2022-06

The Importance of the Job Role in Social Media Cybersecurity Training

Ben Salamah, F

10.1109/eurospw55150.2022.00054
2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)
IEEE

The Importance of the Job Role in Social Media Cybersecurity Training

Fai Ben Salamah
School of Engineering, Computing and Mathematics
University of Plymouth
Plymouth, UK
fai.bensalamah@plymouth.ac.uk

Marco A. Palomino
School of Engineering, Computing and Mathematics
University of Plymouth
Plymouth, UK
marco.palomino@plymouth.ac.uk

Maria Papadaki
School of Computing and Engineering
University of Derby
Derby, UK
m.papadaki@derby.ac.uk

Steven Furnell
School of Computer Science
University of Nottingham
Nottingham, UK
Steven.Furnell@nottingham.ac.uk

***Abstract*—Social media has become embedded in our everyday lives, personal activities and the workplace. Thus, educating users on emerging cybersecurity challenges for social media has become imperative. As such, we have investigated the feasibility of an awareness-raising and adaptive cybersecurity training system. Our investigation is aided by a questionnaire, which was administered online using Google Forms. We collected answers from 641 employees from a variety of sectors: education, healthcare, leadership and management, arts, entertainment, police and the military. We found that a one-size-fits-all training approach is highly ineffective, as people's understanding and knowledge can vary greatly. Thus, we have proceeded to identify the factors that influence the success of any given approach. Information such as gender, age, education level, job roles, and training preferences seem essential considerations for developing a robust training strategy. Our investigation concludes that "job role" is the most significant factor associated with people's preferences and perceptions in cybersecurity training. Also, people appear to be in favour of adaptive training. Moreover, a mixed delivery approach is likely to be welcomed.**

***Index Terms*—cybersecurity, education, social media**

1. Introduction

Cyberattacks on social media increased considerably during the COVID-19 pandemic [1]. The United States FBI registered a 300% increase in reported cybercrimes since the outbreak of COVID-19 [2]. Clearly, social media presents opportunities for hackers to obtain information about employees [3], [4]. Indeed, hackers are now employing a myriad of social engineering techniques that involve luring users to open attachments [5], while the total number of social media users has surpassed 3.8 billion—almost 60% of the current world's population [6]. It is important to note that 95% of the cybersecurity breaches are due to human error [2], and the sharing of information that should not be disclosed. However, a large proportion of social media users do not even know how damaging this could be!

Organisations are still struggling to formalise their social media policies. They have been unable to do so as part of their overall risk management process [7]. Given that most cybersecurity incidents within organisations occur due to individual lapses [8], training the staff becomes essential. Technical measures alone are insufficient to prevent all threats. Thus, training users on how to identify threats is of utmost importance [9], [10].

Despite a variety of training approaches—testing [11], analysis of real cases and video training [12], sustainable training [13], e-learning [14], and gaming [15]—the same mistakes are repeated consistently [16]. Existing approaches do not satisfy the needs of all the staff, their learning objectives and preferences [17], [18]. Thus, we aim to investigate staff attitudes towards social media security and training in preparation for the design of a new training approach. As a first step, we have identified key factors that must be considered for developing an effective social media cybersecurity training strategy.

Our investigation is aided by an online survey which allowed us to collect information from 641 Kuwaiti employees in a variety of sectors, ranging from education to defence and healthcare to entertainment. Kuwait is considered one of the top five Arab countries in their use of social media [19], and it is ranked number eight in email malware attacks and number six in frequency of spam attacks [20]. Thus, analysing Kuwait's case provided us with invaluable insight into cybersecurity issues that are present globally. We have also carried out individual interviews with policymakers involved in cybersecurity training, and members of staff who have received cybersecurity training in the past. The training preferences among participants in cybersecurity training appear to be essential for developing a robust training approach.

The remainder of this paper is organised as follows. First, we summarise the related work in adaptive cybersecurity training, and we describe previous attempts at developing staff training programmes. Then, we present the methodology used in our study and the results of our analysis. Finally, our results are discussed, allowing conclusions to be drawn.

2. Related Work

Many factors contribute to developing a successful training programme, and trainers have a huge role to play in increasing the enthusiasm towards the learning process [21]. A proper mix of training delivery approaches has been deemed to be not only advisable but indispensable [8], [11], [22]. Moreover, given the increase of attacks targeting people, a human-centric approach to cybersecurity training, such as the one proposed by Hatzivasilis *et al.* [23], has greater chances to succeed. On the other hand, mandatory and one-size-fits-all approaches fail to encourage staff [8]. Indeed, the training is more effective when employees feel that it is tailored to them [16].

Table 1 presents a wide range of features, methods, and preferences identified in our review of relevant literature. To summarise our findings, we have listed what we consider to be the most relevant issues for each entry on the table—this may be the type of training, the methods recommended by the authors, or some of the challenges pointed out by the corresponding research work.

From the contents of Table 1, we can conclude that changing people's mindsets requires adequate training, and training is the key to mitigating cyber-attacks. The very nature of social media resides on trusting each other, which is a feature that hackers naturally exploit to their advantage. Thus, we propose a training strategy based on the conclusions of the research presented below.

TABLE 1. PREVIOUS WORK

Author(s)	Finding(s)
Cybersecurity Training Importance	
Tittle *et al.* (2021) [9]; Löffler *et al.* (2021) [24].	Technology alone cannot prevent cyber-attacks, and staff training is an effective way to safeguard an organisation's assets.
Security Policies	
Demek, *et al.* (2018) [24].	Security policies need to be straightforward to implement.
The European Union Agency for Cybersecurity (2017) [25].	Policy alone is insufficient to have a secure environment. Training is indispensable.
Factors Leading to Adaptive Training	
Bada, *et al.* (2015) [26].	Cybersecurity training must be free from complications such as technical terms.
European Network and Information Security Agency (2012) [27]; Alshaikh, *et al.* (2018) [11]; Chowdhury and Gkioulos (2021) [28]; Schreuders and Butterfield (2016) [29].	Training must include case studies, real-world stories linked to the trainee's personal life, videos, games, group activities, hands-on training, team building, and competition.
Alshaikh, *et al.* (2018) [11]; Schürmann, *et al.* (2020) [22]; Zhang, *et al.* (2021) [8].	Mixing delivery approaches is better than relying on one.
von Solms and von Solms (2015) [30].	Cartoon videos can be ideal for some age groups.
Awojana and Chou (2019) [31]; Gjertsen, *et al.* (2017) [32].	Gaming approaches make training enjoyable.
Brilingaitė, *et al.* (2020) [21]; European Network and Information Security Agency (2012) [27]; Stockhardt, *et al.* (2016) [10].	Instructor-based training is more effective. Trainers play a huge role; they are the core of any training programme.
Trainees' Challenges	
Haeussinger and Kranz (2013) [14]; Hatzivasilis, *et al.* (2020) [23]; Bada, *et al.* (2014) [26]; Alshaikh et al. (2018) [11]; Furnell and Vasileiou (2017) [16]; Zhang, *et al.* (2021) [8].	Trainees are discouraged when they feel they are not the target audience, and when the training becomes tedious, repetitive and monotonous.
Policymakers and Training Formation's Challenges	
Brilingaitė, *et al.* (2020) [21]; Dhakal (2018) [33].	It is challenging to fit everyone's needs and interests as part of a training programme.
Gratian, *et al.* (2018) [34].	Employees' skills vary widely in an organisation.
Customising the Training	
Aldawood and Skinner (2019) [35]; Pattinson, *et al.* (2018) [36].	Separating trainees based on knowledge, needs and interests yield positive outcomes.
Gasiba, *et al.* (2021) [37]; Zhang et al. (2021) [8]; Toth and Klein (2014) [38]; Pattinson, *et al.* (2018) [36].	Cybersecurity training should be adapted, depending on the employee's job role.
Social Media Cybersecurity Training	
Demek, *et al.* (2018) [7]; Thakur, *et al.* (2019) [39].	Organisations must perform appropriate training about social media cybersecurity.
Social Media Cybersecurity Challenges	
Blackburn, *et al.* (2018) [40]; Parsons, *et al.* (2014) [41]; Thakur, *et al.* (2019) [39]; Zhang and Gupta (2018) [42].	Awareness of social media cybersecurity is rather low.

3. Methodology

Our research is based on qualitative and quantitative methods—an approach known as *mixed* methods [43]. On the qualitative side, we have conducted in-depth interviews, which helped us to enrich the findings of an online survey distributed among relevant stakeholders. This has led us to a detailed understanding of training-related matters that users face on social media.

3.1. The Survey

The survey's design was based on the necessity to recognise employees' observations of cybersecurity threats related to the use of social media. The survey was arranged to take a broad view of the participants.

We used the quantitative methodology for two purposes: first, to discover the correlation among different factors and, second, to recognise the strength of analytical techniques such as relationship and group analysis. We were able to compare our analysis with others, and future studies can contrast their results with ours.

We requested all the participants of our survey to provide us with information about their practices and experiences in social media and their training backgrounds. We asked them questions about their overall thoughts on social media usage. Our questions aimed to recognise the participant's perceptions of the training in general and the cybersecurity training in particular. We selected this approach because electronic surveys have the benefit of facilitating data collection and analysis [44]. The participants of our survey were Kuwaiti employees who use social media and are above eighteen years old.

Although we only gathered information from Kuwait, the conditions of this country allowed us to gain a deep understanding of cybersecurity issues that are present worldwide [20]. In 2014, the Government of Kuwait endeavoured to create its *National Cyber Security Strategy* [45], which brought about a number of measures to identify and decrease cybersecurity challenges. This has placed Kuwait in an ideal situation to offer insight into cybersecurity issues of global relevance. To expand the scope of our research, we sent out our survey to employees in several organisations, and a pilot test was carried out with ten participants. The survey was developed in English and consisted of twenty five questions. The survey comprised three sections: introduction and right to withdraw, demographics, and cybersecurity training.

3.1.1. Introduction and Right to Withdraw. This section consisted of a brief introduction about the project aims, the participant's eligibility, the time required to complete the survey, and their right to withdraw.

3.1.2. Demographics. This section consisted of five questions about demographic details. Demographic questions were used as crucial variables to examine if training preferences depend on different backgrounds. Demographic items that were added as control variables included questions on age, gender, academic status, job role, and years of experience.

3.1.3. Cybersecurity Training. The third section consisted of four questions that concentrate on those who have received cybersecurity training. We needed to identify where they received this training, how many times a year the training was attended, what was the training approach, and whether the training included social media references.

We used different styles of questions for this purpose: multiple choice, checkboxes, short answers, and a five-point *Likert Scale* [46]. Then, the survey ended with a message asking if the participants were interested in joining us for further investigation (interviews) and requesting their contact details if the response was positive.

3.2. Sample Size

Given that this paper attempts to explore how far the staff in the organisations are aware of the matters of cybersecurity, especially when they interact with other people in social media, it became imperative to find out statistics about those organisations. As of 2019, there were 279,982 employees in Kuwait's public sector [47].

We calculated our sample's confidence interval for the population mean. The sample's confidence interval was from 2.76 to 2.92, which resulted in a 99% confidence level [48]. Accordingly, the recommended sample size for our survey was set at 542 participants.

3.3. Reliability

Reliability is the way to measure the quality and consistency of the data obtained. It indicates the consistency of the results when several participants work under different circumstances.

The internal consistency of our data is excellent (strong), as the overall reliability range is 0.902, calculated according to the *confidence interval calculator* [49]—see Table 2 below.

TABLE 2. RELIABILITY

Scale	Items	Cronbach's Alpha Coefficients
Preferences	13	0.895
Perceptions	3	0.920
Adaption	6	0.886

3.4. Interviews

To capture the thoughts of the participants on our research, we conducted detailed, semi-structured interviews under conditions of strict anonymity. The participants belonged to organisations of diverse sectors and sizes. We targeted policymakers involved in training formation and other members of staff who have attended cybersecurity training. We invited all the respondents to our initial survey to participate in the interviews. However, only fifty one participants agreed to be interviewed, and only twenty five of them were available in the end.

Our interview questions were divided into three sections. Each section has unique questions that aim to a specific objective. At the beginning of the interview, we set ten questions that can show us the participants' backgrounds—age, gender, etc. Then, the first section targeted those who can set policies in their organizations and influence training formation. We asked ten questions to policymakers, and five to training formation officers. The second section is for those who have attended social media security training, and we asked them nine questions. The third section was ten general questions that targeted all the participants and involved general questions about cybersecurity and social media knowledge.

Three trial interviews were carried out for each part of the interview questions, one for policymakers, one for training formation officers, and one for cybersecurity trainees. These trial interviews were not part of those reported in our results. They aimed to test the research questions' clarity and coherence, and the potential replies to be expected. The interviews took place over *Zoom*, following the recommendations of Archibald *et al.* [50], and lasted between thirty and forty-five minutes. The interviews were in English and progressed smoothly in a friendly manner.

3.5. Inter-Rater Reliability Test

The interview coding system facilitates an investigation of interviewees and their replies in a single response. A co-occurrence review of the issues resulted in ten combinations of the codes. With the help of the *KALPHA* test [49], we calculated the inter-coder reliability measure. Our data was coded independently by two coders, following the recommendations of Tang, *et al.* [51]. Overall, the coders accepted 83% of the individual responses, with a multi-value nominal alpha coefficient of $mv n\alpha = 0.803$, meaning that coder-evaluated individual interview responses fell in place over 80% of the time, eliminating the possibility of agreement due to chance.

4. Results and Findings

Responses to the questionnaire were collected online through a *Google Form* [44]. The data was processed using *SPSS* [52]. In total, 641 people received the questionnaire and all of them returned their answers.

4.1. Inferential Analysis

The confidence intervals of the *chi-square* test [53], which we used to examine the relationship between our categorical variables, were set to 95% and 99%, respectively. Hence, P values smaller than 0.05 and 0.01 were considered statistically significant in our study.

4.2. Training Preferences

The training preferences of the participants largely depend on the job roles they do. The chi-square test results reveal that twelve out of thirteen training approaches are significantly associated with the participants' job role—see Table 3 in Appendix A at the end of the paper.

The chi-square test also reveals that those who work on IT favour workshops as their preferred method of cybersecurity training, followed by people working in education and related fields. In-class training is preferred by IT employees for several reasons, such as the fact that the training can be finished within a fixed time frame. Contrary to this, people holding management and leadership positions do not seem to like face-to-face classes.

As far as the technical part of cybersecurity training is concerned, face-to-face classes with an expert trainer are preferred over online classes. According to one of the technicians serving in the IT department of a medium-sized company, "One can raise many technical queries and find answers [in face-to-face sessions], which is somewhat cumbersome in online classes; [an online session] does not lead to any strong interactive feelings either". "Another weakness with online training is that you need some kind of enforcement to make the training mandatory," one expert in training formation stated.

People working in IT consider the online training approach to be the most practical one, whereas people in military and defence consider online training only a moderately suitable approach. People holding leadership and management positions do not favour online training in general. However, a middle-aged executive in a large company expressed the following comment during one of our interviews: "Being an HR professional, I always prefer online training as it allows me to discharge my other urgent assignments".

Administrative personnel consider webinars highly helpful. Financial and business operations personnel consider webinars moderately helpful, and IT personnel consider webinars less valuable. Military and defence organisations do not consider this approach useful at all.

Most of the interviewees prefer a face-to-face interaction to strengthen their conceptual understanding. However, due to the COVID-19 pandemic, online (virtual) training has become a necessity, and many of the interviewees called it not only "convenient" but also "exciting". Online training is convenient because people can record the session and watch it at their own convenience.

In summary, online training provides flexibility, but lacks the close interaction that is only possible with face-to-face attendance.

According to the chi-square test, IT employees consider posters extremely valuable, but they are only slightly valuable for people from the financial and business fields. People from education, and military and defence establishments, do not consider posters important.

Those who work in IT find social media to be an extremely valuable tool, but it is only moderately suitable for those working in the healthcare sector. It has been found slightly valuable by those who are involved in administrative and office jobs. People working in IT strongly agree that offering incentives to raise cybersecurity awareness is extremely beneficial. At the same time, those who work in financial services and businesses find incentive offerings moderately beneficial. People working in management and leadership do not find incentives at all useful for raising cybersecurity awareness.

Storytelling has been found to be an extremely valuable approach by those who work on IT. However, those who work on military and defence find this approach only slightly useful, whereas people involved in education and training, as well as those working in arts, sports, and entertainment, find the approach moderately useful.

One of the trainees with an IT role asserted that she liked listening to real stories related to cyber-attacks. She said: "I like to attend conferences with real people that have real stories." Another interviewee working in the IT field, who attended a cybersecurity training programme in London, informed us that she enjoyed listening to a hacker explaining how he took advantage of the carelessness of Internet users. She said: "I learned a lot from the stories and incidents narrated by the speakers in my previous training programme; the story session was immediately followed by a question-answer session from the audience". Another interviewee from the education sector said: "I have listened to many stories on cybersecurity from my colleagues, which has made me conscious of such issues!" and someone from military roles added: "Listening to real stories on cybersecurity excites me."

Tip-sheets are considered an extremely helpful approach by those working in IT, and a somewhat useful approach by those working in management and leadership. On the other hand, people involved in businesses and financial services consider this method of training "not useful". To be more precise, interviewees offered different comments when discussing tip-sheets as a training alternative. Some people said, "Tip-Sheets for gaining understanding about social media policy is a good approach". However, many others said, "It is not the best way of learning about social media policy protocols."

Conducting mock attacks as part of the training is highly supported by people working in IT, followed by those who are involved in administrative roles. This approach of training is approved moderately by those who work in business and financial fields. Management and leadership personnel does not find this approach useful.

Our interviews show a number of cases in which phishing emails were used by different firms to verify and increase the awareness of their employees. As expressed by some of our interviewees, this approach has also proved useful to identify those who require training.

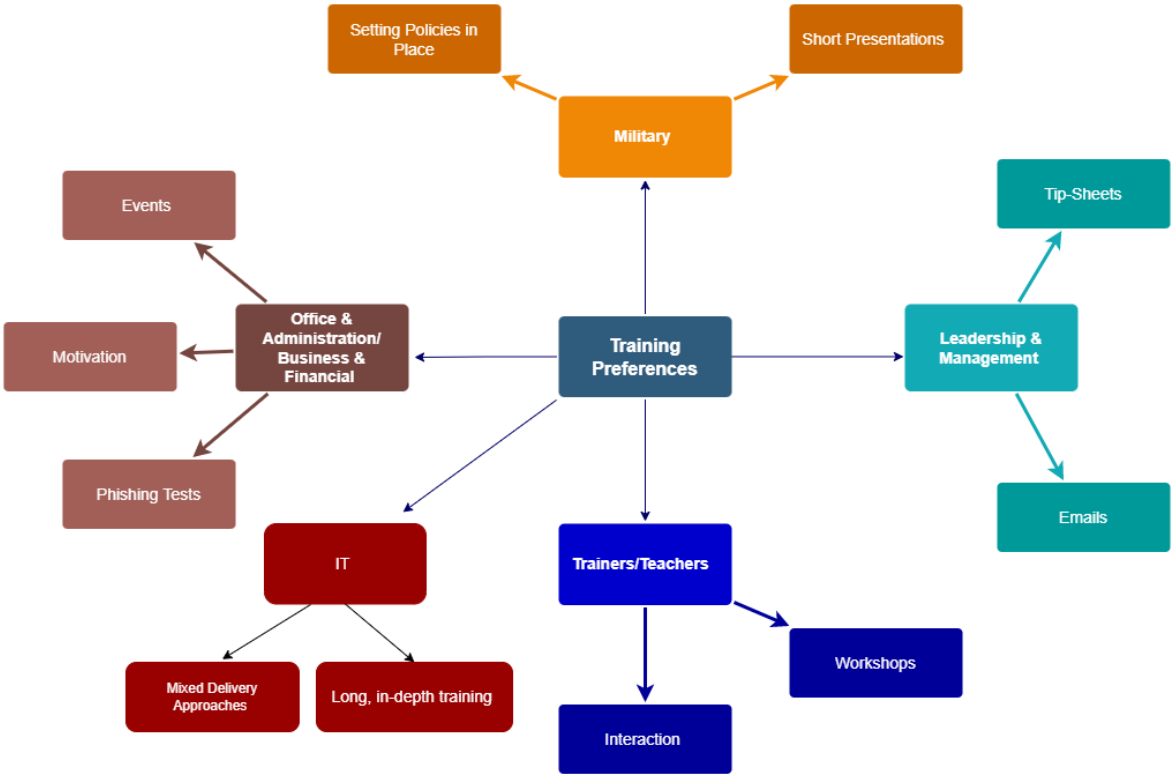

Figure 1. Training Preferences Based on Job Roles

Raising awareness through events appears to be extremely valuable for those working in IT, followed by those in administrative and office jobs. People working in the finance and business sector support events only moderately; yet, people occupying management and leadership positions do not consider such an approach useful.

Emails are the preferred approach by people in management and leadership. Even people serving in administrative roles consider this approach useful. However, people attached to defence and military, along with the business and financial services, do not consider this approach pragmatic. Emails are used for giving guidelines and tips for using the Internet. Many organisations have resorted to using emails during the COVID-19 pandemic. One of the experts from a medium-sized organisation argued that emails could be enough for apprising employees with some level of awareness; yet, she said: "I am not sure if this is sufficient or not".

For many trainers, the gaming approach is highly useful. A trainer told us: "Games can teach people faster than mere words because it is a practical experience that people do not easily forget". However, many involved in IT or administrative roles find it only moderately helpful.

Sometimes, the gaming competition approach among participants accelerates the learning process. One of the female interviewees working in the IT sector said: "The gaming approach is the best approach I have experienced ever as I am fully involved in my learning". At the same time, people involved in leadership or management positions, or military establishments, consider gaming only slightly beneficial. Moreover, people attached with businesses or doing financial services view gaming as an ineffective method.

5. Discussion

This study addresses the need of educating employees on social media risks. Löffler, *et al.*, [24] have pointed out that training is the key to mitigating cyberattacks, and Chowdhury and Gkioulos [28] have stated that a significant investment in organisations is necessary to train the staff. Nevertheless, the issue remains challenging for many organisations, as people keep on repeating the same mistakes. For one reason or another, people remain the weakest link in any security chain [11], [54].

According to Toth and Klein [38], training needs to be based on trainees' roles. For example, training for those who work in stores, and those who deal with customers, must be different. This agrees with the findings of other studies such as [8], [11], [32], emphasising the customisation of cybersecurity training for favourable outcomes.

This study differentiates people's training based on factors such as age, gender, education, years of experience, and, of course, the job role that people have. This matches the findings of Aldawood and Skinner [35] and Morton *et al.* [15]. The one-size-fits-all approach is almost certain to fail, as suggested by various studies [11], [16], [25].

Our research also reveals that many other factors may also lead to cybersecurity training failure. For example, when the training does not coincide with the interests of the trainees, or when the trainees feel that they are not the target audience [14], the training is likely to fail [25].

While it is difficult to develop a training strategy that meets everyone's interests and needs [21], [33], the participants do agree on some common grounds for making the training adaptive. The first and foremost is that the training should be free from any complexity [26].

Employing a mixed delivery training approach is always more fruitful than using a single approach, as reported by [11], [13], [25]. Security policies should be clear, straightforward, and easy in their implementations—as supported by Demek *et al.* [7]. The trainer's role is crucial for the success of the approach, which is supported by Brilingaitė *et al.* [21] and the recommendations made by ENISA [27]. A training programme more pragmatic for trainees [4]. In other words, one-to-one interaction between the trainer and trainees has more chance of productive and successful outcomes [41].

Our study discovered that customised cybersecurity training has a greater chance to succeed, as opposed to generalised training. This aligns well with many previous studies published by various researchers [11], [15], [16], [25], [35]. The reason behind this is that people vary in their preferences, level of awareness, and the responsibilities they undertake. For example, people in leadership and management roles differ in their tasks from those who work in administrative services or day-to-day office tasks. Thus, customised training can lead to better outcomes. That is why a successful trainer makes every attempt to understand the audience before a training session takes place, as suggested by Bada *et al.* [26].

Workshops emerged as the most favoured training method in our study. Other studies agreed with us [38], [55]. Toth and Klein [38] describe workshops as an efficient training method, and Pedley *et al.* [55] as a reliable method. However, workshops are not favoured by those who hold management and leadership positions, because such an approach is time-consuming for them. Instead, they insist on tip-sheets and email messaging.

People in management and leadership positions do not support the idea of giving incentives to staff to raise cybersecurity awareness. While email messaging is favoured by them, they do not support using emails for conducting mock attacks. Similarly, people working on defence and military establishments do not favour long training sessions or workshops; they do not support emails either. Moreover, they are not in support of using posters or organising webinars. They prefer organising short online training classes.

We have found gaming as another one of the most acceptable training methods by the participants of our study. For most of them, gaming is an exciting way of learning cybersecurity lessons. Most trainees prefer workshops and face-to-face sessions. Trainers and those who create training programmes are also in support of such modes of training. However, trainers do not support posters for delivering information.

Trainers prefer mixed delivery methods which include a storytelling approach to engage with the trainees emotionally—this agrees with the findings of Schürmann *et al.* [22] and Zhang *et al.* [8]. Trainers also propose a team-building approach which combines real-world case studies and hands-on training—this agrees with Chowdhury and Gkioulos [28].

People from administrative roles, and people from business and financial services, have many similarities as far as their preferences are concerned. The people from these two categories prefer events, incentives for learning, learning through webinars, and mock attacks.

People from administrative roles, and people from business and financial services, want to come out of their job routines and interact as much as possible with other staff members for expediting their learning process.

It must be noted that people working on IT greatly support most of the cybersecurity training approaches, emphasising their usefulness. It seems that having a good understanding of technology, allows them to understand that even a small lapse by an employee can put the entire organisation at risk; therefore, they fully endorse the importance of raising security awareness for all, as stated in [38]. Moreover, IT workers support longer training programmes. For them, the webinar is the least preferred method of training.

IT staff like to undertake routine programmes at regular intervals with updated content, so that everyone in the organisation remains up-to-date, regardless the ongoing social engineering practices of hackers.

A limitation of this study is that only 28% of the people surveyed had previous cybersecurity training, and those interviewed did not have experience in all the available training approaches. It was challenging for them to compare different training methods as far as their effectiveness is concerned. Owing to this, preferences mentioned, challenges faced, and factors described by participants need to be interpreted with caution. It is suggested, therefore, that future studies focus on participants who have been trained with more than one approach to analyse the reasons for their preferences.

Summarising the discussion, while people differ on the level of agreement on having customised training, most of them agree on classifying the training based on the job role they perform, rather than having a single system of training for all. Moreover, a mixed delivery approach is likely to deliver more favourable outcomes.

6. Conclusions

Raising cybersecurity awareness is considered crucial by many organisations at present. However, having a single training approach to fit all is not an effective way to train employees, as people vary in their preferences and backgrounds. In this study, we have found through a qualitative and quantitative analysis that the most important factor associated with people's cybersecurity training preferences is their job roles.

Our interview results reveal that most of the participants are in favour of having an adaptive training programme. To fulfil the objective of developing an adaptive cybersecurity training (ACST) programme, each training component needs to be customised. Short training sessions are preferred over long ones by a large proportion of participants. Trainers need to adjust to the requirements of the trainees. At the same time, non-technical vocabulary is a must for creating interest and involvement in training. Training content should be relevant, interactive and engaging. Although organisations can undertake various activities to raise security awareness among their employees, trainers can go a long way to improve the quality of their training programmes. The point to be noted is that cybersecurity awareness is an ongoing process that should not only be limited to times of crisis.

Participants do have their preferences towards offline and online training, depending upon whether they are new in the field or have been exposed to cybersecurity for a while. It is no surprise that often, they are found to have been insisting on specialised training rather than generalised one, because they have already undertaken some kind of training in the past. People do have numerous other questions that they look forward to answering by appropriate training programmes.

Cybersecurity training must take into account the job roles of the trainees along with factors such as gender, age, education level, and years of experience. In other words, preferences, backgrounds, and perceptions of trainees are important considerations for developing a robust training programme. Making the trainees feel that the programme is unique to them is extremely useful. Matching delivery approaches with trainees' preferences makes the training adaptive, and that is how organisations are likely to succeed in their endeavours to create an effective ACST programme. *The findings of this paper give us insight into the development of an ACST framework to enable employees to thwart cyber-attacks that are often encountered by many on social media platforms*.

References

[1] L. L. Griffin, "The Effectiveness of Cybersecurity Awareness Training in Reducing Employee Negligence Within Department of Defense (DoD) Affiliated Organizations-Qualitative Exploratory Case Study," Ph.D. dissertation, Capella University, 2021.

[2] D. Milkovich, "15 Alarming Cyber Security Facts and Stats," Cybint Solutions, 2021, https://www.cybintsolutions.com/cyber-security-facts-stats/.

[3] E. Follett, *Discussing the Impact that Social Media Has on Enterprise Cyber Security*. Bournemouth, UK: Bournemouth University, 2021.

[4] P. Van Schaik, J. Jansen, J. Onibokun, J. Camp, and P. Kusev, "Security and privacy in online social networking: Risk perceptions and precautionary behaviour," *Computers in Human Behavior*, vol. 78, pp. 283–297, 2018.

[5] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol. 105, p. 102248, 2021.

[6] S. Kemp, "Digital 2020: 3.8 billion people use social media," We Are Social Ltd, 2020.

[7] K. C. Demek, R. L. Raschke, D. J. Janvrin, and W. N. Dilla, "Do Organizations Use a Formalized Risk Management Process to Address Social Media Risk?" *International Journal of Accounting Information Systems*, vol. 28, pp. 31–44, 2018.

[8] Z. J. Zhang, W. He, W. Li, and M. Abdous, "Cybersecurity Awareness Training Programs: A Cost–Benefit Analysis Framework," *Industrial Management & Data Systems*, 2021.

[9] E. Tittle, J. M. Stewart, and M. Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*. John Wiley & Sons, 2006.

[10] S. Stockhardt, B. Reinheimer, M. Volkamer, P. Mayer, A. Kunz, P. Rack, and D. Lehmann, "Teaching phishing-security: which way is best?" in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2016, pp. 135–149.

[11] M. Alshaikh, S. B. Maynard, A. Ahmad, and S. Chang, "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations," in *51st Hawaii International Conference on System Sciences*, Honolulu, HI, 2018, pp. 5085–5094.

[12] D. Tayouri, "The human factor in the social media security–combining education and technology to reduce social engineering risks and damages," *Procedia Manufacturing*, vol. 3, pp. 1096–1100, 2015.

[13] M. C. Scholl, F. Fuhrmann, and L. R. Scholl, "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations," in *Annual Hawaii International Conference on System Sciences*. Honolulu, HI: IEEE Computer Society, 2018, p. 2235–2244.

[14] F. Haeussinger and J. Kranz, "Understanding the Antecedents of Information Security Awareness–An Empirical Study," in *Americas Conference on Information Systems (AMCIS)*, Chicago, Illinois, USA, 2013.

[15] G. D. Morton, M. Mihelic, M. Moniz, P. R. Thornton, R. Pressley, and L. Lee, "Mission-based, Game-Implemented Cyber Training System and Method," 2018, patent No: WO2018175551A1.

[16] S. Furnell and I. Vasileiou, "Security education and awareness: just let them burn?" *Network Security*, vol. 2017, no. 12, pp. 5–9, 2017.

[17] B. D. Caulkins, K. Badillo-Urquiola, P. Bockelman, and R. Leis, "Cyber workforce development using a behavioral cybersecurity paradigm," in *2016 International Conference on Cyber Conflict (CyCon US)*. IEEE, 2016, pp. 1–6.

[18] L. Christopher, K.-K. Choo, and A. Dehghantanha, "Honeypots for employee information security awareness and education training: a conceptual easy training model," in *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Elsevier, 2017, pp. 111–129.

[19] M. M. Alansari, Z. M. Aljazzaf, and M. Sarfraz, "On Cyber Crimes and Cyber Security," in *Developments in Information Security and Cybernetic Wars*. IGI Global, 2019, pp. 1–41.

[20] G. Cleary, M. Corpin, and O. Cox, "Symantec Internet Security Threat Report," Symantec Corporation, Mountain View, CA, Tech. Rep. 23, 2018, https://docs.broadcom.com/doc/istr-23-executive-summary-en.

[21] A. Brilingaitė, L. Bukauskas, and A. Juozapavičius, "A framework for competence development and assessment in hybrid cybersecurity exercises," *Computers & Security*, vol. 88, p. 101607, 2020.

[22] C. Schürmann, L. H. Jensen, and R. M. Sigbjörnsdóttir, "Effective cybersecurity awareness training for election officials," in *International Joint Conference on Electronic Voting*. Springer, 2020, pp. 196–212.

[23] G. , S. Ioannidis, M. Smyrlis, G. Spanoudakis, F. Frati, L. Goeke, T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis *et al.*, "Modern aspects of cyber-security training and continuous adaptation of programmes to trainees," *Applied Sciences*, vol. 10, no. 16, p. 5702, 2020.

[24] E. Löffler, B. Schneider, T. Zanwar, and P. M. Asprion, "Cysecescape 2.0—a virtual escape room to raise cybersecurity awareness," *International Journal of Serious Games*, vol. 8, no. 1, pp. 59–70, 2021.

[25] European Union Agency for Cybersecurity, "Stocktaking of Information Security Training Needs in Critical Sectors," Dec. 2017, https://www.enisa.europa.eu/news/enisa-news/.

[26] M. Bada, A. M. Sasse, and J. R. Nurse, *Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?* Global Cyber Security Capacity Centre, 2014.

[27] European Network and Information Security Agency (ENISA), "Collaborative Solutions for Network Information Security in Education," Dec. 2012, https://www.enisa.europa.eu/publications/.

[28] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Computer Science Review*, vol. 40, p. 100361, 2021.

[29] Z. C. Schreuders and E. Butterfield, "Gamification for Teaching and Learning Computer Security in Higher Education," in *2016 USENIX Workshop on Advances in Security Education (ASE 16)*, 2016.

[30] R. Von Solms and S. Von Solms, "Cyber Safety Education in Developing Countries," *Systemics, Cybernetics and Informatics*, vol. 13, no. 2, pp. 14–19, 2015.

[31] T. Awojana and T.-S. Chou, "Overview of Learning Cybersecurity Through Game Based Systems," in *ASEE Conference for Industry & Education Collaboration (CIEC)*, New Orleans, LA, Feb. 2019.

[32] E. G. B. Gjertsen, E. A. Gjære, M. Bartnes, and W. R. Flores, "Gamification of information security awareness and training." in *International Conference on Information Systems Security and Privacy*, 2017, pp. 59–70.

[33] R. Dhakal, "Measuring the effectiveness of an information security training and awareness program," 2018.

[34] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *computers & security*, vol. 73, pp. 345–358, 2018.

[35] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues," *Future Internet*, vol. 11, no. 3, p. 73, 2019.

[36] M. R. Pattinson, M. A. Butavicius, B. Ciccarello, M. Lillie, K. Parsons, D. Calic, and A. McCormac, "Adapting cyber-security training to your employees." in *HAISA*, 2018, pp. 67–79.

[37] T. Gasiba, U. Lechner, and M. Pinto-Albuquerque, "Cybersecurity challenges for software developer awareness training in industrial environments," in *International Conference on Wirtschaftsinformatik*. Springer, 2021, pp. 370–387.

[38] P. Toth and P. Klein, "A Role-Based Model for Federal Information Technology/Cybersecurity Training," *National Institute of Standards and Technology (NIST)*, vol. 800, no. 16, pp. 1–152, 2014.

[39] K. Thakur, T. Hayajneh, and J. Tseng, "Cyber security in social media: challenges and the way forward," *IT Professional*, vol. 21, no. 2, pp. 41–49, 2019.

[40] J. Blackburn, E. De Cristofaro, M. Sirivianos, and T. Strufe, "Cybersafety in modern online social networks (dagstuhl reports 17372)," in *Dagstuhl Reports*, vol. 7, no. 9. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[41] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "A study of information security awareness in australian government organisations," *Information Management & Computer Security*, 2014.

[42] Z. Zhang and B. B. Gupta, "Social media security and trustworthiness: overview and new direction," *Future Generation Computer Systems*, vol. 86, pp. 914–925, 2018.

[43] C. A. McKim, "The value of mixed methods research: A mixed methods study," *Journal of mixed methods research*, vol. 11, no. 2, pp. 202–222, 2017.

[44] S. Castro, "Google forms quizzes and substitution, augmentation, modification, and redefinition (samr) model integration," *Issues and Trends in Educational Technology*, vol. 6, no. 2, 2018.

[45] Communications and Information Technology Regulatory Authority, *National Cyber Security Strategy for the State of Kuwait 2017-2020*. CITRA, 2017.

[46] A. Joshi, S. Kale, S. Chandel, and D. K. Pal, "Likert Scale: Explored and Explained," *British Journal of Applied Science & Technology*, vol. 7, no. 4, pp. 396–403, 2015.

[47] Kuwait Central Statistical Bureau, "Population Estimates," 2021.

[48] Calculator.net, "Confidence Interval Calculator," 2022.

[49] K. De Swert, "Calculating Inter-Coder Reliability in Media Content Analysis Using Krippendorff's Alpha," *Center for Politics and Communication*, vol. 15, 2012.

[50] M. M. Archibald, R. C. Ambagtsheer, M. G. Casey, and M. Lawless, "Using Zoom Videoconferencing for Qualitative Data Collection: Perceptions and Experiences of Researchers and Participants," *International Journal of Qualitative Methods*, vol. 18, pp. 1–8, 2019.

[51] W. Tang, Y. Cui, and O. Babenko, "Internal consistency: Do we really know what it is and how to assess it," *Journal of Psychology and Behavioral Science*, vol. 2, no. 2, pp. 205–220, 2014.

[52] R. D. Yockey, *SPSS demystified: A simple guide and reference*. Routledge, 2016.

[53] M. McHugh, "The chi-square test of independence. biochemiamedica. 2013;: 143–149."

[54] A. Ghazvini and Z. Shukur, "Awareness Training Transfer and Information Security Content Development for Healthcare Industry," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 5, pp. 361–370, 2016.

[55] D. Pedley, T. Borges, A. Bollen, J. N. Shah, S. Donaldson, S. Furnell, and D. Crozier, "Cyber security skills in the uk labour market 2020," 2020.

Appendix A.
Experimental Data

TABLE 3. CHI-SQUARE RESULTS (JOB ROLE AND TRAINING PREFERENCES)

1-WORKSHOPS (x2 =54.3888, df = 32, p-value = .008)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	1	3.3	0	1.6	0	0.4	8	2.9	2	1.8	0	0.5	2	1.9	1	1.1
Extremely	37	32	26	15.7	2	3.8	29	27.8	12	14.7	4	5.2	13	17.8	11	10.9
2- ONLINE TRAINING (x2 =67.590, df = 32, p-value = .000)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	5	6.7	1	3.311.3	1	0.8	11	5.8	5	3.6	0	1.1	4	3.7	1	2.3
Extremely	23	17.7	17		4	2.1	10	15.4	8	9.6	3	2.9	3	9.8	5	6
3- POSTERS (x2 =51.495, df = 32, p-value = .016)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	13	9.8	3	4.8	0	1.2	9	8.5	7	5.3	0	1.6	3	5.4	6	3.3
Extremely	15	14.3	12	7	5	1.7	13	12.5	4	7.8	4	2.3	4	8	1	4.9
4- GAMES (x2 =53.582, df = 32, p-value = .010)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	7	8.1	2	4	1	1	8	7.1	7	4.4	3	1.3	3	4.5	3	2.8
Extremely	25	14.3	15	9.3	0	2.2	16	16.4	9	10.2	3	3.1	8	10.5	2	6.4
5-WEBINARS (x2 =67.987, df = 32, p-value = .000)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	2	6.9	1	3.4	2	0.8	9	6	5	3.8	1	1.1	2	3.9	6	2.4
Extremely	18	17.5	13	8.6	1	2.1	18	15.2	11	9.5	1	2.9	6	9.7	3	5.9
6-STORIES (x2 =70.034, df = 28, p-value = .000)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	5	5.5	1	2.7	1	0.6	8	4.8	2	3	2	0.9	3	3.1	1	1.9
Extremely	28	27.3	21	13.4	7	3.2	19	23.7	18	14.8	5	4.5	11	15.1	3	9.3
7- SOCIAL MEDIA (x2 =22.345, df = 24, p-value = .012)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	5	4.3	0	2.1	1	0.5	6	3.7	3	2.3	0	0.7	1	2.4	2	1.5
Extremely	23	24.6	19	12.1	6	2.9	16	21.4	16	13.4	3	4	10	13.7	8	8.4
8-OFFER INCENTIVE (x2 =62.216, df = 32, p-value = .001)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	5	5.3	0	2.6	1	0.6	10	4.6	3	2.9	0	0.9	2	2.9	1	1.8
Extremely	30	30.6	24	15	2	3.6	28	26.6	12	16.6	5	5	13	17	10	10.4
9-TIP-SHEETS (x2 =62.577, df = 32, p-value = .001)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	7	9.1	3	4.5	1	1.1	9	7.9	10	4.9	2	1.5	4	5	1	3.1
Extremely	16	12.4	12	6.1	1	1.5	8	10.8	6	6.7	2	2	2	6.9	2	4.2
10-CONDUCT MOCK ATTACK (x2 =64.730, df = 32, p-value = .001)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	28	21.5	1	10.5	2	2.5	9	7.9	10	11.7	0	3.5	17	12	8	7.3
Extremely	17	20.8	16	10.2	2	2.4	8	10.8	16	11.3	1	3.4	8	11.6	7	7.1
11-AWARENESS RAISING EVENTS (x2 =64.730, df = 32, p-value = .001)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	6	8.8	2	4.3	1	1	17	7.7	8	4.8	0	1.4	2	4.9	1	3
Extremely	23	18.4	15	9	2	2.2	15	16	1	10	5	3	7	10.2	4	6.3
12- EMAILS (x2 =64.730, df = 32, p-value = .001)																
	Edu, Training		Computer & IT		Healthcare		Leadership		Business		Art, Design		Office		Military	
	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp	Count	Exp
Not Useful	22	23.4	13	11.5	7	2.8	20	20.4	18	12.7	3	3.8	10	13	5	8
Extremely	14	17	9	8.3	1	2	23	14.8	4	9.2	3	2.8	9	9.4	5	5.8