

Client-Centred Cybercrime Training: A Scottish SME Case Study

Juraj Sikra^{1,2}[0000-0003-4557-1256]

Karen V. Renaud^{2,3,4,5}[0000-0002-7187-6531]

Daniel R. Thomas²[0000-0001-8936-0683]

¹ Karlsruhe Institute of Technology (KIT)

² University of Strathclyde

³ Rhodes University (Department of Information Systems)

⁴ University of South Africa (School of Computing)

⁵ Abertay University (Division of Cybersecurity)

{juraj.sikra,karen.renaud,d.thomas}@strath.ac.uk

Abstract. The UK's neoliberal government cyber responsabilises Small-to-Medium enterprises (SMEs), meaning that they receive advice but little direct support if they fall victim to a cyber attack. Possibly as a direct consequence, SMEs tend not to report falling victim to cybercrimes. The aim of this research was to develop, deliver, and evaluate a client-centred cybercrime training session with an accompanying booklet as means of engendering post-attack closure, upskilling, enhancing knowledge and improving reporting incidence. We surveyed nine staff of an attacked SME to elicit their training preferences; six staff members subsequently attended and five supplied feedback in the form of a post-training survey. Two staff members were also interviewed. We provide a list of five guidelines that were derived from our experiences in delivering this training. It became clear that the UK government's responsabilization of Scottish SMEs did indeed appear to deter staff from reporting cybercrimes to Police Scotland.

Keywords: Cybercrime · Responsibilization · Reporting · Training · Small-to-medium sized enterprises (SMEs)

1 Introduction

Capitalising on the findings by Bada *et al.* [1], we have taken a case study approach [6] to develop a bespoke cybercrime training for a Scottish Small-to-Medium Enterprise (SME) that had fallen victim to ransomware. Even though Bada *et al.* [1] were mainly concerned with delivering training on Privacy Enhancing Technologies (PETs), their research angle is closely aligned to cyber and particularly cyber-resilience. Cyber-security is related to securing a system from an attack [16] whereas cyber-resilience is related to the system's ability to recover from an attack [20].

In this context, training teaches employees how to prevent stressors to the cyber system or to reduce their impacts post-onset. In our case, the stressors are cyber-attacks and cybercrime and the cyber systems are the software and hardware components of an SME. Bada *et al.* [1, p. 278] explain that cyber-resilience frameworks are often produced for technically-minded people. However, the authors themselves then also recruited SME participants from IT, science, technical activities and public administration. We, on the contrary, engaged with an SME from a deprived area in Scotland which employed staff with minimal understanding of cyber-resilience, thereby addressing a research gap. Our approach reflects the assumptions of Chetty [6, p.75], who states that case studies investigate the SME’s status quo within a real-life setting, the boundaries between the context and the research question being less than clear cut and utilising multiple sources of evidence.

The SME operates in the West of Scotland, which is an area that contains some of the nation’s most deprived regions [17]. For that reason, SMEs are a vital source of employment and contribute to community life.

Policy-makers should also take this research seriously. The Small Business Survey Scotland 2022-23 (SBSS 2022-23) identified that 75% SMEs used external finance with many accessing multiple methods simultaneously such as credit cards (37%), leasing or hire purchases (30%) and bank overdrafts (28%). Yet, when it comes to reporting on the obstacles the SMEs face, the SBSS 2022-23 does not mention cybersecurity risks. We interpret the evidence from the SBSS 2022-23 as an example of responsabilization by omission. Responsibilization in cybersecurity occurs when the state transfers responsibility for cybersecurity onto the SMEs [15]. Here, the SBSS 2022-23 has identified that SMEs simultaneously use multiple methods of external finance, yet it has omitted the cybersecurity risks that external financing carries. We argue that this omission is there because it is implicit that SMEs alone are responsible for managing cybersecurity risks and cybercrime harms. Policy-makers must address these types of responsabilizing omissions to support struggling SMEs.

The paper is structured in the following way: In Section 2 (Methods), we guide the reader through the methodology used to design this study. In Section 3 (Results), we describe the results of the study which contain the Training Development, Training Delivery, and Training Evaluation with the use of participants’ responses.

In Section 4 (Discussion), we use the insights from the results to formulate a set of five guidelines for training. Finally, the Conclusion integrates the findings and offers justification for further research.

2 Methods

2.1 Design

Quantitative Section The purpose of this research was to evaluate a client-centred cybercrime training for victims who are staff of an SME. We compiled

two Qualtrics questionnaires for this training. The aim of the pre-training questionnaire was to gather the staff’s requirements for training. The results from this questionnaire served to devise the client-centred cybercrime training. The aim of the post-training questionnaire was to gather staff’s feedback after the training. We then compared the pre-training and post-training questionnaires to evaluate the effectiveness of the training.

The core part of the training was making it engaging and playful [10]. Next, expertise of designing [18] and evaluating [19] an academic course that was delivered during the Russian invasion of Ukraine was used based on the assumption that approaches that mitigate negative emotions during learning in war will be useful for cybersecurity unaware employees of an attacked SME.

We did not neglect the empirical component and as our approach was designed to diligently map out increases in self-rated knowledge over time, but also changes in emotions in response to new and potentially slightly unsettling cybercrime material. Lastly, we included the rating of lecturer’s supportiveness as an added factor that could be used to make inferences from scores.

Also, research that focused on designing a student-led curriculum to cyber-resilience was utilised [14]. These findings underpin the current research because we have taken the view that participants themselves ought to identify their learning needs to which the training will be reflexive. We also followed the recommendations of prior research and focused on the use of real-world examples during training [12].

We also made important insights for the questionnaire design by highlighting the influence of computer anxiety as a mediating factor over IT performance [21]. Hence, we integrated three Likert scales measuring depression, anxiety, and confidence with respect to preventing cybercrime in the pre-training and post-training questionnaires.

Qualitative Section This segment of research aims to evaluate how people’s views and practices in cyber-resilience evolved since they have received the training after a period of at least eight weeks. We aimed to enrich the research into client-centred cybercrime training as it was merely based on quantitative surveys. Hence, introducing the qualitative interviews aided a more holistic evaluation of this approach.

The participants received the interview questions, the information sheet and consent form in advance. These were supplied in advance to make them more comfortable but in addition there was no added value to spontaneity.

2.2 Participants

Quantitative Section - Survey This part of the study employed an online pre-training and post-training questionnaire which contained the consent form. ⁶.

⁶ The full questionnaire is available in the Appendix 5. The ID of the approved ethical application is 2161.

Qualitative Section - Interview This section employed a semi-structured interview which contained the consent form. Though the initial plan was to interview the participants in person, due to practical constraints placed upon the SME, both participants decided to submit written responses to the interview questions⁷.

2.3 Analysis

Survey The data were analysed with Qualtrics by comparing the pre-training and post-training scores, which is rooted in the methods of Bunge [5], to get an indication of change in mood as a measurement of the intervention. In addition, the pre-training Likert scale scores were contrasted with post-training scores in cases where participants have submitted both sets of scores to get an indication of changes in knowledge acquisition.

Interview The data were analysed in accordance with Braun and Clarke’s [4, p. 6] description of “*coding reliability thematic analysis (TA)*”, which is an approach where: “*Themes are developed early in the analytic process prior to or following some data familiarisation, and often reflecting data collection questions.*” Hence, in line with Braun and Clarke’s theorising, our themes are best understood as summaries of particular topics, mainly in connection to the training effectiveness and improved cybercrime reporting.

3 Results

Training Development We sought to ensure a supportive approach, which was informed by psychotherapeutic theory to mitigate any anxiety towards academics.

Therefore, the booklet - “Client-centred cybercrime training for Scottish small-to-medium sized enterprises” and approach were built after sampling people’s subjective level of knowledge alongside desired improvement.

Specific quotes from the forms were used to add detail to the training materials and approaches to delivery. Generally speaking, the staff noted that the need for attending the training emerged as a result of falling victim to an attack, as one staff member explained in their pre-training form:

“As a team we recently fell victim to a cyber attack on our reception computer. We lost some files and documents unfortunately but this hacking also interfered massively with our membership system. We want to take part in this training to ensure this does not happen in the future. I am confident this training will equip us with the knowledge to identify any suspicious activity.”

⁷ The full qualitative interview questions are available in the Appendix 5. The ID of the approved ethical application is 2213.

In terms of training delivery staff expressed a preference for an interactive mode of delivery, which was accommodated with the use of an interactive flip-chart that utilised sticky post-it notes and colour pens as a part of group exercises. These approaches alongside the evidence collected from them will be discussed in detail in the 3 delivery section.

Training Delivery The following subsection contains information about how the training was delivered. It commences with three facilitation skills and then describes three interactive exercises.

1. Contracting This skill should be understood as derived from a psychotherapy contract [9]. This is separate from the research consent form which were the necessary requisites for the ethical delivery of this study. Rather, a psychotherapy contract, pertains to a collaboratively agreed set of expectations about how individual and group interactions shall be conducted to achieve maximum self-actualisation within a safe environment. For example, Hough [9, p. 281] states that: “*Establishment of a contract ensures that both client and counsellor understand the nature of the commitment between them, and that they work together in harmony.*” We contracted with the staff team when we presented them with a contract at the beginning of their session, which was captured on the flip-chart. We included the following items: 1. Non-judgemental (approach), 2. Honesty, 3. Time keeping (60 minutes), 4. Confidentiality within physical and research limits and left points open for inclusion based on staffs’ preferences.

2. Self-disclosure This skill should be understood as derived from psychotherapeutic practice, namely as a tool for building connection and increasing transparency [22]. It has been found that when a psychotherapist is able to become vulnerable by revealing something personal, perhaps embarrassing, it levels the playing field between them and the client in terms of power. As a result of this technique, which must be practised sincerely, the client will become more open and engaged. Self-disclosure is a useful addition to the existing research by Cross and Kelly [7], which focuses on simplifying cybersecurity training materials but neglects the importance of the human connection during the delivery of those materials.

3. Dialogic approach This skill relates to the general notion that the training was delivered as form of dialogue from start to finish, which enabled staff to step in during any moment of the process and make changes. The dialogic approach was most apparent in the group interactive exercises, which reflected Finney’s [8] applied and extended theory. What follows is a breakdown of the three group exercises alongside our reflective account. In order to mitigate any legibility problems from the original flip-chart photographs, we have transferred them into a vector graphic version.

Exercise 1: Identifying your assets This interactive exercise was derived from Finney’s [8] idea that a company’s assets ought to be divided in a way that prioritises the protection of the cardinal ones, which he also likened to the crown jewels. The aim of this exercise was to get staff to analyse which assets are “priceless” and which are “priced”, which would enable them to structure an effective defensive posture.

Staff tended to view “Members” (i.e., people) alongside more transcendental values such “Our community” and “Reputation” as priceless. Whilst viewing equipment related items such as “IT Equipment” and the like as priced.

Exercise 2: Understanding harm to your assets As before, we used an adapted version of Finney’s [8] theorising about assets in order to invite staff to think about how each could come to harm. Hence, we were aiming to gradually build up their strategic understanding of how to articulate their security posture. Whilst we will not regurgitate the entire discussion, we will note several sources of harm a community based Scottish SME can experience.

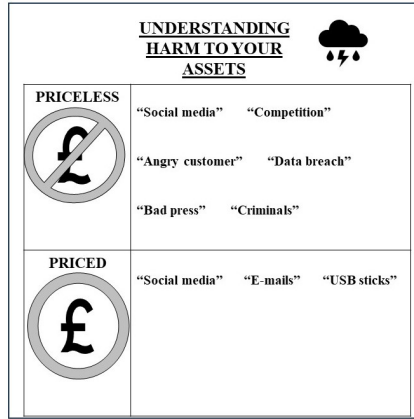


Fig. 1: Understanding harm to your assets

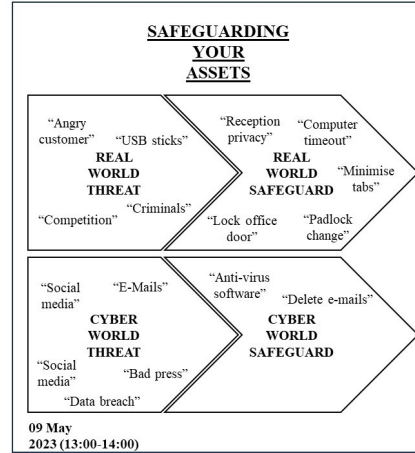


Fig. 2: Safeguarding your assets

As shown in Fig.1, in the priceless category, staff have identified “social media” and “angry customer” as sources of harm. This was related to their experiences of trolling, which required thoughtful crisis management. This placed the SME in a difficult position as it had to retain its social media in order to communicate with its clients, but also carefully resolve a trolling campaign. In regards to the staff’s experience of trolling, Barney [2] draws attention to the social complexity involved in the use of technology in firms. Barney [2] describes that even though multiple firms possess the same technology, it will be the social substrate of the company that will engage that technology to gain competitive advantage.

Exercise 3: Safeguarding your assets This exercise is a theoretical extension of Finney’s [8] cyber-resilience concepts. We required the SME’s staff to think about cyber-resilience as emerging from physical world security. Thus, they put together piles of items that constituted a “REAL WORLD THREAT” alongside items that were a “REAL WORLD SAFEGUARD.”

Then, they repeated the process for the cyber domain as is exemplified in Fig. 2. When we facilitated this exercise, the staff self-divided into small groups, which means that the safeguards do not directly reflect the threats either in numbers or in content.

Using interactive exercises as a learning tool has potential for this type of training. For example, an interactive exercise could be derived from Memory card game (also referred to as Concentration or Pexeso). In this game a large number of cards with different themes contain pairs which are the same from both sides. The top sides of the cards would be labelled with a “CYBER WORLD THREAT” and the bottom sides with a “CYBER WORLD SAFEGUARD” respectively. Then, people would have to turn them around to find matching pairs, which could also incentivise staff by introducing a competitive criterion. For example, a pair of cards with “Social media” on the one side could contain advice to the effect of “Think before you post: Will your post be interpreted by everyone in your intended way? How will your post age over time?”

Training Evaluation

Quantitative data The quantitative data were evaluated based on the criterion that only staff members who submitted both the pre-training questionnaire and the post-training questionnaire were included in the analysis as they were the only attendees where progress could be fully monitored. Thus, 9 participants filled in the pre-training questionnaire, but only 6 participants attended the training, whilst only 5 participants completed post-training questionnaire. This brought the overall dropout rate through the process close to 50%. Only the 5 participants that attended the entire process from development, to delivery to evaluation are a part of this study even though the views of those that dropped out have been considered.

Participant 1 In this case, the participant rated their knowledge of cyber-crime as 4 pre-training and desired to achieve an 8 post-training. Subsequently, they have rated their knowledge at a 6 post-training, which showed evidence of improvement. In terms of their affective response, their anxiety remained at a 2 before and after, whilst depression increased from 0 to 1 and confidence decreased from 4 to 3. They rated the lecturer as 50% supportive. They found group-work helpful, they experienced the training as interactive and easy to understand, they stated that nothing was unhelpful and listed noticing a hacker and a scam as relevant to their personal and professional life respectively.

Participant 2 In this case, the participant rated their knowledge of cyber-crime as 5 pre-training and desired to achieve an 8 post-training. Subsequently, they have rated their knowledge at a 6 post-training, which showed evidence of

improvement. In terms of their affective response, their anxiety increased from 2 to 3 from pre-training to post-training, whilst depression increased from 0 to 1 and confidence from 8 to 9. They rated the lecturer as 100% supportive. They found *“discussing areas that could put our business in danger”* helpful, they experienced the training as interactive and easy to understand, they stated that nothing was unhelpful and listed most and all of the training as helpful.

Here, it is evident that even though the participant experienced a small increase in negative affectivity, they also experienced an incremental increase in confidence.

Participant 3 In this case, the participant rated their knowledge of cyber-crime as 2 pre-training and desired to achieve a 6 post-training. Subsequently, they have rated their knowledge as 5 post-training, which showed improvement. In terms of their affective response, their anxiety increased from 4 to 5, depression remained a 0 and confidence increased from 1 to 5. They rated the lecturer as 80% supportive. In terms of what they found helpful, they stated that: *“I enjoyed how engaging the training was as this massively helped keep my focus and not get bored.”* This participant also offered additional insight into what could be improved by stating that:

“There were a few occasions where someone would ask a question and they would be told just wait I’m going to cover that later. I think it might have been more useful if the question was answered briefly and then by all means go more in depth later.”

In hindsight, this highlights the importance of letting people make their own uninterrupted discoveries along the way. Moreover, the participant was able to connect the training to their workplace practice evidencing a degree of improvement:

“Moving forward I will be sure to delete all emails which are suspicious or have links attached. In addition, I will be be mindful of data protection and asking members to confirm their personal details before providing information of their account”.

Here, it is evident that even though the participant experienced a small increase in negative affectivity, they also experienced a 4 point increase in confidence. Also, whilst their approach reflected a genuine effort to improve the cyber-resilience posture, deletion of e-mails would risk loss of evidence or loss of real e-mails if it turns out to be a false positive identification as a scam.

Participant 4 In this case, the participant rated their knowledge of cyber-crime as 5 pre-training and desired to achieve an 8 post-training. Subsequently, they have rated their knowledge as 5 post-training, which showed no improvement. In terms of their affective response, their anxiety decreased from 5 to 0, depression remained a 0 and confidence decreased from 4 to 0. They rated the lecturer as 100% supportive. They found *“discussing areas that could put*

our business in danger” helpful, they experienced the training as interactive and easy to understand, they stated that *“learning how we can protect ourselves going forward”* was helpful and that the *“the exercise with sticky notes”* was unhelpful although they did not specify which one as all the interactive exercises used sticky notes. They will change their work practices by *“making sure member information isn’t accessible to anyone else”* and will benefit from the training in their personal life by knowing *“how to prevent being scammed on social media.”*

Participant 5 In this case, the participant rated their knowledge of cybercrime as 2 pre-training and desired to achieve a 3 post-training. Subsequently, they have rated their knowledge as 2 post-training, which showed no improvement. In terms of their affective response, their anxiety remained an unchanged 0, depression remained a 0 and confidence increased from 0 to 10. They rated the lecturer as 100% supportive. In terms of what they were able to take away for their job role and personal life, they conjointly listed: *“Nothing new after the training.”* This comment alongside the 0 affective scores and rapid increase in confidence from 0 to 10 is indicative of a break-off pattern in responses [13]. According to Peytchev [13, p.95]: *“those who break off seem to put in effort, and larger or targeted efforts should be made to retain them.”* Given that the questions pertained to emotional insight, they could have also made the participant uncomfortable if they were preparing for a completely theoretical training delivery.

Qualitative data As a part of this research, participants 2 and 3 who represented accounting and managerial functions were also interviewed ⁸.

Participant 2 The answers of the participant complemented their scores from the post-training questionnaire. Specifically, they have stated that the course resulted in a small improvement in knowledge and awareness of how various assets ought to be safeguarded both in their private and professional life. This is reflective of the participants scores post-training which also marked a small improvement. The training has also helped the participant take an active role in improving the SMEs cyber-resilience posture by:

“Simple things like logging out of computers even if only going away for a short period, more mindful of data breaches and how they could occur in the organisation and also of not being tempted to click on links that could have serious issues for the organisation’s security.”

The training also attempted to help participants formulate a cybercrime resilience strategy by getting them to think about prioritising certain assets as “priceless” vs. “priced.” We have specifically probed whether the participant was able to glean any benefit from this exercise to which they responded that:

⁸ The training had taken place on 09 May 2023, the post-training questionnaires were filled out between 04-10 July 2023 and the qualitative interviews were carried out on the 30 August 2023.

“I didn’t particularly think of them in this way prior to the course although was aware of them as assets but it is useful to categorise them in this way and how to protect them.”

This response conveys the theme of awareness raising that we have already touched upon, the participant does not go into any detail with regards to what they might do with this categorisation in practice, but they simply note it.

The participant’s responses start to betray the effects of responsibilized thinking when they were asked about how they would report an attack either against themselves or against the company. On the one hand, they state that they would report the attack regardless of how it made them feel whether “*silly*” or otherwise. But when they were asked about how they would go about it, they stated that if the SME was attacked, then they would report to management and if they were attacked personally, then they would report to their bank. Hence, the participant did not mention the possibility of reporting to Police Scotland at all. Instead, when faced with the same situation in the future, they would conduct themselves in an unchanged way.

Participant 3 The answers of the participant complemented their scores from the post-training questionnaire. The participant has described their learning in terms of increased awareness, knowledge attainment as well as an improvement in confidence. With respect to confidence, as stated previously, their score increased from 1 to 5 based on the values listed in the pre- and post-training questionnaires respectively, which they retained until the time of the interview.

Just like their colleague, this participant has found the categorisation of assets into priced vs. priceless helpful and interesting. Importantly, they stated that it placed them in a better position to protect them: *“I didn’t think of our assets as two separate entities but with this new perspective, I am more aware of how to protect them.”*

Interestingly, the participant’s view of their own skills development has shifted since the time of the post-training questionnaire, where they explained a change in work practices. At the time of the interview, they provided mixed feedback by initially stating that:

“While I don’t believe this training has improved my skills, it has made me more mindful of the cybercrime that exists today and how often people fall victim to this crime.”

However, then they followed up with showcasing how they engaged in cyber-resilience leadership in their SME by taking up initiative:

“I would say I have been more cautious when it comes to data security and the protection of our passwords. For example, I find myself making a conscious effort to close down all tabs and membership accounts before I vacate the reception area, even if only for a short time. In addition, I have vocalised in staff meetings

the importance of confirming a member's personal details before proceeding with membership updates etc."

This is interesting because on the one hand, the participant is stating that the training has not improved their skills, but on the other they provide a highly specific example of how their work practices were altered in a positive way. It is difficult to assert a specific reason for this incongruence, but it could be the case that some of the learning integrated on a subconscious level and the participant was not aware that what they were doing was the result of their training.

With regards to reporting cybercrime, much like their colleague, the participant notes that they would have always reported cybercrime. That is, if their SME was attacked, they would report to management who would decide what to do next and if their private online banking was attacked they would report to the bank. Once again, there is no mention of Police Scotland. Instead, the responsibilized mindset prevails.

4 Discussion

SMEs which have had to fend for themselves in the cyber-resilience arena have adapted their instincts to this harsh reality as we have demonstrated via direct quotes in Section 3. This is why they associate reporting cybercrime with their own internal process but not with the police. Opening themselves up to formal policing and investigation techniques can seem alien and anxiety provoking. According to Batchelor and Gormley [3, p.53-58], this can also be due to a culture of self-reliance, of "*sorting things yourself*", which is connected to Scottish people's assimilation to experiences of repeat violence in the online and real world.

The current training approach is a good starting point for bridging the gap which is formed by a lack of trust between the responsibilized SMEs and the state.

As we illustrate via Fig. 3, the training's life cycle allows for a reflexive adjustment of the approach because each stage prepares the conditions for the following one. Stage 1. Training Development is focused on reducing negative emotions and increasing knowledge. Stage 2. Training Delivery concentrates on the required facilitation skills (i.e., contracting, self-disclosure and dialogic approach as well as the three key exercises (i.e., Identifying your assets, Understanding harm to your assets and Safeguarding your assets). The purpose of Stage 3. Training Evaluation is the use of Quantitative Surveys and Qualitative interviews to gather feedback for the training. Stage 4. Five guidelines is based on the authors' reflection of the process for the purposes of formulating recommendations for future trainers. These five guidelines feed back into Stage 1. Training Development. Here they serve the purpose of reducing negative emotions and increasing knowledge. Subsequently, the refined training lifecycle repeats itself based on participants' feedback and trainers' self reflection. This refinement can carry on endlessly to reflect the evolving cybersecurity threats.

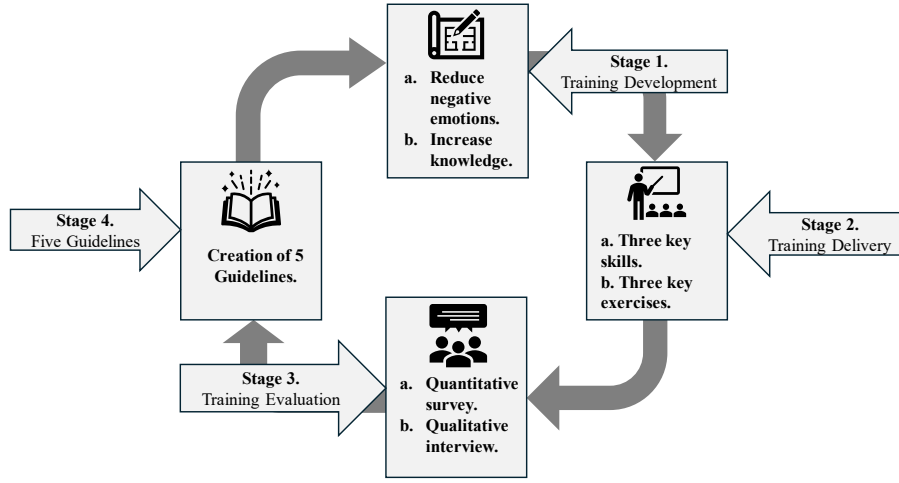


Fig. 3: Client-centred cybercrime training life cycle

Finally, we describe the already mentioned set of 5 guidelines that must be followed when training SMEs from socially deprived areas:

1. Reduce the amount of staff participation in the design of the training to save time. Saving time is important in a context, where participation in training design does not increase attendance in training.
2. Set time aside for finding an appropriate training time slot. It might take weeks and even months to agree with staff on a time that suits them for training delivery.
3. Practice contracting [9], self-disclosure [22,23] and a dialogic approach to effectively facilitate the training.
4. Use interactive exercises with the help of learning aids such as flip-charts, coloured pens and coloured post it notes.
5. Divide staff into groups to play educational competitive games [11]. It could be helpful to further incentivise the participants by offering a small prize at the end.

Limitations Whilst our sample was not representative of the Scottish population as a whole, it gives insight into the training needs of those working in areas that are economically struggling. Further research into the cybersecurity needs of SMEs in poorer areas is justified because they pay taxes to the state but are responsabilised by the same state post-attack.

5 Conclusion

Within, we have rejected an exposé approach that would showcase our knowledge against the naivete of a non-academic SME for the generation of cheap insights. Instead, this case study aimed to set a precedent for an empathetic interaction between scholars and experts vs. non-academic SMEs. Hence, we went beyond an analysis of the problem of poor victim aftercare. Rather, a victim private institution from Scottish victims of cybercrime was identified as a suitable candidate for a client-centred cybercrime training which was delivered post-attack. The first contribution of the training was in awareness raising whilst some shift in working practices and behaviours was evidenced. The second contribution of the training was that, to the best of our knowledge, it was the first of its kind to engage an SME from a disadvantaged region whereas other trainings omit this population.

Academia should collaborate more closely with the government in informing the education of all SMEs, compromised or not yet compromised because documents such as the SBSS 2022-23 underline that not enough attention is given to the cybersecurity costs associated with running SMEs.

Acknowledgments. This research was funded by the Scottish Institute for Policing Research (SIPR) with a grant number of `SIPR21MFS_003` and the University of Strathclyde in Glasgow.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

Appendix

A CCCT Pre-training questionnaire

Qualtrics, 24 March 2023

Age:

Gender:

Date:

Position:

Cybercrime client-centred pre-training questionnaire

1. How would you rate your current understanding of cybercrime on a scale of 1-10, where 1 is “no understanding” and 10 is “cybercrime expert.”
2. What kind of improvement are you hoping to achieve at the end of this training on a scale of 1-10, where 1 is “no understanding” and 10 is “cybercrime expert.”
3. What do you want to learn about that will be useful for your role in the company?
4. What do you want to learn about that will be useful for your personal life?
5. What made you choose this training?
6. Tell me about what kind of learning is most enjoyable to you.
7. Is there anything that you’re looking especially forward to about this training?
8. Is there anything that makes you apprehensive about this training?
9. Please rate how you feel about preventing cybercrime before completing this training where 0 is no emotion and 10 is extreme emotion.
10. Do you have a disability that may impact your learning? If so, what supports do you require to make your learning effective?

B CCCT Post-training questionnaire

Qualtrics, 24 March 2023

Age:

Gender:

Date:

Position:

Cybercrime client-centred post-training questionnaire

1. How would you rate your cybercrime knowledge after the training on a scale of 1-10, where 1 is “no understanding” and 10 is “cybercrime expert.”
2. Was the training material and content helpful for you? (Yes/ No)
3. What was a helpful aspect of the training?
4. What was an unhelpful aspect of the training?
5. Was the training programme interactive and engaging? (Yes/ No)
6. What part of the training will you apply into your job role?
7. What part of the training will you apply into your personal life?
8. Was the training easy to understand?
9. Please rate the supportiveness of the course leader during your learning, where 0 is “completely unsupportive” and 10 is “extremely supportive.”
10. Please rate how you feel about preventing cybercrime after completing this training where 0 is no emotion and 10 is extreme emotion.

References

1. Bada, M., Furnell, S., Nurse, J.R.C., Dymydiuk, J.: Supporting small and medium-sized enterprises in using privacy enhancing technologies. In: *HCI for Cybersecurity, Privacy and Trust*. pp. 274–289. Springer (2023).
https://doi.org/10.1007/978-3-031-35822-7_19
2. Barney, J.: Firm resources and sustained competitive advantage. *Journal of Management* **17**(1), 99–120 (1991).
<https://doi.org/10.1177/014920639101700108>
3. Batchelor, S.A., Gormley, C.: Repeat Violence in Scotland: A Qualitative Approach. Scottish Centre for Crime and Justice Research University of Glasgow (2023)
4. Braun, V., Clarke, V.: Conceptual and design thinking for thematic analysis. *Qualitative Psychology* **9**(1), 3–26 (2022).
<https://doi.org/10.1037/qap0000196>
5. Bunge, E., Williamson, R., Cano, M., Leykin, Y., Muñoz, R.: Mood management effects of brief unsupported internet interventions. *Internet Interventions* **5**, 36–43 (2016). <https://doi.org/10.1016/j.invent.2016.06.001>
6. Chetty, S.: The case study method for research in small-and medium-sized firms. *International Small Business Journal* **15**(1), 73–85 (1996).
<https://doi.org/10.1177/026624269615100>
7. Cross, C., Kelly, M.: The problem of “white noise”: Examining current prevention approaches to online fraud. *Journal of Financial Crime* **23**(4), 806–818 (2016). <https://doi.org/DOI10.1108/JFC-12-2015-0069>
8. Finney, G.: Well Aware - Master the nine cybersecurity habits to protect your future. Greenleaf Book Group, 1st. edn. (2020),
<https://wellawaresecurity.com/>
9. Hough, M.: *Counselling Skills & Theory*. Hodder Arnold, 2nd. edn. (2006)
10. Huang, R.T.: Overcoming invisible obstacles in organizational learning: The moderating effect of employee resistance to change. *Journal of Organizational Change Management* **28**, 356–368 (2015).
<https://doi.org/10.1108/JOCM-07-2014-0130>
11. Kayali, F., Schwarz, V., Purgathofer, P., Götzenbrucker, G.: Using game design to teach informatics and society topics in secondary schools. *Multimodal Technologies and Interaction* **2**(4), 77 (2018).
<https://doi.org/10.3390/mti2040077>
12. Payne, B., He, W., Wang, C., Wittkower, D., Wu, H.: Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course. *Journal of Information Systems Education* **32**(2), 134+ (2021)
13. Peytchev, A.: Survey Breakoff. *Public Opinion Quarterly* **73**(1), 74–97 (2009).
<https://doi.org/10.1093/poq/nfp014>
14. Pike, R., Brown, B., West, T., Zentner, A.: Digital Badges and E-Portfolios in Cybersecurity Education. *Information Systems Education Journal* **18**(5), 16–24 (2020)
15. Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., Orgeron, C.: Is the responsabilization of the cyber security risk reasonable and judicious? *Computers & Security* **78**, 198–211 (2018). <https://doi.org/10.1016/j.cose.2018.06.006>
16. Schatz, D., Bashroush, R., Wall, J.: Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law* **12**(2), 8 (2017).
<https://doi.org/10.15394/jdfsl.2017.1476>

17. Scottish Government: Scottish index of multiple deprivation 2020 (2020), <https://www.gov.scot/news/scottish-index-of-multiple-deprivation-2020/>
18. Sikra, J.: Delivering an interactive university curriculum during Russia's invasion of Ukraine. In: VII International Scientific Conference Military Psychology in the Dimensions of War and Peace. pp. 13–16. Taras Shevchenko Kyiv National University (2022)
19. Sikra, J.: Evaluating a university curriculum delivered during Russia's invasion of Ukraine. *The Bulletin of Taras Shevchenko University of Kyiv Social Work* **8**(1), 78–80 (2023)
20. Smith, S.C.: Toward a scientific definition of cyber resilience. *Proceedings of the 18th International Conference on Cyber Warfare and Security* **18**(1) (2023)
21. Thatcher, J.B., Perrewé, P.L.: An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy. *MIS Quarterly* **26**(4), 381–396 (2002). <https://doi.org/10.2307/4132314>
22. Yalom, I.D.: *Staring at the sun - Overcoming the dread of death*. Clays Ltd, St Ives plc, 2008 and 2011 edn. (2011)
23. Yalom, I.D., Leszcz, M.: *The theory and practice of group psychotherapy*. Basic Books, 5th. edn. (2005)