), pp.197-208.

Limayem, M. and Hirt, S.G., 2003. Force of habit and Information Systems Usage: Theory and Initial Validation. Journal of the Association for Information Systems, 4(1), p.3.

Limayem, M. and Hirt, S.G., 2003. Force of Habit and Information Systems Usage: Theory and Initial Validation. Journal of the Association for information Systems, 4(1), p.3.

Luszczynska, A. and Schwarzer, R., 2015. Social Cognitive Theory. *Fac Health Sci Publ*, pp.225-51.

MacLaughlin, E.J., Raehl, C.L., Treadway, A.K., Sterling, T.L., Zoller, D.P. and Bond, C.A., 2005. Assessing medication adherence in the elderly. Drugs & aging, 22 (3), pp.231-255.

Madu, C.O. and Obiozor, O.R., 2012. Conducive learning environment: A panacea for effective learning among adult learners.

Mäläskä, M., Saraniemi, S. and Tähtinen, J., 2011. Network actors' participation in B2B SME branding. *Industrial Marketing Management*, *40*(7), pp.1144-1152.

Manpower Services Commission (1981) Glossary of Training Terms. London: HMSO

Marx R.D. (1982), "Relapse prevention for managerial training; A model for maintenance of behaviour change", Academy of Management Review, Vol. 7 No. 3, pp. 433-41.

Masadeh, M., 2012. Training, Education, Development and Learning: What is the difference?. European Scientific Journal, 8(10).

Mathieu, J. E., Tannenbaum, S. I. & Salas, E. (1992). Influences of Individuals and Situational Characteristics on Measures of Training Effectiveness. Academy of Management Journal, 35: 828-847.

Mathur, M.B. and Reichling, D.B., 2019. Open-source software for mouse-tracking in Qualtrics to measure category competition. Behaviour research methods, 51(5), pp.1987-1997.

Mattar, J. (2018), “Constructivism and Connectivism in Education Technology: Active, Situated, Authentic, Experiential, and Anchored Learning”, RIED Revista Iberoamericana De Educacion a Distancia, Vol. 21 No. 2, pp. 201-217.

Mazzarolo, G. and Jurcut, A.D., 2019. Insider threats in Cyber Security: The enemy within the gates. arXiv preprint arXiv:1911.09575.

McCambridge, J., Witton, J. and Elbourne, D. R., 2014. Systematic review of the Hawthorne Effect: New concepts are needed to Study Research Participation effects. Journal of Clinical Epidemiology, 67 (3), 267–277.

McLeod, C.E.H.J. and King, L.A., 1996. Continuing Professional Development for the Information Discipline of Records Management. Part 1: Context and initial indications of current activities. Librarian Career Development.

McLeod, S.A., 2007. Bf skinner: Operant conditioning. Retrieved September, 9(2009), pp.115-144.

McIlwraith, A., 2021. *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. and Giannakopoulos, G., 2014. The human factor of information security: Unintentional damage perspective. Procedia-Social and Behavioral Sciences, 147, pp.424-428.

Michael E. Whitman, Herbert J. Mattord, Management of Information Security. Canada: Thomson Course Technology, 2004, p. 532.

Moodie, G., 2002. Identifying Vocational Education and Training. Journal of Vocational Education and Training, 54(2), pp.249-266.

Moore, J., 2013. Methodological behaviourism from the standpoint of a radical behaviourist.

Motta, R.C., de Oliveira, K.M. and Travassos, G.H., 2018, September. On challenges in engineering IoT software systems. In *Proceedings of the XXXII Brazilian symposium on software engineering* (pp. 42-51).

Muda, I., Sidauruk, H. and Siregar, H.S., 2018. The Effect of Corporate Social Responsibility on Company's Value with Common Effects Model (CEM), Fixed Effects Model (FEM) and Random Effects Model (REM) Approaches (Empirical Evidence in Indonesia Stock Exchange). Quality-Access to Success, 19(165).

Mujtaba, B., 2004. Faculty Training and Development Practices in Distance Education to Achieve High Performance through Extraordinary Teaching. Journal of College Teaching & Learning (TLC), 1(6).

Musti-Rao, S. and Haydon, T., 2011. Strategies to increase behaviour-specific teacher praise in an inclusive environment. Intervention in School and Clinic, 47(2), pp.91-97.

Nathanson, D., 1992. Affect, sex, and the birth of the self.

NCSC. 2019. Board Toolkit. [online] Available at: <https://www.ncsc.gov.uk/collection/board-toolkit/embedding-cyber-security> [Accessed 8 September 2022].

Ng, B.Y., Kankanhalli, A. and Xu, Y.C., 2009. Studying users' computer security behaviour: A health belief perspective. Decision Support Systems, 46(4), pp.815-825.

Nickerson, R.S., 1998. Confirmation bias: A ubiquitous phenomenon in many guises. Review of general psychology, 2(2), pp.175-220.

Noe, R.A. and Schmitt, N., 1986. The influence of trainee attitudes on training effectiveness: Test of a model. Personnel psychology, 39(3), pp.497-523.

Nowell, L.S., Norris, J.M., White, D.E. and Moules, N.J., 2017. Thematic analysis: Striving to meet the trustworthiness criteria. International Journal of Qualitative Methods, 16(1), p.1609406917733847.

Nurse, J.R., Creese, S., Goldsmith, M. and Lamberts, K., 2011, September. Guidelines for usable cybersecurity: Past and present. In 2011 third international workshop on cyberspace safety and security (CSS) (pp. 21-26). IEEE.Professional, 18(5), pp.26-32.

Overman, S., 1994. Games companies play. HR Magazine, 39(5), pp.61-62.

Pasculli, L., 2020. The global causes of cybercrime and state responsibilities. Towards an integrated interdisciplinary theory. *Journal of Ethics and Legal Technologies*, *2*(1).

Pashler, H., McDaniel, M., Rohrer, D. and Bjork, R., 2008. Learning Styles. Psychological Science in the Public Interest, 9(3), pp.105-119.

Patall, E.A., 2013. Constructing motivation through choice, interest, and interestingness. Journal of Educational Psychology, 105(2), p.522.

Payne, S.L., Flynn, J. and Whitfield, J.M., 2008. Capstone business course assessment: Exploring student readiness perspectives. Journal of Education for Business, 83(3), pp.141-146.

Peker, Y.K., Ray, L., Da Silva, S., Gibson, N. and Lamberson, C., 2016, October. Raising Cybersecurity awareness among college students. In Journal of The Colloquium for Information Systems Security Education (Vol. 4, No. 1, pp. 17-17).

Peltier, T.R., 2005. Implementing an Information Security Awareness Program. Inf. Secur. J. A Glob. Perspect., 14(2), pp.37-49.

Perez, C., 2020. A Cybersecurity Strategy for the Small Business (Doctoral dissertation, Utica College).

Pham, H.C., Pham, D.D., Brennan, L. and Richardson, J., 2017. Information Security and People: A conundrum for compliance. *Australasian Journal of Information Systems*, *21*.

Phillips, J.J., Phillips, P.P. and Hodges, T.K., 2004. Making Training Evaluation Work: Show Value and Communicate Results, Select the Right Model and Find Resources, Get Management Buy-in and Overcome Resistance. American Society for Training and Development.

Phillips, P.P. and Phillips, J.J., 2009. Return on investment. Handbook of Improving Performance in the Workplace: Volumes 1-3, pp.823-846.

Piaget, J. (1957). Construction of reality in the child. London: Routledge & Kegan Paul.

Pieters, W., 2011. The (social) construction of information security. The Information Society, 27(5), pp.326-335.

Pusey, A.E. and Bolhuis, J.J., 2005. The behaviour of animals: mechanisms, function, and evolution.

Reason, J., 2000. Human error: models and management. Bmj, 320(7237), pp.768-770.

Reeves, A., Calic, D. and 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*, p.102281.

Reeve, J. and Cheon, S.H., 2021. Autonomy-supportive teaching: Its malleability, benefits, and potential to improve educational practice. Educational Psychologist, 56(1), pp.54-77.

Reeve, J., Nix, G. and Hamm, D., 2003. Testing models of the experience of self-determination in intrinsic motivation and the conundrum of choice. Journal of educational psychology, 95(2), p.375.

Reiss, S., 2012. Intrinsic and extrinsic motivation. Teaching of psychology, 39(2), pp.152-156.

Renaud, K. and Dupuis, M., 2019, September. Cyber security fear appeals: Unexpectedly complicated. In Proceedings of the New Security Paradigms Workshop (pp. 42-56).

Renaud, K. and Weir, G.R., 2016, August. Cybersecurity and the Unbearability of Uncertainty. In *2016 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 137-143). IEEE.

Renaud, K., Searle, R. and Dupuis, M., 2021, October. Shame in cyber security: effective behavior modification tool or counterproductive foil?. In New Security Paradigms Workshop (pp. 70-87).

Research in practice (2012) Training transfer: Getting learning into practice. Dartington: research in practice

Rhee, H.S., Kim, C. and Ryu, Y.U., 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & security, 28(8), pp.816-826.

Robertson, I. and Downs, S. (1979), "Learning and the prediction of performance: development of trainability testing in the United Kingdom", Journal of Applied Psychology, Vol. 64, pp. 42-55.

Robinson, A., 2013. Using Influence Strategies to Improve Security Awareness Programs. *SANS Institute InfoSec Reading Room*.

Ruiter, R.A., Kessels, L.T., Peters, G.J.Y. and Kok, G., 2014. Sixty years of fear appeal research: Current state of the evidence. International Journal of Psychology, 49(2), pp.63-70.

Rupere, T. and Muhonde, M., 2012. Towards Minizing Human Factors in End-User Information Security.

Ryan, F., Coughlan, M. and Cronin, P., 2009. Interviewing in qualitative research: The one-to-one interview. International Journal of Therapy and Rehabilitation, 16 (6), 309–314

Saarijärvi, M. and Bratt, E.L., 2021. When face-to-face interviews are not possible: tips and tricks for video, telephone, online chat, and email interviews in qualitative research.

Safa, N.S., Von Solms, R. and Furnell, S., 2016. Information security policy compliance model in organizations. computers & security, 56, pp.70-82.

Schein, E.H., 1991. What is culture. Newbury Park, CA: Sage, pp.243-253.

Schunk, Dale H., and Frank Pajares. "Self-efficacy beliefs." (2010): 668-672.

Scroggins, R., 2014. SDLC and development methodologies. *Global Journal of Computer Science and Technology*.

Selznick, L.F. and LaMacchia, C., 2017. Cybersecurity liability: How technically savvy can we expect small business owners to be. J. Bus. & Tech. L., 13, p.217.

Sharma, K., Giannakos, M. and Dillenbourg, P., 2020. Eye-tracking and artificial intelligence to enhance motivation and learning. *Smart Learning Environments*, *7*(1), pp.1-19.

Sharma, R., Gulia, S. and Biswas, K.K., 2014, April. Automated generation of activity and sequence diagrams from natural language requirements. In *2014 9th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE)* (pp. 1-9). IEEE.

Singer, E. and Couper, M.P., 2008. Do incentives exert undue influence on survey participation? Experimental evidence. Journal of empirical research on human research ethics, 3(3), pp.49-56.

Skinner, B.F., 1971. Operant conditioning. The encyclopedia of education, 7, pp.29-33.

Skinner, B.F., 1988. The selection of behaviour: The operant behaviourism of BF Skinner: Comments and consequences. CUP Archive.

Slusky, L., 2020. Cybersecurity of online proctoring systems. Journal of International Technology and Information Management, 29(1), pp.56-83.

Srinidhi, B., Yan, J. and Tayi, G.K., 2015. Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, *75*, pp.49-62.

Stacey FG, James EL, Chapman K, Courneya KS, Lubans DR. A systematic review and meta-analysis of social cognitive theory-based physical activity and/or nutrition behavior change in

Staddon, J.E. and Cerutti, D.T., 2003. Operant conditioning. Annual review of psychology, 54, p.115.

Stanton, B., Theofanos, M.F., Prettyman, S.S. and Furman, S., 2016. Security fatigue. It

Statista. 2021. Share of United Kingdom (UK) businesses where staff have had cyber security training in 2019, by size of business. [online] Available at: <https://www.statista.com/statistics/586594/cyber-security-training-by-united-kingdom-uk-business-by-size/> [Accessed 5 November 2021].

Stefaniuk, T., 2020. Training in shaping employee information security awareness. Entrep. Sustain, 7.

Stufflebeam, D. (2003). The CIPP model of evaluation. In T. Kellaghan, D. Stufflebeam & L. Wingate (Eds.), Springer international handbooks of education: International handbook of educational evaluation. Retrieved from http://www.credo Saarijärvirence.com.ezproxy.lib.ucalgary.ca/entry/spredev/the_cipp_model_for_evaluation

Stufflebeam, D. L., & Shinkfield, A. J. (2007). Evaluation theory, models, & applications. San Francisco, CA: Jossey-Bass.

Taatgen, N.A., 2021. Theoretical models of training and transfer effects. In Cognitive training (pp. 41-54). Springer, Cham.

Tamkin, P., Yarnall, J. and Kerrin, M., 2002. Kirkpatrick and Beyond: A review of models of training evaluation. Brighton, England: Institute for Employment Studies.

Tangney, June Price, Jeff Stuewig, and Debra J. Mashek. "Moral emotions and moral behavior." Annual review of psychology 58 (2007): 345.

Tannenbaum, S. and Yukl, G. (1992), "Training and development in work organizations", Annual Review of Psychology, Vol. 43, pp. 399-441.

Tashakkori, A. and Creswell, J.W., 2007. Exploring the nature of research questions in mixed methods research. *Journal of Mixed Methods Research*, *1*(3), pp.207-211.

Taylor, D.C. and Hamdy, H., 2013. Adult learning theories: implications for learning and teaching in medical education: AMEE Guide No. 83. Medical teacher, 35(11), pp.e1561-e1572.

Terry, G., Hayfield, N., Clarke, V., & Braun, V. (2017). Thematic analysis. In C. Willig, & W. Stainton Rogers (Eds.), The SAGE Handbook of Qualitative Research in Psychology (17-37). (2nd). London: SAGE Publications

Thomas, B., Mimiaga, M.J., Mayer, K.H., Johnson, C.V., Menon, S., Chandrasekaran, V., Murugesan, P., Swaminathan, S. and Safren, S.A., 2009. HIV prevention interventions in Chennai, India: are men who have sex with men being reached?. AIDS patient care and STDs, 23(11), pp.981-986.

Thomson, K.-L. and von Solms, R. (2005), "Information Security Obedience: A Definition", Computers and Security, Vol. 24 No. 1, pp. 69-75.

Tracey, J.B., Hinkin, T.R., Tannenbaum, S. and Mathieu, J.E., 2001. The influence of individual characteristics and the work environment on varying levels of training outcomes. Human resource development quarterly, 12(1), pp.5-23.

Tracey, J.B., Tannenbaum, S.I. and Kavanagh, M.J. (1995), "Applying trained skills on the job: the importance of the work environment", Journal of Applied Psychology, Vol. 80 No. 2, pp. 239-52.

Trainer, A.G., Tongue, B., Heel, E.A. and Outsole, I.D.D.P., Characteristics of.

Uskul, A.K., Sherman, D.K. and Fitzgibbon, J., 2009. The cultural congruency effect: Culture, regulatory focus, and the effectiveness of gain-vs. loss-framed health messages. *Journal of Experimental Social Psychology*, *45*(3), pp.535-541.

Van Bavel, R., Rodríguez-Priego, N., Vila, J. and Briggs, P., 2019. Using protection motivation theory in the design of nudges to improve online security behaviour. International Journal of Human-Computer Studies, 123, pp.29-39.

Verbert, K., Manouselis, N., Ochoa, X., Wolpers, M., Drachsler, H., Bosnic, I. and Duval, E., 2012. Context-aware recommender systems for learning: a survey and future challenges. *IEEE transactions on learning technologies*, *5*(4), pp.318-335.

Vygotsky, L.S. and Cole, M., 1978. Mind in society: Development of higher psychological processes. Harvard university press.

Waite, A., 2010. InfoSec Triads: Security/Functionality/Ease-of-use.

Walker, B.N. and Kramer, G., 2004. Ecological psychoacoustics and auditory displays: Hearing, grouping, and meaning making. In Ecological psychoacoustics (pp. 149-174).

Wang, V.C. ed., 2015. Handbook of research on learning outcomes and opportunities in the digital age. IGI Global.

Wang, Y., Yu, S. and Xu, T., 2017. A User Requirement Driven Framework for Collaborative Design Knowledge Management. Advanced Engineering Informatics, 33, pp.16-28.

Warshall, S., 1962. A theorem on Boolean matrices. *Journal of the ACM (JACM)*, *9*(1), pp.11-12.

Wickström, G. and Bendix, T., 2000. The" Hawthorne effect"—What did the original Hawthorne studies actually show?. Scandinavian Journal of Work, Environment & Health, pp.363-367.

Wiggins, G.P., Wiggins, G. and McTighe, J., 2005. Understanding by design. Ascd.

Wilson, M. and Hash, J., 2003. Building an information technology security awareness and training program. NIST Special publication, 800(50), pp.1-39.

Wilson, M., de Zafra, D.E., Pitcher, S.I., Tressler, J.D. and Ippolito, J.B., 1998. Information technology security training requirements: A Role-and Performance-based Model. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD COMPUTER SECURITY DIV.

Wisdom, J. and Creswell, J.W., 2013. Mixed methods: Integrating Quantitative and Qualitative Data Collection and Analysis while Studying Patient-centered Medical Home Models. Rockville: Agency for Healthcare Research and Quality.

Wong, A., Holmes, S. and Schaper, M.T., 2018. How do small business owners actually make their financial decisions? Understanding SME financial behaviour using a case-based approach. *Small Enterprise Research*, *25*(1), pp.36-51.

Working From Home—COVID19—ENISA. ENISA—European Union Agency for Cybersecurity. Accessed 04 17, 2020. https://www.enisa.europa.eu/topics/wfh-covid19

Zamawe, F.C., 2015. The Implication of using NVivo software in Qualitative Data Analysis: Evidence-based reflections. Malawi Medical Journal, 27(1), pp.13-15.

Zhang, G., Zeller, N., Griffith, R., Metcalf, D., Williams, J., Shea, C. and Misulis, K., 2011. Using the Context, Input, Process, and Product Evaluation Model (CIPP) as a Comprehensive Framework to guide the Planning, Implementation, and Assessment of Service-learning Programs. Journal of Higher Education Outreach and Engagement, 15(4), pp.57-84.

Zhou, M. and Brown, D., 2015. Educational Learning Theories.

Zhuang, J., 2014. Are guilt and shame distinguishable? Exploring persuasive effects of guilt and shame on information processing from two novel dimensions. Michigan State University.

Zimmerman, C., 2014. Cybersecurity operations center. *The MITRE Corporation*.

Zweighaft, D., 2017. Business email compromise and executive impersonation: Are financial institutions exposed?. *Journal of Investment Compliance*.

Appendix A BEIS Interview Questions

The introduction questions will create a narrative of trends and themes across business type, from which conclusions can be drawn.

Introduction Questions

What is the name and nature of your business?

Does this involve dealing directly with the public?

How many work colleagues do you interact with on a daily basis?

What is the set-up of your workplace? Are there people working in the same location as you?

Has this changed due to COVID?

What is your job role?

Does your job involve you doing things outside of your official role?

Does your job include being responsible for cybersecurity?

If not you then is there someone else in your organisation who leads on cybersecurity?

What is your age?

Part 1- Motivation

(**Literature to support question)**

Research depicts that one of the ways to evaluate the effectiveness of training is to establish trainee readiness at the pre-training stage including, motivational, behavioural, and cognitive readiness (Rachmaliya, 2017). Studies into vocational training tend to be more persuasive when there is a match between the recipients cognitive, affective, or motivational characteristics and the content of framing of the message. This suggests the importance of trainee characters, motivation being frequent in studies, it is crucial to understand what the drivers are behind trainee motivation.

One of the benefits of understanding this factor is that, if these drivers are understood by the company, employers can manipulate these drivers to cause favourable motivation towards cyber security.

Question 1 (BCP): What did you like and dislike about the training?

What motivates you to pay attention to cyber security training?

Is there anything about training in general that you find tends to make you disengage?

How interactive did you find the Cyber Well training?

Ideally, what do you think training should look like? What motivates you to use cyber security knowledge at work?

Do you find there are barriers to implementing this knowledge?

Do you feel that there are any gaps in your knowledge that the training did not address?

How do you think cyber security and productivity are linked within the workplace?

How do you think good cyber security habits affect your organisations productivity?

How do you think poor cyber security behaviours affect your productivity at work?

Why do you feel this way?

Do you feel more confident in your reaction to cyber threat as a result of this training?

How do you think the training has affected your ability to deal with a cyber threat?

How do you feel about cyber security after completing the training?

(**Literature to support question)**

Some researchers have attempted to examine the role of peer support and supervisor support in motivation towards learning proposed that peer support can help trainees learn and maintain new skills (Burke-Smalley, 2007).

In addition, research note that supervisors promote training transfer by explaining to their employees their expectations about their post-training behaviour and performance, by helping them identify opportunities for the implementation of learning, and by providing information that is helpful to employees. The support offered by supervisors seems to be of crucial importance when employees encounter problems while using new knowledge (Holton, 2003). Besides supervisor support, the success of training and its transfer also seems to depend on peer support realised by joint identification and implementation of learning opportunities and the application of learning. Wieland Handy (2008) emphasises the need for appropriate norms (i.e. intra-group norms) which encourage the whole group to learn.

Therefore we examine the influence supervisors and peers have towards trainee motivation, to identify any correlations in the cyber security context. However, there may be instances where participants may be a business of one person, therefore we acknowledge this may be the case in some interviews.

How does your team leader/manager influence your motivation towards cyber security?
How do your peers motivate your cyber security habits at work?

Do you find that you are more motivated when your peers follow cyber security?

Are you likely to follow cyber security if your peers follow it?

Will you follow cyber security if you see your colleagues follow it?

Part 2- Social environment

(**Literature to support question)**

Organizational learning culture which reflects the values and beliefs about the importance of learning at work has been found to be positively related to trainee's transfer motivation (Zubairy et al., 2015). Kontoghiorghes (2002) shows that transfer motivation is high when trainees understand that they are accountable for the training application, that is, when the organization expects trainees to use the training in the workplace. Thus, before the training program even started, the organization normative context already functions to promote or hinder the development of transfer motivation. This is vital in cyber security, if trainees take account for their actions there is more attention on transfer knowledge and the appropriate application in the work place.

In this section we examine the social environment also known as the organisational culture within the business; what are norms and values of the company and how do these factors affect motivation towards cyber security.

Question 2 BCP: How do you think the training will be beneficial for your whole company?

Do you think it's applicable to everyone within your organisation? If no- why?

Question 3 BCP: Has your business changed the way you operate, for example processes since the training?

Question 4 BCP: Would you recommend the training to another company, if yes who?

Are there certain procedures you follow at work?

Do you have a certain way of doing things at work?

Are there factors within the workplace that influence your motivation to learn?

Are there things at work that help you follow cyber security?

Are there things at work that help transfer knowledge you learned in cyber security?

Are you likely to use cyber security after training if your peers do?

Why?

Will you follow cyber security at work if your peers follow it?

Part 3- Cognitive factors

(**Literature to support question)**

In life, various situations require people to focus attention on two locations simultaneously, for example cooks devote attention to multiple pots and ingredients, waiters focus on managing multiple tables and food orders and lifeguards monitor children playing in different locations (Huttermann et al., 2015). In the work context, for example, users must consider and be mindful of cyber security in addition, to their day to day tasks. It is human nature to look for shortcuts and workarounds, especially when users do not understand why their behaviour compromises security. This is linked to human memory, and the attentional limitation each user has towards their own working memory. Each individual's working memory differs from one to another, so the information Mr Smith can retain and use over time maybe significantly less to Mr Nick, whereas they both embarked on the same training. Therefore, just like motivation factors, if companies have an idea what increases or decreases user attention, they can possibly manipulate this for favourable outcome towards cyber security.

Although user education and training have a substantial role to play, changing user behaviour requires motivation and persuasion most especially when the user's own assets are not at risk (Sasse and Flechais 2005).

In this section we examine the influence of peers towards, social environment factors and how these can affect user attention. Therefore in this section of questions we examine where users place predominantly allocate their attention.

Question 5 BCP: After the training what key lessons did you take away?

Question 6 BCP: What would you change about the training?

How do you think this style of teaching affected your motivation to making changes to cyber behaviours compared to typical cyber 'push-learning' training?

Which elements of the training keep you most motivated?

What tends to be your main distractions?

Do you feel that you always have enough time to read through emails properly before replying?

Does your attention to cyber security reduce when you are under pressure?

Does your attention to cyber security lessen if your peers do not follow it?

Do positive opinions on cyber security help you follow it?

Do you feel negative opinions from your peers on cyber security reduce cause you to pay less attention to it?

Do you feel positive opinions from your peers can increase your attention to cyber security?

References

Burke-Smalley, Lisa & Hutchins, Holly. (2007). Training Transfer: An Integrative Literature Review. Human Resource Development Review. 6. 263-296. 10.1177/1534484307303035.

Holton, E. F., Hsin-Chih, C. and Naquin, S. S. (2003), “An examination of learning transfer system characteristics across organizational settings”, Human Resources Development Quarterly, Vol. 14, No. 4, pp. 459-82.

Hüttermann, S. and Memmert, D., 2015. The influence of motivational and mood states on visual attention: A quantification of systematic differences and casual changes in subjects' focus of attention. Cognition and Emotion, 29(3), pp.471-483.

Kontoghiorghes, C., 2001, February. Predicting Motivation to Learn and Motivation to Transferin a Service Organization. In AHRD 2001 CONFERENCE.

Montesino, M.U., 2002. Strategic alignment of training, transfer-enhancing behaviors, and training usage: A posttraining study. *Human Resource Development Quarterly*, *13*(1), pp.89-108.

Rachmaliya, N.S. and Efendy, H., 2017. Analysis of employee performance, organization culture, work satisfaction and organization commitment. Human Resource Research, 1(1), pp.41-57.

Sasse, M.A. and Flechais, I., 2005. Usable security: Why do we need it? How do we get it?. O'Reilly.

Appendix B Response to Individual Attitude Measures at Baseline

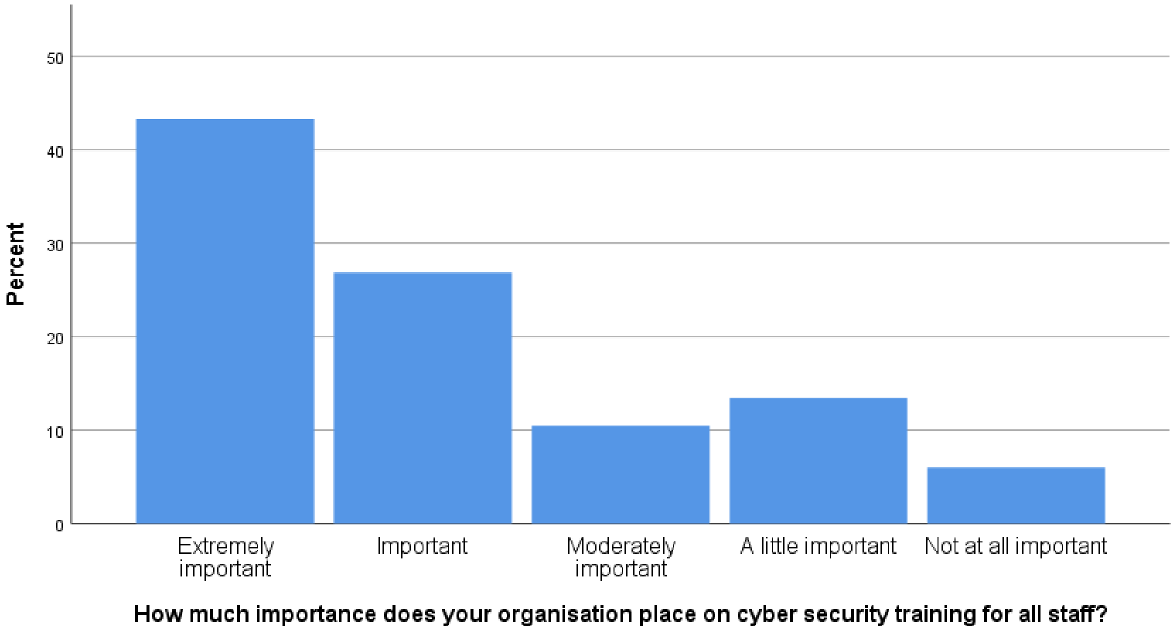


Figure 20 Attitude towards how much importance organisation places on cyber security training for staff

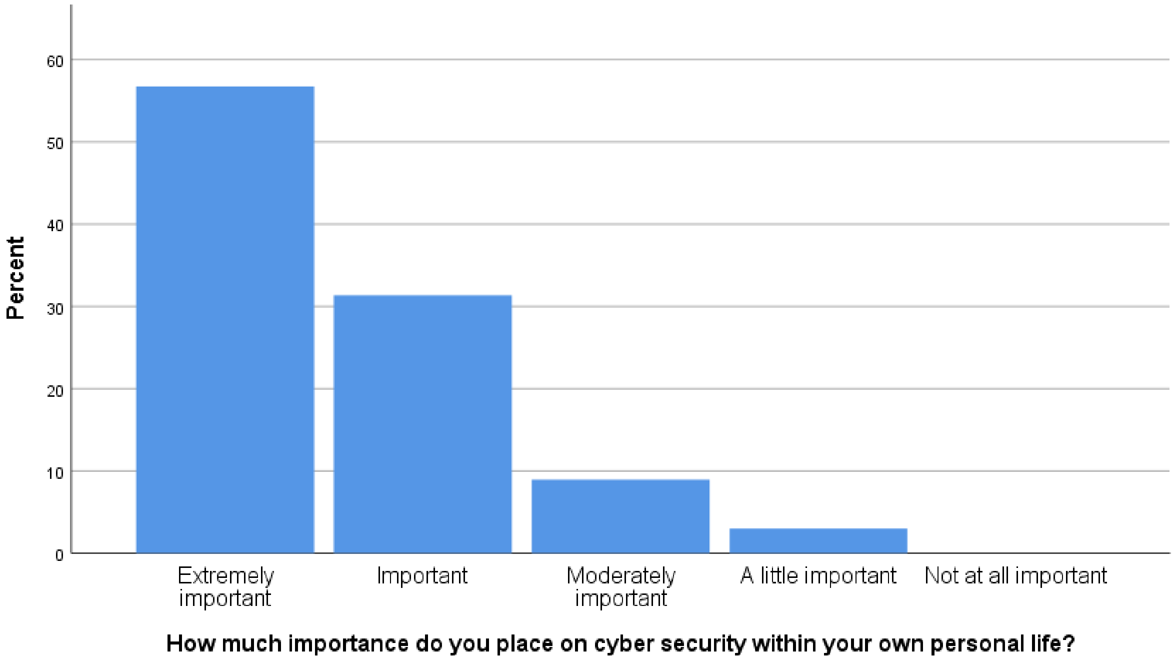


Figure 21: Attitude towards importance placed on cyber security within personal life

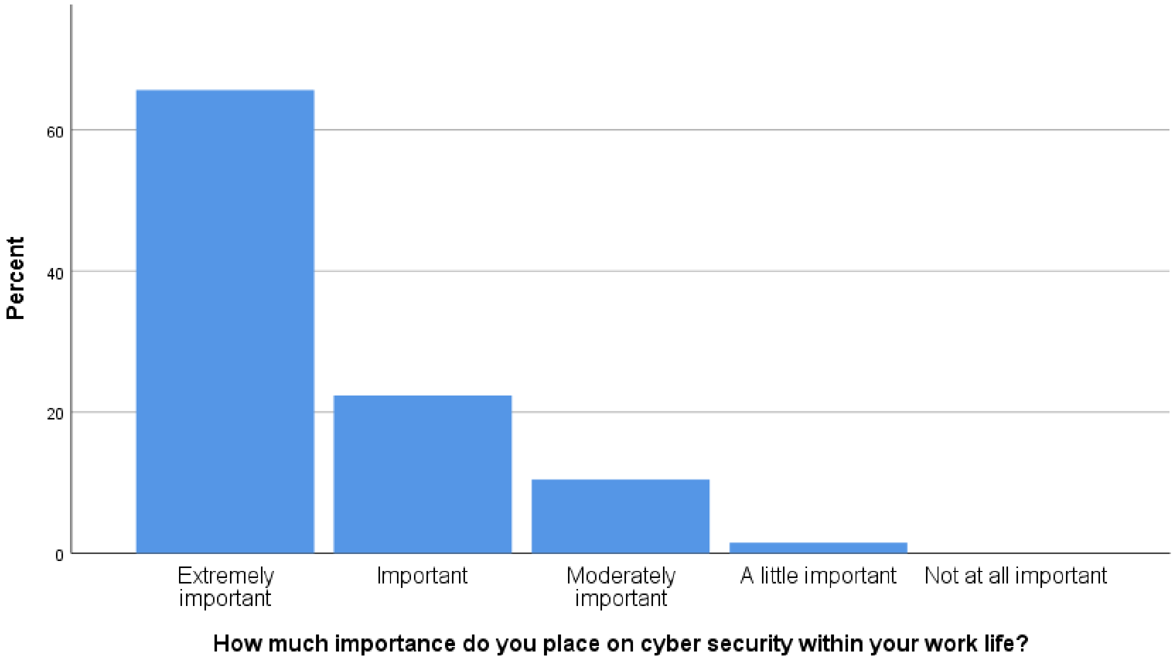


Figure 22. Attitude towards importance placed in cyber security within work life.

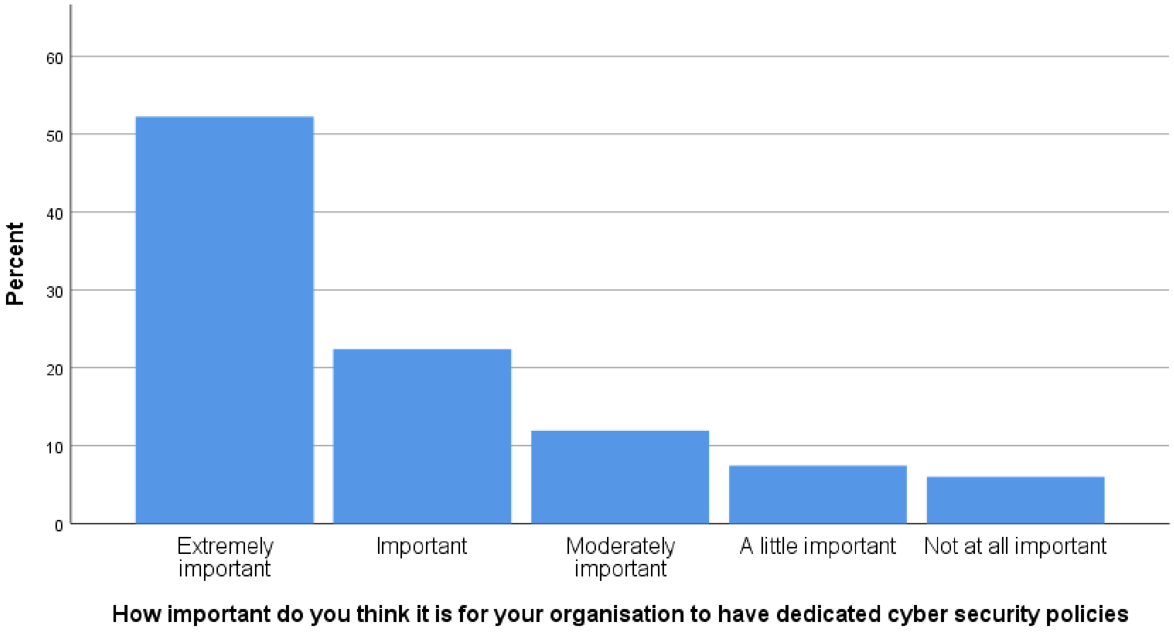


Figure 23: Attitude towards the organisation having dedicated cyber security policies.

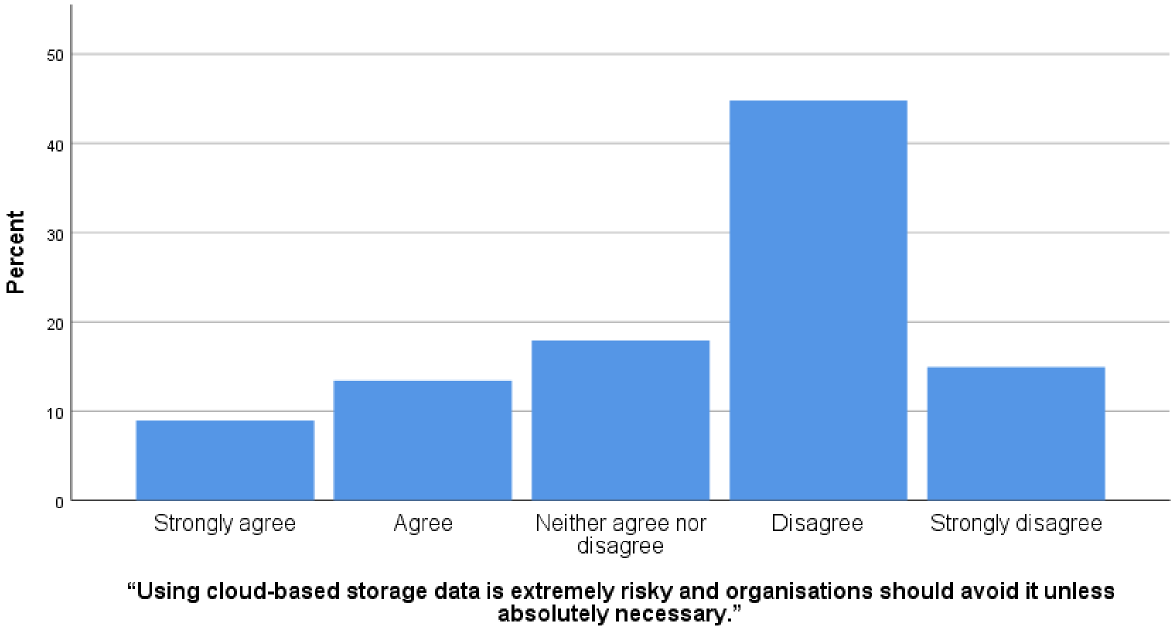


Figure 24: Attitude towards risk of using cloud-based storage.

*Note the scores for the item above were reversed prior to the sub-scale being calculated.

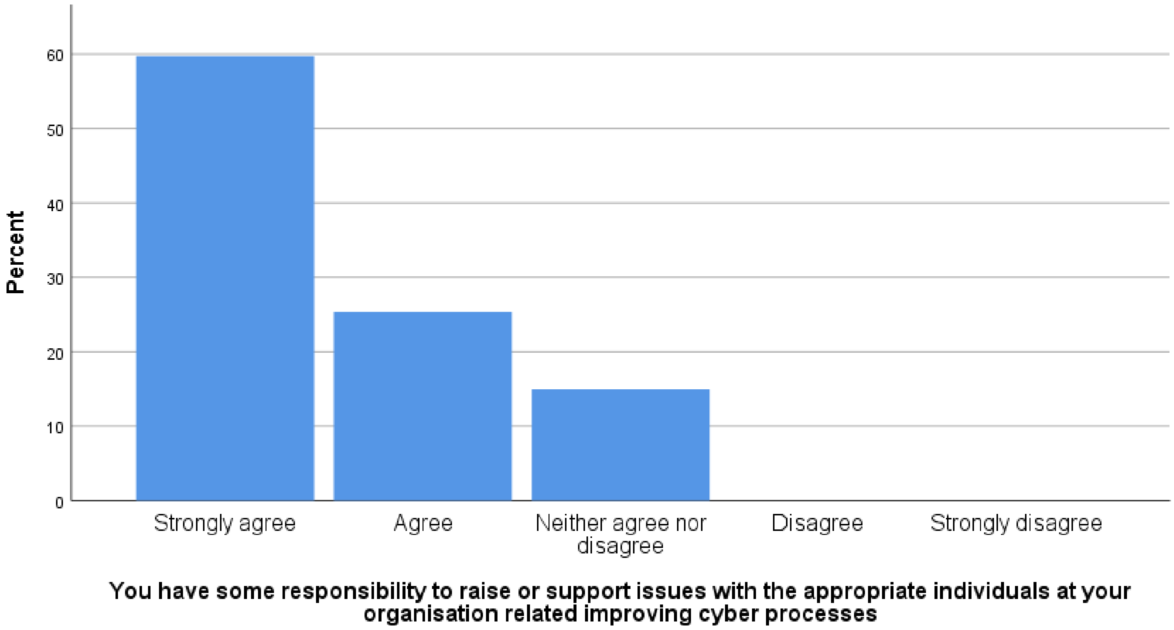


Figure 25. Attitude towards raising issues relating to improving cyber processes.

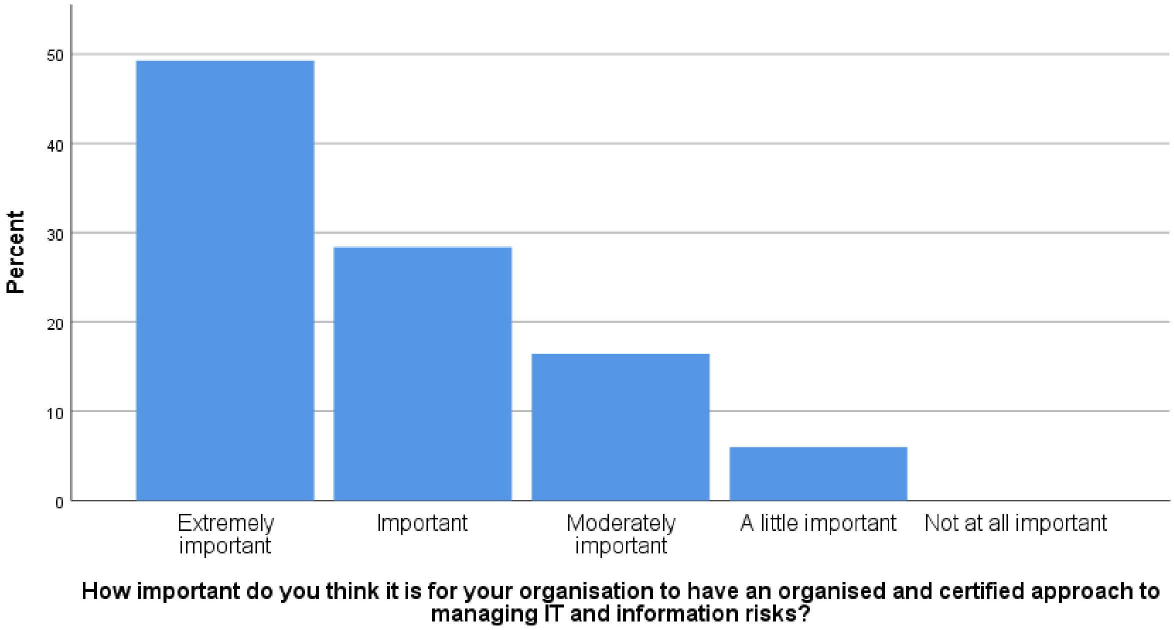


Figure 26. Attitude towards the organisation having an organised and certified approach managing IT and information risks.

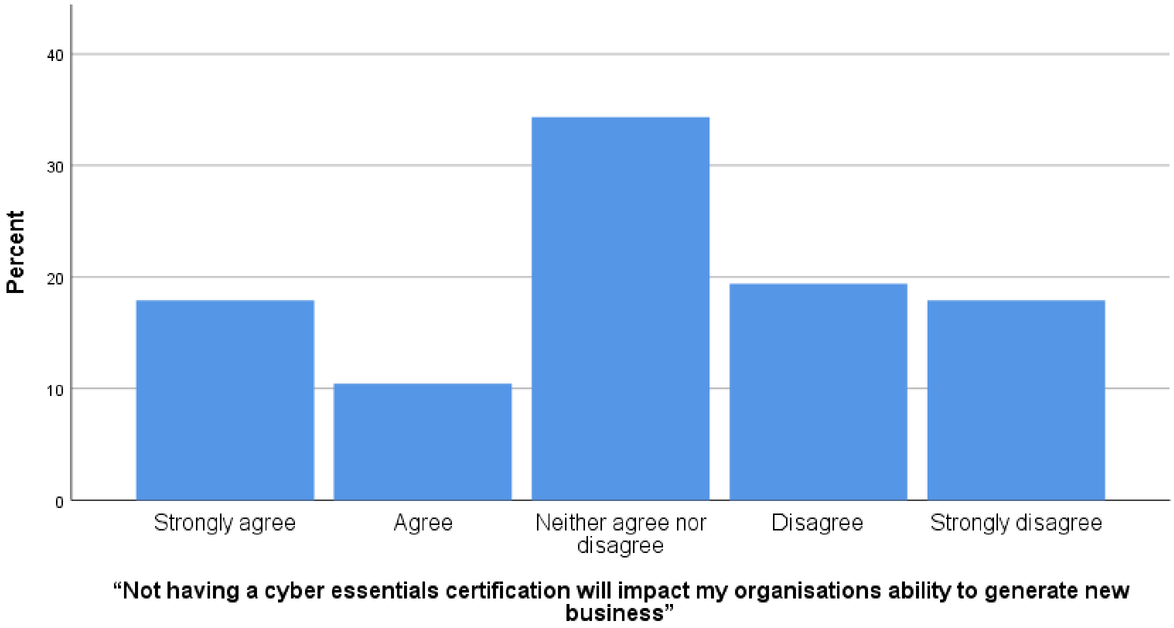


Figure 27. Attitude towards having Cyber Essentials.

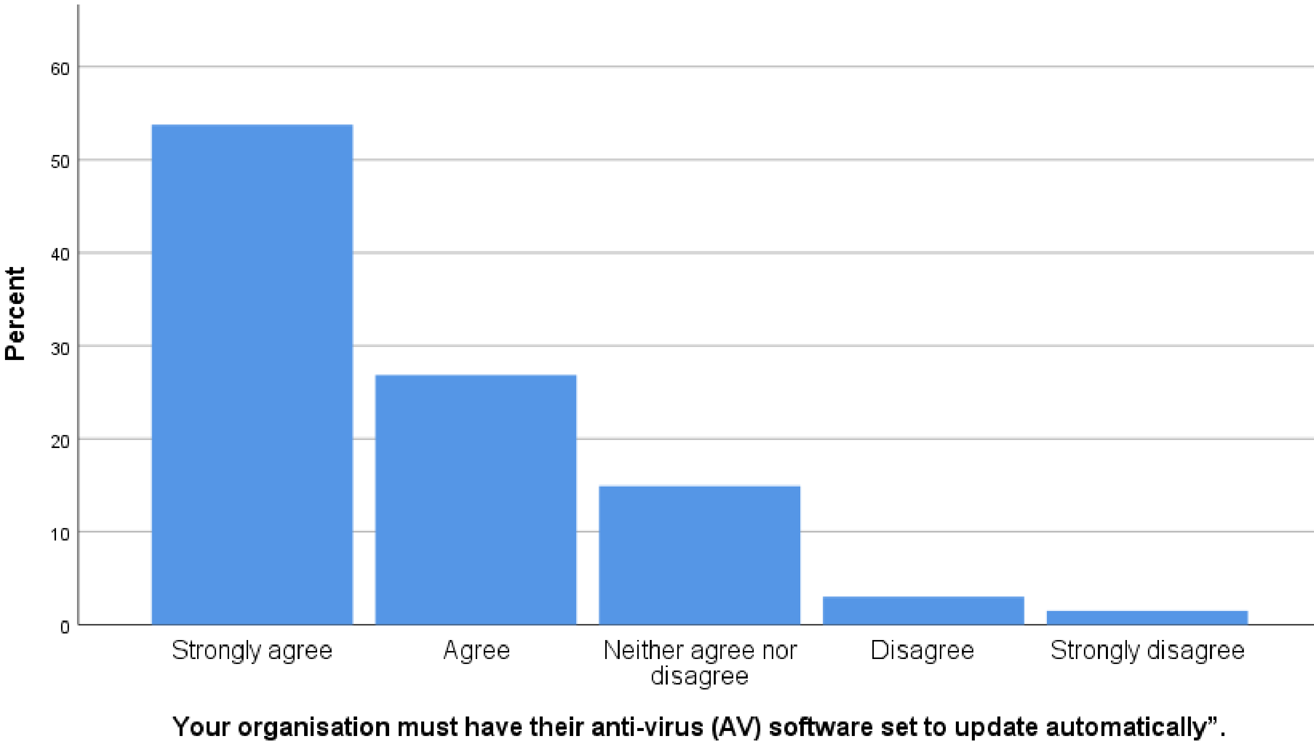


Figure 28. Attitude towards anti-virus software updates.

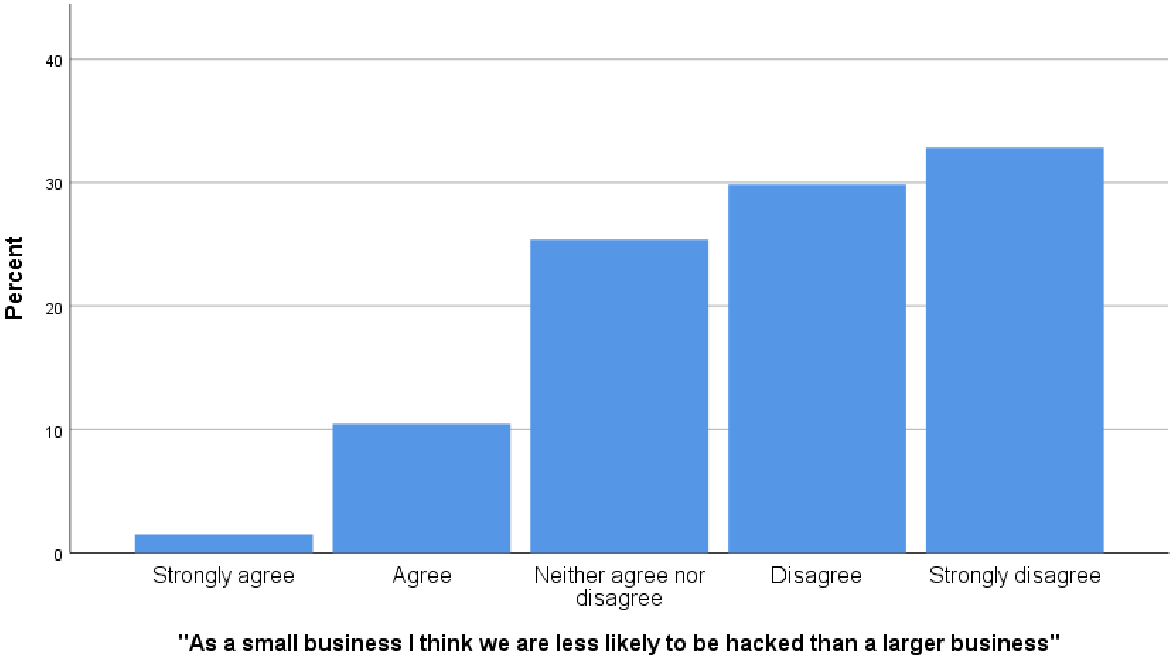


Figure 29. Attitude towards risk of being hacked and organisation size

*Note the scores for the item above were reversed prior to the sub-scale being calculated.

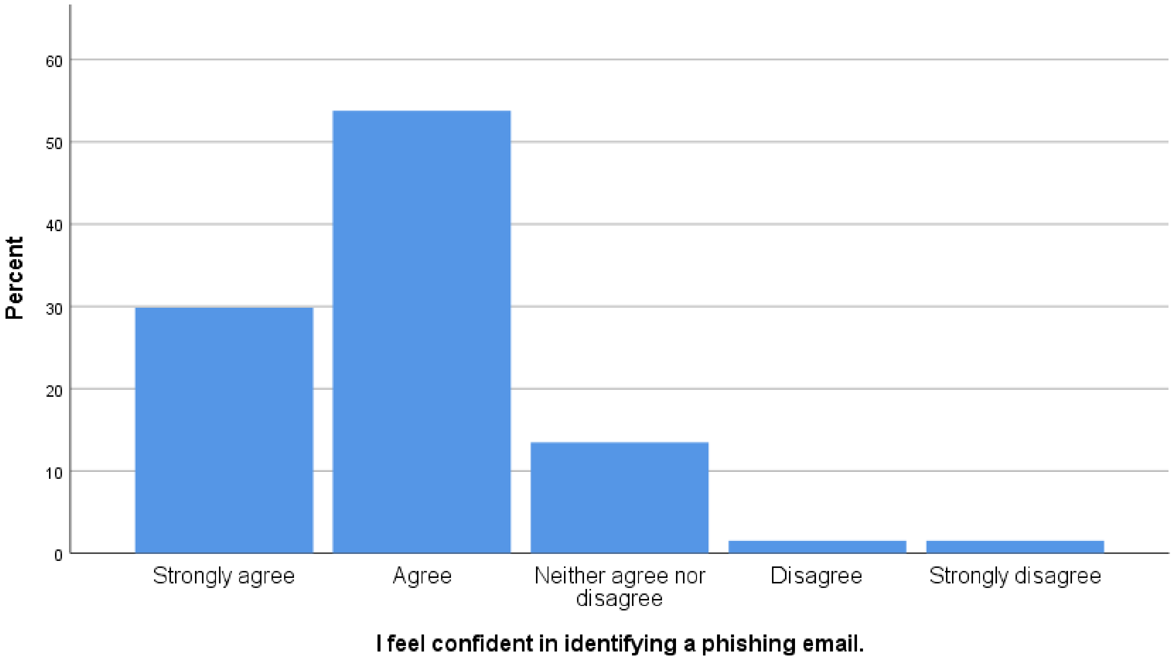


Figure 30. Attitude towards confidence of identifying phishing emails.

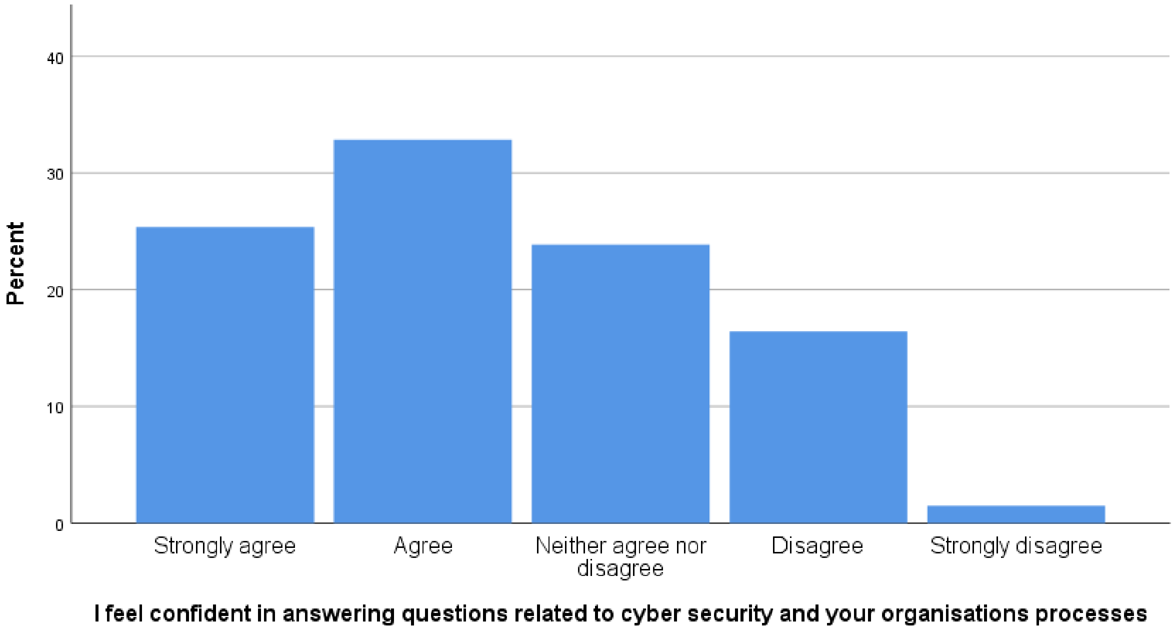


Figure 31. Attitude towards confidence in answering questions related to cyber security and organisational processes.

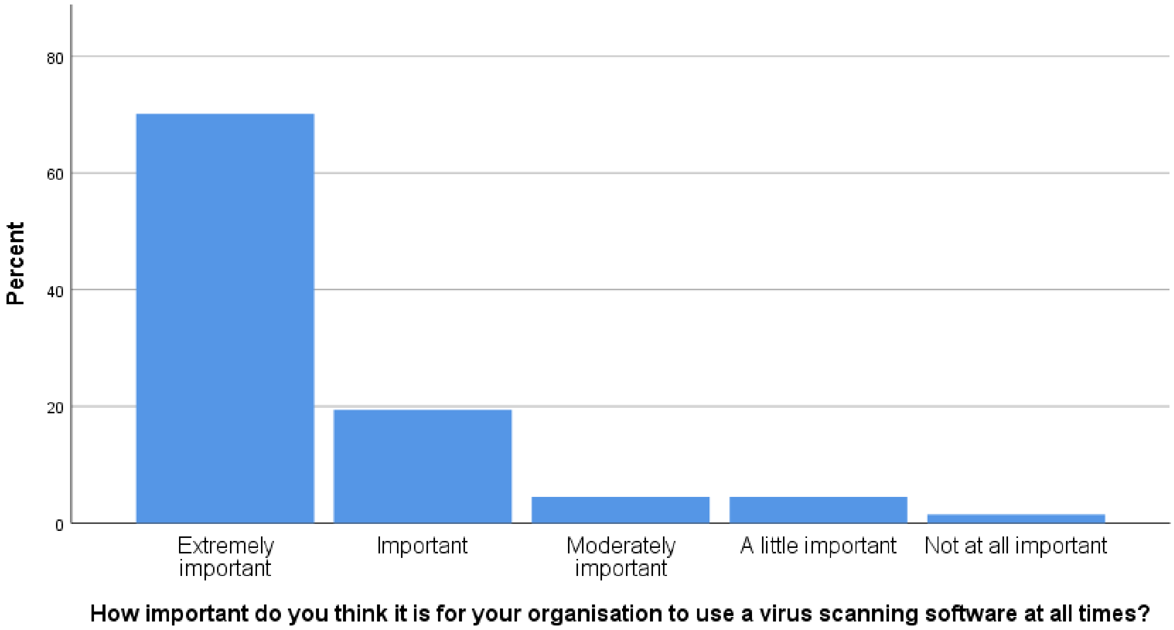


Figure 32. Attitude towards the use of using virus scanning software.

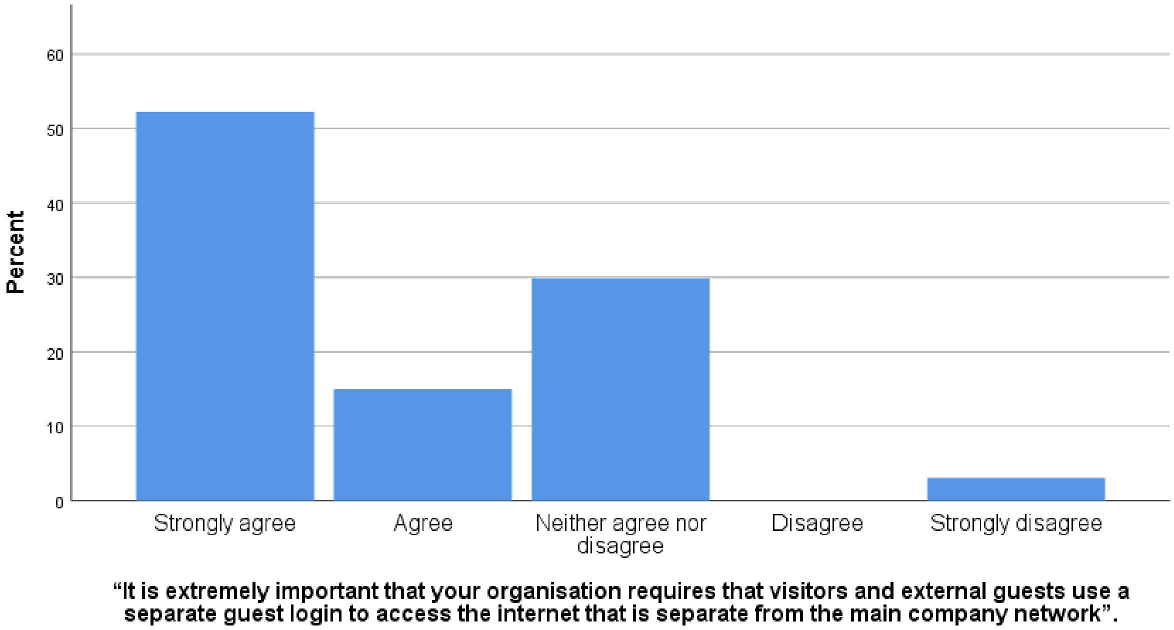


Figure 33. Attitude towards guest logins.

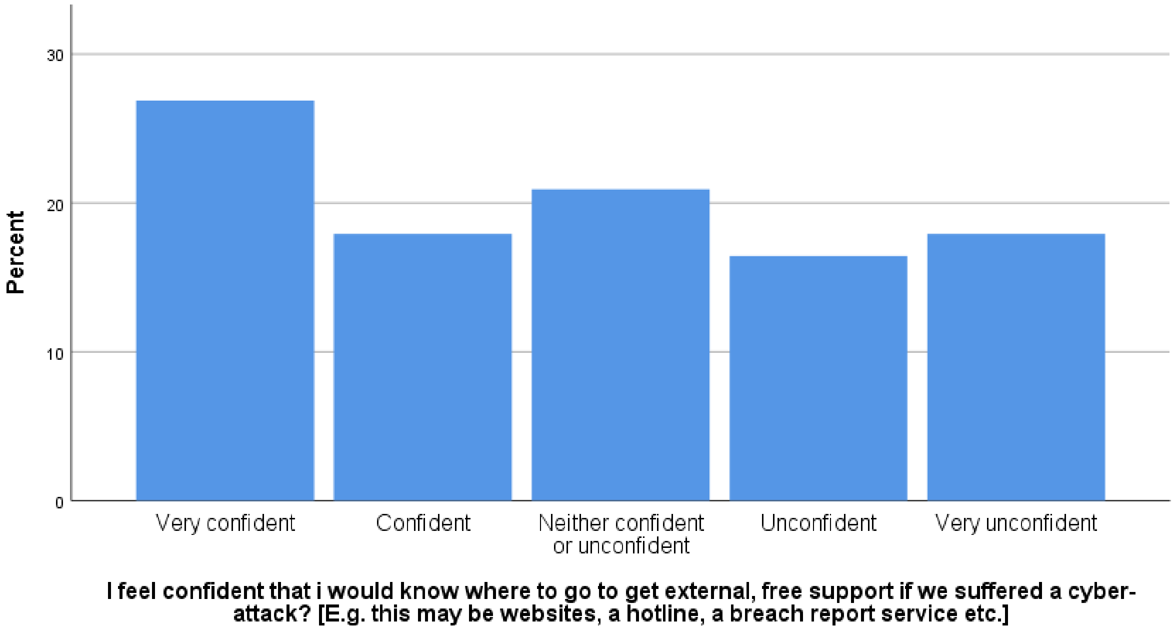


Figure 34. Attitude towards confidence in knowing where to seek external support.

Appendix C Response Rate

Question	% correct responses
Which of the following is an example of a hacker using methods that require them to be physically present instead of online to gain information from an individual's device? (3 response options)	71.6
How can you ensure that external users are authenticated before they are given internet-based access to organisational data? (3 response options)	28.4
An employee picked up a USB stick that they found on their organisation's office floor and plugged it into their company laptop. This USB contains a virus and once the employee plugged it into their laptop, a virus was implemented onto their organisation' (3 response options)	40.3
An example of an active cyber-attack is… (3 response options, plus 'I don't know' option)	56.7
A computer worm is... (3 response options, plus 'I don't know' option)	38.8
Many organisations use passwords that are connected to the business itself. What type of password attack can hackers use to take advantage of this? (3 response options, plus 'I don't know' option)	13.4
What is the main benefit of using staff data monitoring and auditing technology? (3 response options, plus 'I don't know' option)	32.8
A cyber security policy is… (3 response options, plus 'I don't know' option)	35.8
Multi-Factor Authentication is… (3 response options, plus 'I don't know' option)	83.6
What is the purpose of a firewall on computer networks? (3 response options)	71.6
Your organisation has an important new client project which involves a few of your team. Not all employees in your organisation are involved directly. Which is the	83.6

best step to take to best protect your new clients project data? (4 response options, plus ‘I don’t know’ option)	
The goal of whitelisting is to… (4 response options)	43.3
Do you think this is an example of a phishing email? (Yes/ No response option)	98.5
Which answer only describes examples of Malware? (3 response options, plus ‘I don’t know’ option)	50.7
Which of the following do you think your organisation is most likely to suffer from? (2 response options, plus ‘I don’t know’ option)	77.6

Table 2 Percentage of correct response from multiple-choice knowledge questions at baseline

Appendix D Study 2 Training selection Interview Questions (Employees)

1. Tell me about your job role

2. Prompt question: What does your job entail?

3. How many employees are in your business?

4. Prompt question: How many employees are in your team?

5. Who is responsible for cyber security?

6. Prompt question: Whose job is to make sure you follow cyber security?
    a. Is cyber security important to completing tasks at work?

7. Do you see cyber security as a barrier to working efficiently?
    a. Prompt question: Does cyber security make work difficult for you?

8. Is cyber security a priority in your role?

9. How do you decide which is most important between work tasks and cyber security?
    a. Prompt question: Is there a trade-off between work priorities and cyber security?

10. Are there barriers that make it hard to follow cyber security?
    a. Prompt question: If yes, describe the barriers that make it hard to follow cyber security.

11. Is there influence from your managers to follow cyber security?
    a. Prompt question: How does your managers influence you to follow cyber security?

12. Are there repercussions for not following cyber security?
    a. Prompt question: Are there punishments for not following cyber security?

13. Does your manager or team leader ask you if you have challenges using cyber security?

14. From your experience when was the last time you had cyber security training?

15. Do you ever have refresher training?

16. In your opinion, how do you know if cyber security training has worked?

17. Do you feel like cyber training address the challenges you experience with cyber security?

18. Before your manager looks for training for the team, do they ask you what your challenges are with cyber security?

Appendix E Study 2 Training selection Interview Questions (Content developer)

1. Describe your job role

Prompt question: What does your job entail?

2. Thinking back to when you last started the training projects, How do you develop training material?

3. What is the process for developing training material?

Prompt question: Do you or the company develop training from scratch?

4. When you develop training do you pilot the training? Who do you pilot training to?

5. What is the objective of training you develop?

Prompt question: What is the purpose of training?

6. In your view, what is the process for you selecting training material, if any?

Prompt question: What process do you take when you select training material?

7. Do you look for certified training material?

8. In your role, do you explore topics like adult learning?

9. How much of adult learning is involved in training you develop?

10. How long have you been offering training?

11. Who is responsible for your process within your company for selecting training material?

Follow up question: How do you know this process is best for selecting training material?

12. How do you determine what material is best for training?

13. How do you know training material will be successful?

14. What resources or concepts are your training materials based on?

15. How do you determine what the trainee needs?

Prompt question: For example, do you gather trainee requirements before the development of training?

16. How do company needs contribute to the development of training material? (reword)

17. In a broader picture, are you aware of the risks of the company you are developing training for?
Prompt question: Do you know what cyber risks the end users are struggling with?
Prompt question: Do you know what poor cyber practice needs addressing?

18. How do you assess training?
Prompt question: How do you know if training assessment has worked?

19. What feedback have you had back from training?

20. What actions have you taken from the feedback?

21. As far as you are aware, are there any follow up assessments?
Prompt question: Do you measure any poor behaviour after training?

22. Are there follow up training?

Appendix F Study 2 Training selection Interview Questions (Awareness professional)

1. Tell me about your role
    1. Prompt question: What does your job entail?

2. How do you find training packages which you use?
Prompt: What motivated you to look for training?

3. How do you determine what training package is best for your business?
Prompt question: What process do you take in selecting training?
Prompt question: Do you look for certified training?

4. How important are user training needs when choosing training?

5. Do you consider what user training needs most when choosing training?
Prompt question: Do you gather user training requirements before training?

6. What challenges do you think users have with cyber security?

7. Do you look into how engaged the staff were in the training?
a. If yes, how?
Prompt question: What are the barriers in engaging staff with training?
Prompt question: Do you have any specific examples from your experiences?

8. Do you participate in training?
Prompt question: Do you have specific training for your job role?

9. Do senior staff receive training?
If yes, is the training package different to the employee training package?

10. How does senior staff measure if training has been personally effective in their role?

11. How do you measure if the training has been effective for the team?
Prompt question: Do you have follow up training?
Prompt question: Do you measure training effectiveness after training?
If yes, how long after do you measure this?
Prompt question: Do you measure user behaviour?

12. Do you measure poor cyber practice?

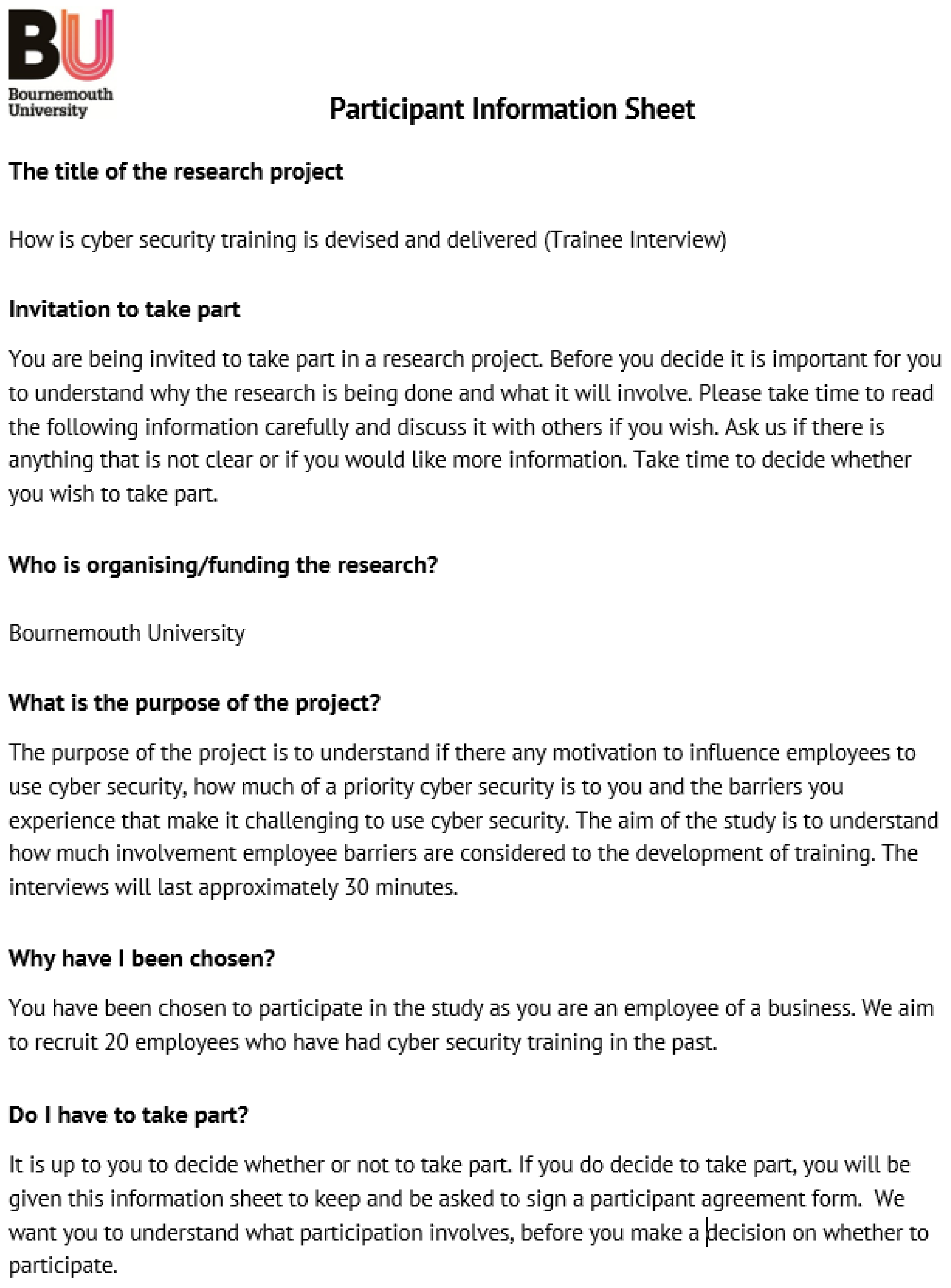
13. If yes, how do you measure poor cyber practice?

14. What is the next action if there is still poor cyber practice?

13. Have you had any experience in training people?

14. What challenges do you think smaller businesses have that, larger do not have?

Appendix G Participant Information Sheet Study 2 Training selection (Employees)



Participant Information Sheet

The title of the research project

How is cyber security training is devised and delivered (Trainee Interview)

Invitation to take part

You are being invited to take part in a research project. Before you decide it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or if you would like more information. Take time to decide whether you wish to take part.

Who is organising/funding the research?

Bournemouth University

What is the purpose of the project?

The purpose of the project is to understand if there any motivation to influence employees to use cyber security, how much of a priority cyber security is to you and the barriers you experience that make it challenging to use cyber security. The aim of the study is to understand how much involvement employee barriers are considered to the development of training. The interviews will last approximately 30 minutes.

Why have I been chosen?

You have been chosen to participate in the study as you are an employee of a business. We aim to recruit 20 employees who have had cyber security training in the past.

Do I have to take part?

It is up to you to decide whether or not to take part. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a participant agreement form. We want you to understand what participation involves, before you make a decision on whether to participate.

If you or any family member have an on-going relationship with BU or the research team, e.g. as a member of staff, as student or other service user, your decision on whether to take part (or continue to take part) will not affect this relationship in any way.

Can I change my mind about taking part?

Yes, you can stop participating in study activities at any time and without giving a reason.

If I change my mind, what happens to my information?

After you decide to withdraw from the study, we will not collect any further information from or about you. However, if analysis has started your data cannot be withdrawn from the analysis or future reports.

What would taking part involve?

The participation includes a voice Zoom call that will last approximately 30 minutes.

What are the advantages and possible disadvantages or risks of taking part?

Whilst there are no immediate benefits to you participating in the project, it is hoped that this work will demonstrate employee barriers to using cyber security, which we aim to aid the development and design of cyber security training.

What type of information will be sought from me and why is the collection of this information relevant for achieving the research project's objectives?

The questions are around the priorities employees place on cyber security, challenges experienced when using cyber security and questions around motivation to use cyber. The purpose for this is to identify any gaps or challenges your business face that training do not necessarily identify or resolve.

Will I be recorded, and how will the recorded media be used?

The audio recordings of your activities made during this research will be used only for analysis and the transcription of the recording(s) for illustration in conference presentations and lectures. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recordings.

How will my information be managed?

Bournemouth University (BU) is the organisation with overall responsibility for this study and the Data Controller of your personal information, which means that we are responsible for looking after your information and using it appropriately. Research is a task that we perform in the public interest, as part of our core function as a university.

Undertaking this research study involves collecting and/or generating information about you. We manage research data strictly in accordance with:

- Ethical requirements; and
- Current data protection laws. These control use of information about identifiable individuals, but do not apply to anonymous research data: "anonymous" means that we have either removed or not collected any pieces of data or links to other data which identify a specific person as the subject or source of a research result.

BU's Research Participant Privacy Notice sets out more information about how we fulfil our responsibilities as a data controller and about your rights as an individual under the data protection legislation. We ask you to read this Notice so that you can fully understand the basis on which we will process your personal information.

Research data will be used only for the purposes of the study or related uses identified in the Privacy Notice or this Information Sheet. To safeguard your rights in relation to your personal information, we will use the minimum personally-identifiable information possible and control access to that data as described below.

Publication

You will not be able to be identified in any external reports or publications about the research without your specific consent. Otherwise your information will only be included in these materials in an anonymous form, i.e. you will not be identifiable.

Research results will be published in the Dorset Cyber Alliance (DCA) newsletter.

Security and access controls

BU will hold the information we collect about you in hard copy in a secure location and on a BU password protected secure network where held electronically.

Personal information which has not been anonymised will be accessed and used only by appropriate, authorised individuals and when this is necessary for the purposes of the research or another purpose identified in the Privacy Notice. This may include giving access to BU staff or others responsible for monitoring and/or audit of the study, who need to ensure that the research is complying with applicable regulations.

Keeping your information if you withdraw from the study

If you withdraw from active participation in the study we will keep information which we have already collected from or about you, if this has on-going relevance or value to the study. This may include your personal identifiable information. As explained above, your legal rights to access, change, delete or move this information are limited as we need to manage your information in specific ways in order for the research to be reliable and accurate. However if you have concerns about how this will affect you personally, you can raise these with the research team when you withdraw from the study.

You can find out more about your rights in relation to your data and how to raise queries or complaints in our Privacy Notice.

Retention of research data

Project governance documentation, including copies of signed **participant agreements**: we keep this documentation for a long period after completion of the research, so that we have records of how we conducted the research and who took part. The only personal information in this documentation will be your name and signature, and we will not be able to link this to any anonymised research results.

Research results:

As described above, during the course of the study we will anonymise the information we have collected about you as an individual. This means that we will not hold your personal information in identifiable form after we have completed the research activities.

You can find more specific information about retention periods for personal information in our Privacy Notice.

We keep anonymised research data indefinitely, so that it can be used for other research as described above.

Contact for further information

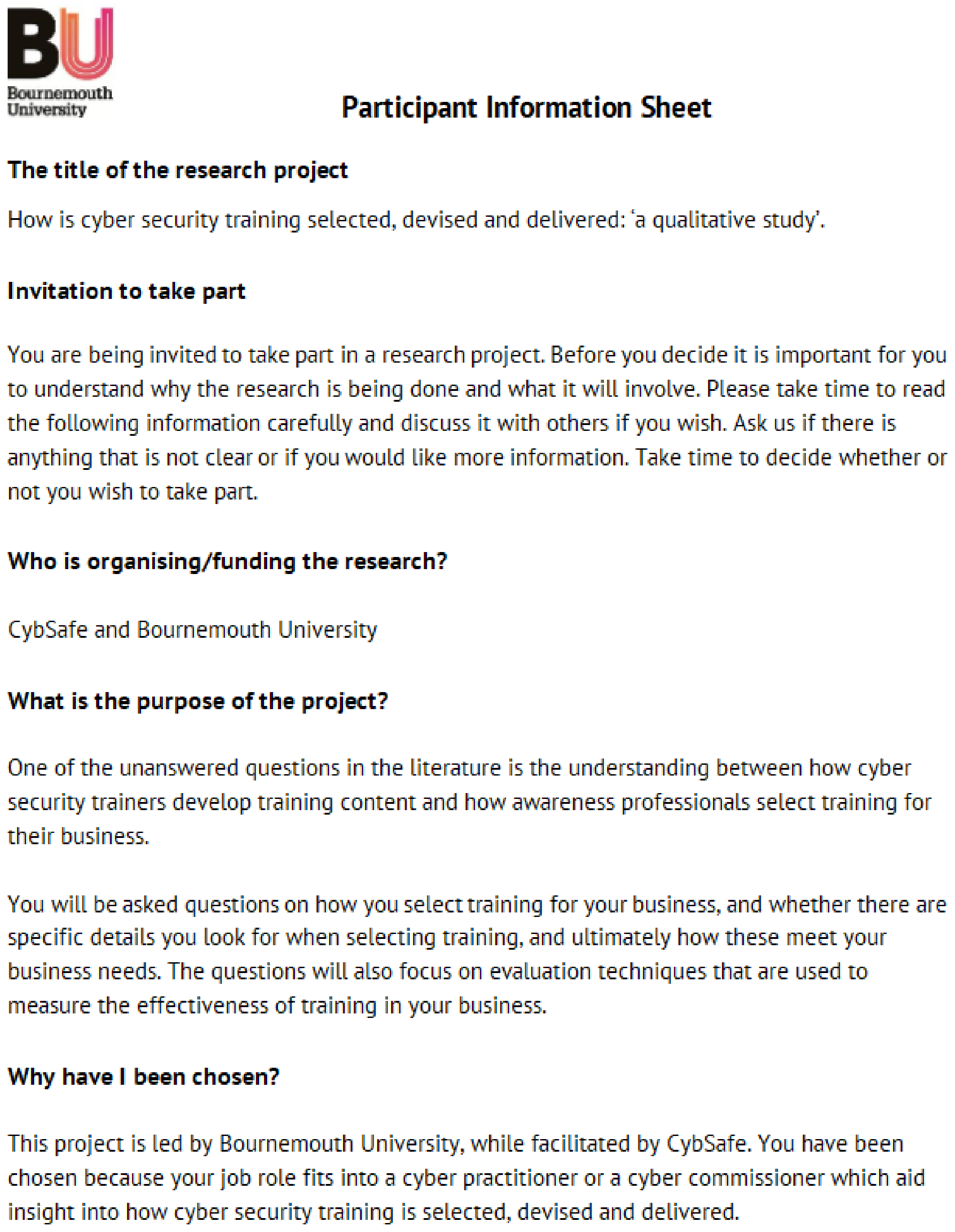
If you have any questions or would like further information, please contact Omolola Fagbule ofagbule@bournemouth.ac.uk

In case of complaints
Any concerns about the study should be directed to Professor Tiantian Zhang by email to researchgovernance@bournemouth.ac.uk

Finally

If you decide to take part, you will be given a copy of the information sheet and a signed participant agreement form to keep.

Appendix H Participant Information Sheet Study 2 Training selection (Content developer)



Bournemouth University

Participant Information Sheet

The title of the research project

How is cyber security training selected, devised and delivered: 'a qualitative study'.

Invitation to take part

You are being invited to take part in a research project. Before you decide it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or if you would like more information. Take time to decide whether or not you wish to take part.

Who is organising/funding the research?

CybSafe and Bournemouth University

What is the purpose of the project?

One of the unanswered questions in the literature is the understanding between how cyber security trainers develop training content and how awareness professionals select training for their business.

You will be asked questions on how you select training for your business, and whether there are specific details you look for when selecting training, and ultimately how these meet your business needs. The questions will also focus on evaluation techniques that are used to measure the effectiveness of training in your business.

Why have I been chosen?

This project is led by Bournemouth University, while facilitated by CybSafe. You have been chosen because your job role fits into a cyber practitioner or a cyber commissioner which aid insight into how cyber security training is selected, devised and delivered.

Do I have to take part?

It is up to you to decide whether or not to take part. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a participant agreement form. We want you to understand what participation involves, before you make a decision on whether to participate.

If you or any family member have an on-going relationship with BU or the research team, e.g. as a member of staff, as student or other service user, your decision on whether to take part (or continue to take part) will not affect this relationship in any way.

Can I change my mind about taking part?

Yes, you can stop participating in study activities at any time and without giving a reason. Any collected data will be deleted immediately and will not be used in the project.

If I change my mind, what happens to my information?

After you decide to withdraw from the study, we will not collect any further information from or about you and data will be deleted and omitted in the project.

What would taking part involve?

The participants will participant in an online interview using Zoom. The interview will consist of a voice call and will last for approximately 30 minutes.
The participants data will be anonymised to protect information shared, this includes names and organisation. Some responses can include information about your organisation, these will be redacted in the transcripts if there is potential to identify your business.

What are the advantages and possible disadvantages or risks of taking part?

Whilst there are no immediate benefits to you participating in the project, it is hoped that this work will contribute to the research of how cyber security training is selected, devised and delivered from the niche lens of cyber-psychology.

What type of information will be sought from me and why is the collection of this information relevant for achieving the research project's objectives?

The information that will be gathered will pertain how training is selected, how it is developed and how it is delivered i.e. what methods of training is used to train businesses. This information is vital to understanding how requirements are met between commissioners and practitioners.

Will I be recorded, and how will the recorded media be used?

The interviews will be voice to voice, so participants do not have to show their video. The interviews will be recorded on Zoom to retrieve vital information discussed that can aid analysis and research. The recording for the Zoom phone call will be downloaded for transcription and then deleted from both Zoom and the PC which the recording is downloaded on.
The recording will be used to listen over and to clarify any uncertainties. The audio of your activities made during this research will be used only for analysis and the transcription of the recording(s) for illustration in conference presentations. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recordings.

How will my information be managed?

Bournemouth University (BU) is the organisation with overall responsibility for this study and the Data Controller of your personal information, which means that we are responsible for looking after your information and using it appropriately. Research is a task that we perform in the public interest, as part of our core function as a university.

Undertaking this research study involves collecting and/or generating information about you. We manage research data strictly in accordance with:

- Ethical requirements; and
- Current data protection laws. These control use of information about identifiable individuals, but do not apply to anonymous research data: “anonymous” means that we have either removed or not collected any pieces of data or links to other data which identify a specific person as the subject or source of a research result.

BU’s Research Participant Privacy Notice sets out more information about how we fulfil our responsibilities as a data controller and about your rights as an individual under the data protection legislation. We ask you to read this Notice so that you can fully understand the basis on which we will process your personal information.

Research data will be used only for the purposes of the study or related uses identified in the Privacy Notice or this Information Sheet. To safeguard your rights in relation to your personal information, we will use the minimum personally-identifiable information possible and control access to that data as described below.

Publication

You will not be able to be identified in any external reports or publications about the research without your specific consent. Otherwise your information will only be included in these materials in an anonymous form, i.e. you will not be identifiable.

Security and access controls

BU will hold the information we collect about you in hard copy in a secure location and on a BU password protected secure network where held electronically.

Personal information which has not been anonymised will be accessed and used only by appropriate, authorised individuals and when this is necessary for the purposes of the research or another purpose identified in the Privacy Notice. This may include giving access to BU staff or others responsible for monitoring and/or audit of the study, who need to ensure that the research is complying with applicable regulations.

Further use of your information

The information collected about you will not be used to support other research projects in the future.

Keeping your information if you withdraw from the study

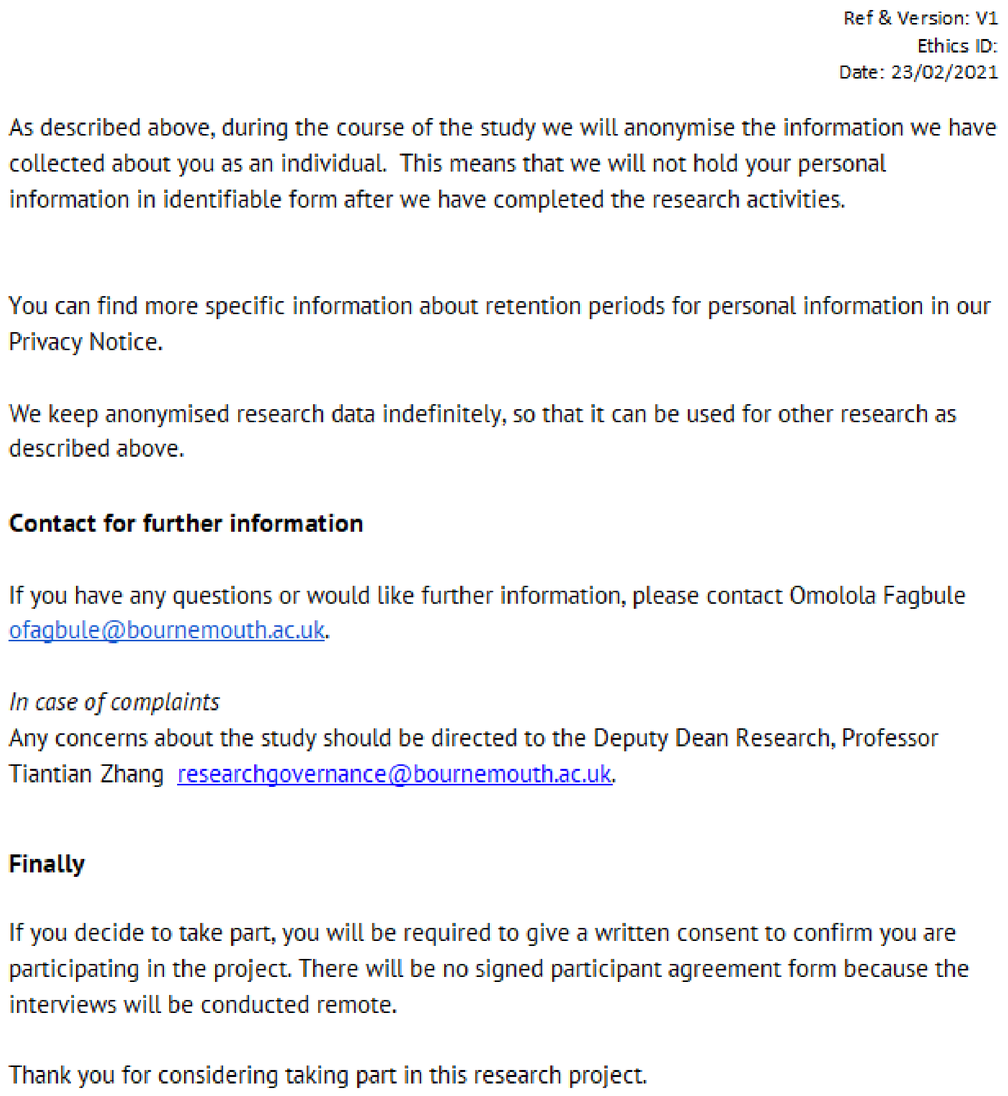
If you withdraw from active participation in the study we will keep information which we have already collected from or about you, if this has on-going relevance or value to the study. This may include your personal identifiable information. As explained above, your legal rights to access, change, delete or move this information are limited as we need to manage your information in specific ways in order for the research to be reliable and accurate. However if you have concerns about how this will affect you personally, you can raise these with the research team when you withdraw from the study.

You can find out more about your rights in relation to your data and how to raise queries or complaints in our Privacy Notice.

Retention of research data

Project governance documentation, including copies of signed **participant agreements**: we keep this documentation for a long period after completion of the research, so that we have records of how we conducted the research and who took part.

Research results:



Ref & Version: V1
Ethics ID:
Date: 23/02/2021

As described above, during the course of the study we will anonymise the information we have collected about you as an individual. This means that we will not hold your personal information in identifiable form after we have completed the research activities.

You can find more specific information about retention periods for personal information in our Privacy Notice.

We keep anonymised research data indefinitely, so that it can be used for other research as described above.

Contact for further information

If you have any questions or would like further information, please contact Omolola Fagbule ofagbule@bournemouth.ac.uk.

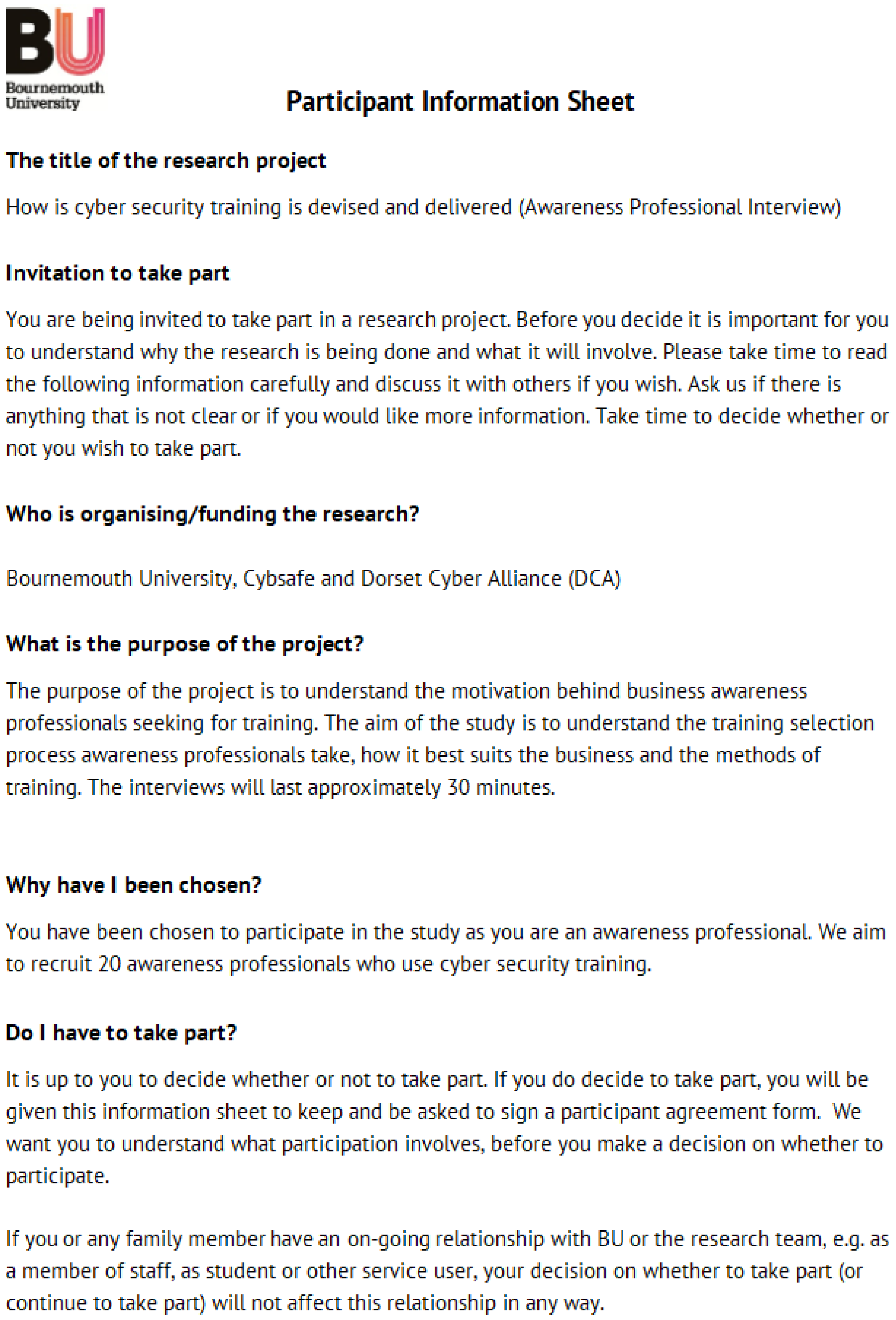
In case of complaints
Any concerns about the study should be directed to the Deputy Dean Research, Professor Tiantian Zhang researchgovernance@bournemouth.ac.uk.

Finally

If you decide to take part, you will be required to give a written consent to confirm you are participating in the project. There will be no signed participant agreement form because the interviews will be conducted remote.

Thank you for considering taking part in this research project.

Appendix I Participant Information Sheet Study 2 Training selection (Awareness professional)



Bournemouth University

Participant Information Sheet

The title of the research project

How is cyber security training is devised and delivered (Awareness Professional Interview)

Invitation to take part

You are being invited to take part in a research project. Before you decide it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or if you would like more information. Take time to decide whether or not you wish to take part.

Who is organising/funding the research?

Bournemouth University, Cybsafe and Dorset Cyber Alliance (DCA)

What is the purpose of the project?

The purpose of the project is to understand the motivation behind business awareness professionals seeking for training. The aim of the study is to understand the training selection process awareness professionals take, how it best suits the business and the methods of training. The interviews will last approximately 30 minutes.

Why have I been chosen?

You have been chosen to participate in the study as you are an awareness professional. We aim to recruit 20 awareness professionals who use cyber security training.

Do I have to take part?

It is up to you to decide whether or not to take part. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a participant agreement form. We want you to understand what participation involves, before you make a decision on whether to participate.

If you or any family member have an on-going relationship with BU or the research team, e.g. as a member of staff, as student or other service user, your decision on whether to take part (or continue to take part) will not affect this relationship in any way.

Ref & Version: 1
Ethics ID: 38681
Date: 26/5/2021

Can I change my mind about taking part?

Yes, you can stop participating in study activities at any time and without giving a reason.

If I change my mind, what happens to my information?

After you decide to withdraw from the study, we will not collect any further information from or about you. All collected information will destroyed and not included in any analysis or reports.

What would taking part involve?

The participation includes a voice Zoom call that will last approximately 30 minutes.

What are the advantages and possible disadvantages or risks of taking part?

Whilst there are no immediate benefits for those people participating in the project, it is hoped that this work will assist awareness professionals in decision making for cyber security training.

What type of information will be sought from me and why is the collection of this information relevant for achieving the research project's objectives?

The questions are around the process and decision making process you take when you select training for your business. The purpose for this is to identify any gaps or challenges your business face that training do not necessarily identify or resolve.

Will I be recorded, and how will the recorded media be used?

The audio recordings of your activities made during this research will be used only for analysis and the transcription of the recording(s) for illustration in conference presentations and lectures. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recordings.

How will my information be managed?

Bournemouth University (BU) is the organisation with overall responsibility for this study and the Data Controller of your personal information, which means that we are responsible for looking after your information and using it appropriately. Research is a task that we perform in the public interest, as part of our core function as a university.

Undertaking this research study involves collecting and/or generating information about you. We manage research data strictly in accordance with:

- Ethical requirements; and
- Current data protection laws. These control use of information about identifiable individuals, but do not apply to anonymous research data: "anonymous" means that we have either removed or not collected any pieces of data or links to other data which identify a specific person as the subject or source of a research result.

BU's Research Participant Privacy Notice sets out more information about how we fulfil our responsibilities as a data controller and about your rights as an individual under the data protection legislation. We ask you to read this Notice so that you can fully understand the basis on which we will process your personal information.

Research data will be used only for the purposes of the study or related uses identified in the Privacy Notice or this Information Sheet. To safeguard your rights in relation to your personal information, we will use the minimum personally-identifiable information possible and control access to that data as described below.

Publication

You will not be able to be identified in any external reports or publications about the research without your specific consent. Otherwise your information will only be included in these materials in an anonymous form, i.e. you will not be identifiable.

Research results will be published in the Dorset Cyber Alliance (DCA) newsletter.

Security and access controls

BU will hold the information we collect about you in hard copy in a secure location and on a BU password protected secure network where held electronically.

Personal information which has not been anonymised will be accessed and used only by appropriate, authorised individuals and when this is necessary for the purposes of the research or another purpose identified in the Privacy Notice. This may include giving access to BU staff or others responsible for monitoring and/or audit of the study, who need to ensure that the research is complying with applicable regulations.

Further use of your information

The information collected about you may be used in an anonymous form to support other research projects in the future and access to it in this form will not be restricted. It will not be possible for you to be identified from this data.

Keeping your information if you withdraw from the study

If you withdraw from active participation in the study, we will keep information which we have already collected from or about you, if this has on-going relevance or value to the study. This may include your personal identifiable information. As explained above, your legal rights to access, change, delete or move this information are limited as we need to manage your information in specific ways in order for the research to be reliable and accurate. However, if you have concerns about how this will affect you personally, you can raise these with the research team when you withdraw from the study.

You can find out more about your rights in relation to your data and how to raise queries or complaints in our Privacy Notice.

Retention of research data

Project governance documentation, including copies of signed **participant agreements**: we keep this documentation for a long period after completion of the research, so that we have records of how we conducted the research and who took part. The only personal information in this documentation will be your name and signature, and we will not be able to link this to any anonymised research results.

Research results:

STATEMENT 1 – *Use if you have provided details of how you will anonymise information during the active period of the research study:*

As described above, during the course of the study we will anonymise the information we have collected information about you as an individual. This means that we will not hold your personal information in identifiable form after we have completed the research activities.

You can find more specific information about retention periods for personal information in our Privacy Notice.

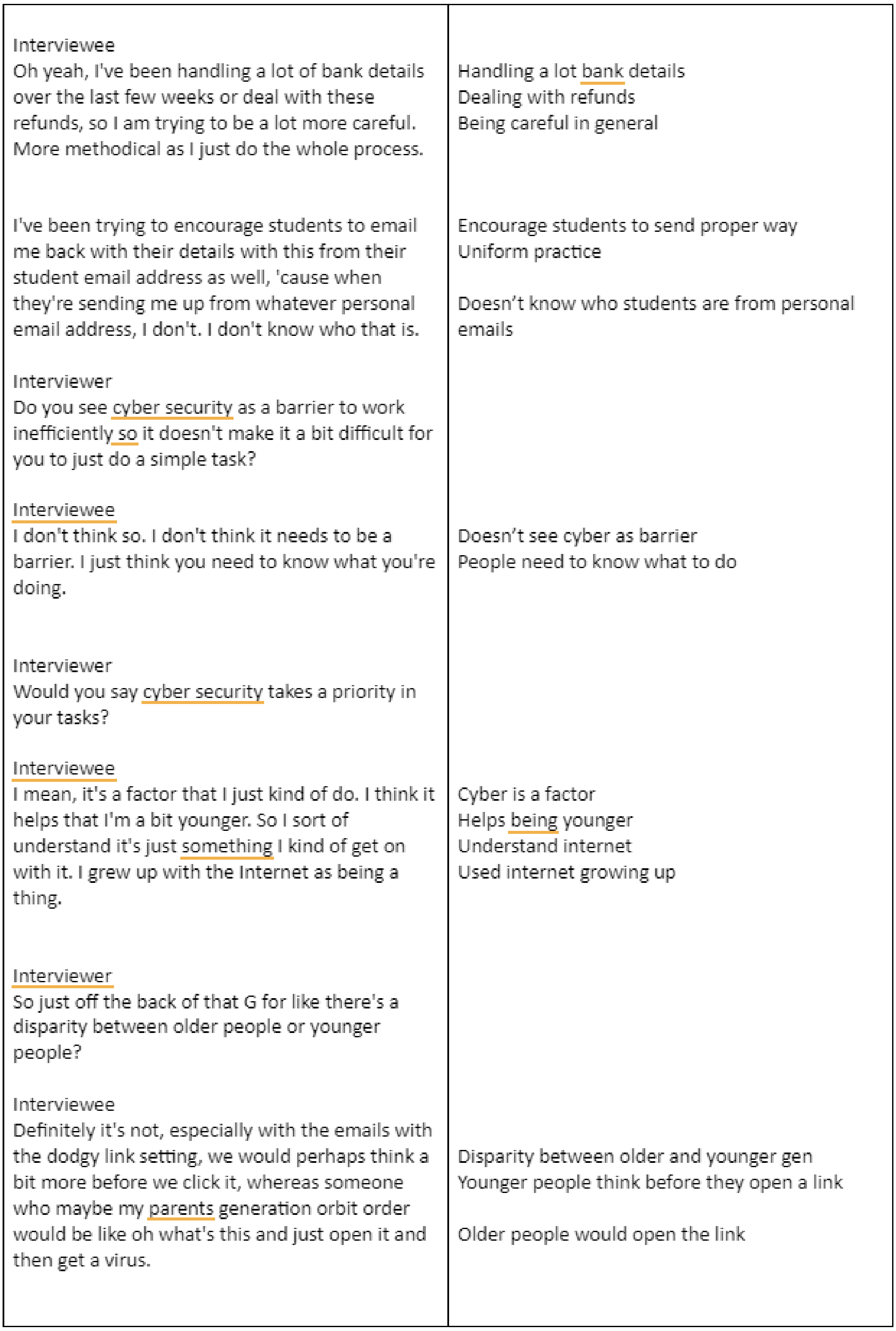
We keep anonymised research data indefinitely, so that it can be used for other research as described above.

Further guidance - to be deleted, do not include in final version

* In some circumstances, the nature of the research will make it difficult to safeguard anonymity of data, which should be explained to participants here and the entire statement modified throughout as appropriate. This explanation should include how their data and /or identity would be shared and the consequences they may face in such instances.

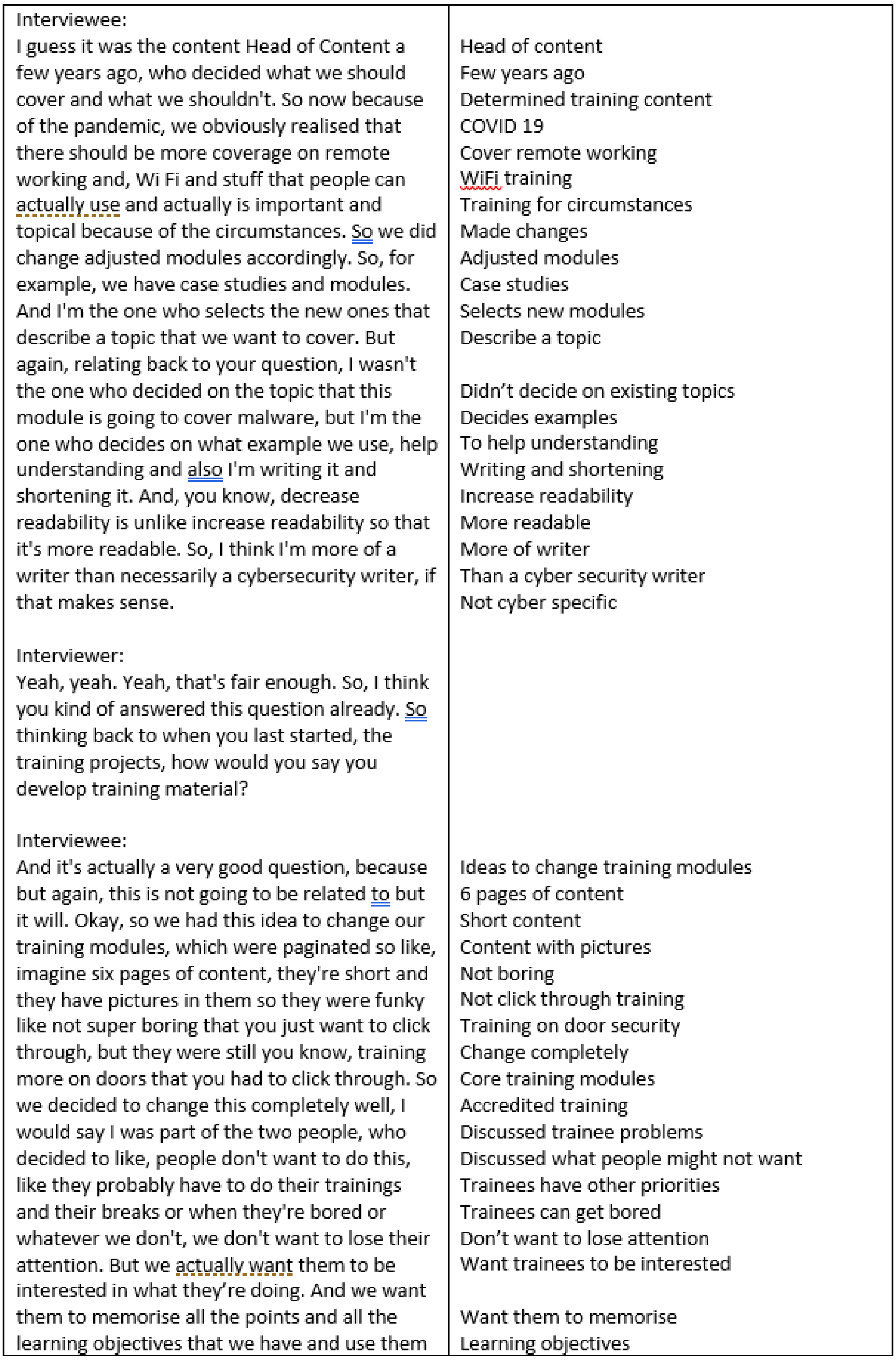
Contact for further information

Appendix J Coded Transcript Sample Study 2 Training selection (Employees)



Interviewee Oh yeah, I've been handling a lot of bank details over the last few weeks or deal with these refunds, so I am trying to be a lot more careful. More methodical as I just do the whole process.	Handling a lot bank details Dealing with refunds Being careful in general
I've been trying to encourage students to email me back with their details with this from their student email address as well, 'cause when they're sending me up from whatever personal email address, I don't. I don't know who that is.	Encourage students to send proper way Uniform practice Doesn't know who students are from personal emails
Interviewer Do you see cyber security as a barrier to work inefficiently so it doesn't make it a bit difficult for you to just do a simple task?	
Interviewee I don't think so. I don't think it needs to be a barrier. I just think you need to know what you're doing.	Doesn't see cyber as barrier People need to know what to do
Interviewer Would you say cyber security takes a priority in your tasks?	
Interviewee I mean, it's a factor that I just kind of do. I think it helps that I'm a bit younger. So I sort of understand it's just something I kind of get on with it. I grew up with the Internet as being a thing.	Cyber is a factor Helps being younger Understand internet Used internet growing up
Interviewer So just off the back of that G for like there's a disparity between older people or younger people?	
Interviewee Definitely it's not, especially with the emails with the dodgy link setting, we would perhaps think a bit more before we click it, whereas someone who maybe my parents generation orbit order would be like oh what's this and just open it and then get a virus.	Disparity between older and younger gen Younger people think before they open a link Older people would open the link

Appendix K Coded Transcript Sample Study 2 Training selection (Content developer)



Interviewee: I guess it was the content Head of Content a few years ago, who decided what we should cover and what we shouldn't. So now because of the pandemic, we obviously realised that there should be more coverage on remote working and, Wi Fi and stuff that people can actually use and actually is important and topical because of the circumstances. So we did change adjusted modules accordingly. So, for example, we have case studies and modules. And I'm the one who selects the new ones that describe a topic that we want to cover. But again, relating back to your question, I wasn't the one who decided on the topic that this module is going to cover malware, but I'm the one who decides on what example we use, help understanding and also I'm writing it and shortening it. And, you know, decrease readability is unlike increase readability so that it's more readable. So, I think I'm more of a writer than necessarily a cybersecurity writer, if that makes sense.	Head of content Few years ago Determined training content COVID 19 Cover remote working WiFi training Training for circumstances Made changes Adjusted modules Case studies Selects new modules Describe a topic Didn't decide on existing topics Decides examples To help understanding Writing and shortening Increase readability More readable More of writer Than a cyber security writer Not cyber specific
Interviewer: Yeah, yeah. Yeah, that's fair enough. So, I think you kind of answered this question already. So thinking back to when you last started, the training projects, how would you say you develop training material?	
Interviewee: And it's actually a very good question, because but again, this is not going to be related to but it will. Okay, so we had this idea to change our training modules, which were paginated so like, imagine six pages of content, they're short and they have pictures in them so they were funky like not super boring that you just want to click through, but they were still you know, training more on doors that you had to click through. So we decided to change this completely well, I would say I was part of the two people, who decided to like, people don't want to do this, like they probably have to do their trainings and their breaks or when they're bored or whatever we don't, we don't want to lose their attention. But we actually want them to be interested in what they're doing. And we want them to memorise all the points and all the learning objectives that we have and use them	Ideas to change training modules 6 pages of content Short content Content with pictures Not boring Not click through training Training on door security Change completely Core training modules Accredited training Discussed trainee problems Discussed what people might not want Trainees have other priorities Trainees can get bored Don't want to lose attention Want trainees to be interested Want them to memorise Learning objectives

Appendix L Coded Transcript Sample Study 2 Training selection

Interviewee: Yeah, I do think there's a fear of lack of knowledge, what you don't know, not knowing. I think there's a fear of not being able to understand stuff. I think if you've got people that aren't, aren't technological. And that's not to say they don't have value in loads of other stuff. So if they're not technological, that tends to be some some concern about, whether they know enough or whether missing information is there a liability, and for those people that are self aware, that's a challenge for them, and that they're aware of, and that can be stressful and, and fear inducing. And then on the flip side of that, those are technological sometimes there can be some cavalier attitude, lackadaisical attitudes to technology. I know best. Oh, yeah. I always, put a firewall on and always use a VPN, and I changed the password. Oh, I've had a breach. I think when you're technological, sometimes you can just make assumptions about assumptions, which, which doesn't tend to happen. On the other side, on the flip side, if you're not technological, usually making mistakes, because you don't know, and there's a fear around, or I don't know enough about this. And I'm worried. And of course, the antidote to that is training. But equally, if it's not your thing, it can be very hard to understand what's the difference between a phishing attack and this other thing? Yeah, I think it's a natural distinction in our company, at least, you're either one thing or you're the other.	Fear What you don't know Fear not been able understand Not technological Valuable in other ways Concerns Missing information Liability Self aware Challenge Stress and fear Technological people Cavalier attitude Complacent attitude Always uses security Technological person Can make assumptions Leading assumptions Doesn't manifest Making mistakes Lack of awareness Fear of unknown Worries Training is solution Hard to understand Disparities Phishing attack Natural distinction Company culture One or other
Interviewer: If training is the solution or the remedy, then what should training look like and what is the most ideal training or most effective training that you think will be suitable for your business?	
Interviewee: It's a great question. If I'm honest, I would like to see training that just is a drip, drip. scenario, say for instance, I use some applications like to use a thing called Rescue Time, which monitors my use of my mobile and my desktop or, how I'm using my time, whether it's productive or watching YouTube or whatever. And it's really useful, but every day tells me, it gives me either	Nudge training Drip fed training Rescue Time Monitors mobile use Monitors time use Measures Productivity Useful Inspirational quote