Client-Centred Cybercrime Training - A Scottish Case Study

Sikra, Juraj
University of Strathclyde
juraj.sikra@strath.ac.uk

Renaud, Karen V.
University of Strathclyde
karen.renaud@strath.ac.uk

Thomas, Daniel R.
University of Strathclyde
d.thomas@strath.ac.uk

ABSTRACT

Background: The UK neoliberal government responsibilizes Small-to-Medium enterprises (SMEs) to take care of their own cyber-resilience, meaning that they do not receive any support if they fall victim to a cyber attack. Consequently, SMEs tend not to report cybercrimes.

Aim: The aim of this case study was to collaboratively develop, deliver, and evaluate a client-centred cybercrime training session with an accompanying booklet as means of achieving closure post-attack, upskilling an SME, increasing their knowledge and improving reporting.

Methods: We surveyed 9 staff of an attacked SME to elicit their training preferences; 6 staff members attended and 5 supplied feedback in the form of a post-training survey. From those who completed the survey, 2 staff members were interviewed. The results showed that the training helped some staff members take cyber-resilience into consideration because they provided evidence of their learning either via the post-training survey or via the interviews.

Results: The training served to improve staff's cyber-resilience awareness and skill-set to a limited degree. It became clear that the government's responsibilization agenda deterred staff from reporting cybercrimes to Police Scotland.

Conclusions: Building on our case study, future work should engage with victimised SMEs and foster a trusting relationship. Academia can play a part in upskilling government-appointed cyber-resilience trainers.

***K*eywords** Cybercrime, Responsibilization, Reporting, Training, Small-to-medium enterprise (SME)

1 Introduction

Capitalising on the findings by Bada *et al.* [1] we have taken the case study approach [11] to develop a bespoke cybercrime training for a Scottish SME that was attacked by ransomware. Even though Bada *et al.* [1] were mainly concerned with delivering training on Privacy Enhancing Technologies (PETs) we view their research angle as closely overlapping with cyber-resilience and cybercrime. According to Smith [44, p.32]: "Cyber-resilience is the ability of

a cyber system to recover from stress that causes a reduction in performance." Bada *et al.* [1, p. 278] critique that cyber-resilience frameworks are often aimed at technically minded people. However, the authors themselves then recruited SME participants from IT, science, technical activities and public administration. In other words, they have fallen into the limitation that they themselves highlighted. We, to the contrary, engaged with an SME from a deprived area in Scotland which employed staff with minimal cyber-resilience understanding, thereby addressing a research gap. Our approach reflects the assumptions of Chetty [11, 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 are not clear cut and multiple sources of evidence are used.

The SME operates in the West of Scotland, which is an area that contains some of the nation's most deprived regions [40]. For that reason, SMEs are a vital source of employment and community life. This SME has been operating in the services sector for several decades. Thus, it is also an important community hub and a place for people to socialise. A cyberattack on this type of business extends to the community too.

This research will mainly benefit professionals and practitioners that are interested in enhancing the cyber-resilience posture of SMEs that operate in a hands-on non-academic environment. The approaches within ought to be transferable across different industries (e.g., hospitality, entertainment, or health and beauty). On the other hand, familiarising oneself with the pitfalls that we encountered with training an over-stretched team can also be helpful.

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 responsibilization by omission. Responsibilization in cybersecurity occurs when the state transfers responsibility for cybersecurity onto the SMEs [37]. 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 responsibilizing omissions to support struggling SMEs.

The paper is structured in the following way: Section 2 reviews the related research and motivates an investigation into upskilling a Scottish SME. In Section 3, we guide the reader through our main research questions RQ1 and RQ2 and the methodology that was used to design a study that addressed them. In Section 4, we describe the results of the study which contain the development (§4.1), delivery (§4.2), and evaluation (§4.3) of the training materials with the use of participants' responses. Section 5 answers RQ1 'Will a collaborative and client-centred approach to cybercrime training improve staff's cyber-resilience posture?' (§5.1) and RQ2 'Will a collaborative and client-centred approach to cybercrime training improve reporting?' (§5.2). Finally, Section 7 concludes.

2 Related Research

This section details cyber-resilience and cyber-security training, which was uncovered via a scoping literature review. Cyber-security is related securing a system from an attack [39, p.66] whereas cyber-resilience is related to the system's ability to recover from an attack [44, p.32]. In this context, training teaches people how to prevent stressors to the cyber system or reduce their effects post-onset. In our case, the stressors are cyber-attacks and cybercrime and the cyber system are the software and hardware components of an SME.

The pieces within this review were used to inform our approach but also to highlight the research gap with regards to training industry professionals that lack an academic background. Most of this section is focused on training delivered via mainstream education which was chosen as a benchmark for cyber-resilience skills since most people are legally obliged to have some amount of formal schooling. We also went beyond the mainstream education system to scope research that could inform our approach from new angles (e.g., considering people with disabilities). Research that was particular to SMEs was not reviewed because the focus was not on SMEs per se, but on the non-academic staff that populate them and how to best develop their cyber-resilience skills post-attack. We acknowledge that there is current SME research that is connected to cybercrime [26, 49], but it is unconnected to upskilling its non-academic staff post-attack.

The results of this search are presented both thematically and chronologically. From a thematic perspective they are organised into six subheadings. The first three subheadings are based on the educational level: Secondary (§2.1), Higher (§2.2), and Industry (§2.3). The second three are standalone: Non-Traditional Learning (§2.4), People with a Disability (§2.5), and A Practical Framework (§2.6).

We have selected these pieces of literature as illustrations of how cyber-resilience education is delivered via a person's life-cycle, but also to highlighted varied modes of delivery that could be tied into our current approach even though they do not fit neatly within the life-cycle narrative.

The contribution of this literature review for the client-centred cybercrime training is that it contextualises our empirical investigation within cyber-resilience training. In this study we shift from speaking about cyber-resilience training to client-centred cybercrime training, because the attendees of our training were all motivated by having their organisations violated by cybercrime, which required a more niche approach.

Usually cyber-resilience training is sophisticated [15], which means that is is focused on people with ample pre-existing technical knowledge. This further underscores the need for our research as it is geared specifically for practical and non-technological people as it utilises simple and engaging exercises delivered within an hour.

2.1 Secondary School

Research looked at how to teach cyber-resilience subjects in secondary schools via game design [27]. The researchers were interested in examining the effectiveness of games in teaching the pupils a range of IT skills. Overall, they found

that games did not enable the students to learn about the subjects in a way that was more effective than theoretical classroom learning. Instead, games were useful in terms of raising the students' awareness of the topics under debate. With regards to cyber-resilience in particular, the authors found that games with a multiple-choice component were effective. We have taken this into consideration when designing the organisation's own client-centred cybercrime training by making the activities as engaging as possible.

Appreciating the role of teachers in the education process of cyber-resilience from the middle and high school contexts, Ivy *et al.* [23] examined a program that prepared teachers in this domain. The program concentrated on inquiry-based learning, focused classroom disclosure, and collaborative learning. The outcomes of this study showed that teachers were able to apply the principles referred to within to their roles, which improved their abilities to deliver improved cyber-resilience education to their students. In our view, even though this study was focused on middle and high school teachers, the material that was covered was too specialist for people without prior interest in this domain. We felt that if we used language such as "resource encapsulation", "domain separation" and the like, then this alone could have triggered a mental block in people whose primary interests laid in running an extremely busy SME.

Bolun *et al.* [6] argued that cyber-resilience should be cultivated at school and throughout the educational journey. Moreover, people should be instructed to see themselves as a part of a whole class, working group or team. Hence, social components are gradually starting to creep into a domain formerly populated exclusively by technological language. As we go on to demonstrate in the Results: CCCT for Private institution Victims (§4), socially interactive exercises played a crucial role in the delivery of our client-centred cybercrime training, which was positively highlighted by the participants.

2.2 Higher Education

The lack of cyber-resilience skills is widely recognised by universities and has prompted some changes to existing curricula to cater to this need. In the research by Harris and Patten [17] the authors tackled the inclusion of cyber-resilience topics into the curriculum whilst not increasing the overall credit requirements. Harris and Paten [17] solved this problem by prioritising cyber-resilience skills over other security skills, which they have moved into the lower levels. The authors note that if this type of training is included, then it should reduce the workload elsewhere otherwise people become overwhelmed. We have done our best to account for this during training delivery by being as flexible as possible and allowing the company as much time as required to schedule a time that was most suitable.

In research by Tagarev [45] the author examined the creation of a reference curriculum by NATO that could be used as a starting point for universities and training organisations in the field of cyber-security. The curriculum has four themes. The first theme serves as an introduction into cyber-security. The second theme examines risk vectors. The third theme is aimed at good practices derived from international institutions and organisations. The fourth theme is concerned with ground management of cyber-security in the national context. Taken together, the reference curriculum is a useful benchmarking tool for countries interested in cyber-security education. Nevertheless, the underlying assumption for

this type of research is that the education is for people who will oversee national cyber-security structures, but that task is too expansive for most organisations. Once again, we are seeing the need for a client-centred cybercrime training specifically aimed at local SMEs.

Vain and Kcharchenko [48] related their findings from the Tempus Serien project, which aims to modernise university studies for MSc and PhD students in the areas of engineering and management. The MSc students will receive a review in challenges in dependability, cryptography, and risk analysis of security resilience among others. The PhD students will be taught systems security and resilience management as well as cloud management among others. Much like the research by Tagarev [45], the latter offers highly advanced skills that are unrelatable for people overseeing the running of a legacy SME.

Research has also examined the development of the cyber-resilience curriculum for undergraduate business schools [54]. They developed a descriptive cyber-resilience curriculum, which commenced with an introduction to information systems and continued with app development, IT infrastructure, data and information management, systems analysis and design, information systems strategy and management and acquisition policy. Yang [54] also put forward elective courses that can be considered by institutions, which included technical electives such as digital forensics and organizational electives such as legal and ethical subjects. Yet a reader would struggle to find an example of how people with these skills could be paid for by SMEs on a tight budget, which underlines the need for our approach.

As most cyber-security university courses tend to aim at people seeking graduate employment as cyber-security specialists, Cabaj *et al.* [10] analysed the content of curricula in this domain. After examining courses across different universities, they found components such as an emphasis on cryptography, data protection, operating systems security, malicious code, vulnerability analysis and system security evaluation. Furthermore, topics such as defensive programming, secure software engineering, reverse engineering and malware were represented across some masters' programs. Taken together, the evidence suggests that universities across the globe devote significant resources to cyber-security education however most of it seems to be highly specialised for people wishing to work in the area.

Based on the findings of Marquardson and Gomillon [31] hands-on practical exercises are best suited for developing cyber-resilience skills in graduates. Yet, the very exercises that enable effective learning to take place carry most risk to harm the systems on which those skills are practised. According to Marquardson and Gomillon [31] the educational institution can take steps to manage these risks effectively. This can be done by putting 'preventive controls' in place such as adequate student training before the commencement of exercises. Also 'detective controls' should be in place, which will enable the course supervisor to detect risky activity. Next, 'corrective controls' can help mitigate the effects of an exploited vulnerability such as using effective back-ups. Subsequently, 'deterrent controls' can be used to sanction the students for not following secure behaviours such as expulsion from the course. These types of exercises are important in teaching students how to safeguard organisations, which can be adapted in principle to those working for Small-to-medium enterprises (SMEs).

Researchers have also noted problems with the heterogeneity of courses in cyber-resilience. Specifically, Liu and Tu [30] noted that the differences between various university programs make it difficult to draw effective comparisons. This prompted them to program a database system, which allows for the quick categorisation and comparison of various cyber-resilience qualifications. Scotland faces a similar problem in terms of the cyber-resilience qualifications lacking a unifying framework, hence the implementation of such a framework into a program could support the resolution of this issue. Moreover, Scotland could take things a lot further and become a pioneer in designing training for SMEs, which are most vulnerable to cyberattacks. On the other hand, there is promising UK initiative referred to as The Cyber Security Body of Knowledge [36] (CyBOK for short), which aims to bring together and "underpin education and professional training for the cyber security sector."

In the next research piece, Pike *et al.* [34] explored a student-lead approach to the cyber-resilience curriculum from middle-school to university. The scientists focused on designing a curriculum that would enable students to organise their studies from complete beginners to entry level professionals. The advantage of their approach is that students played a leading role in identifying their own needs and hence structuring their education through digital badging. Since this study was a pilot, data were not available as to how students structured their learning, but it is assumed that this flexibility would improve both their experience and educational attainment. We have engaged with the principles of this research in collaboratively designing our client-centred cybercrime training, which may have correlated with higher engagement from our participants.

A study which analysed the learning needs of both teachers and students in higher education examined the vulnerabilities of these institutions [4]. It found that personally identifiable information was most valuable to the victims and the criminals. This was followed by student grades, and administration data. The most regular attacks were in the areas of intrusion and malware. The sources of these attacks were organised criminals, state espionage, and mistakes by other people. This information is useful in designing a client-centred cybercrime training because it mirrors the modus operandi behind the ransomware attack on the client.

In Dragoni *et al.* [13], the researchers highlighted that software design was extremely important in this respect, the appreciation and evaluation of threats, automated security analysis, and the testing and assessment of newly developed and externally acquired software components. This is an important piece of research that could improve the knowledge of graduates aiming for employment in the SMEs sector tasked with insuring that the cyber-resilience architecture of the company is fit for purpose.

Khader *et al.* [28] focused on understanding university students' attitudes and behaviours after supplying them with cyber-security subjects into the curriculum. These researchers put forward their own Cybersecurity Awareness Framework, which aims to guide the application of solutions to improve the cyber-security awareness of graduates at the university. This is a versatile framework that can be easily adjusted to the various needs of the implementing university. We have used this approach to inform our flexible use of educational methods, which we have made significantly as accessible as possible to the practice-oriented lay person working in an SME.

Next, Payne *et al.* [32] designed and delivered an interdisciplinary course on cyber-security based on the rationale that cyberspace is not populated by IT professionals alone. Rather it reflects all the diversity that is reflective of the inhabited world. Payne *et al.* [32] have argued that other professionals that seek to integrate similar courses into their curricula should follow their five recommendations. Firstly, developers should draw on real world examples when developing course materials, which are not contained within disciplinary boundaries. Secondly, the developers should practice what they preach in that the curriculum should be developed by professionals across the disciplines and should not be headed by an individual or a group from the same discipline. Thirdly, developers should think small as opposed to think big. This is because cyber-security is a developing and evolving discipline. Materials that are too comprehensive run the risk of becoming outdated very fast, shorter materials on the other hand, can be easily continuously updated. Fourthly, developers should be pro-active in encouraging the university to integrate cyber-security education across the board. Fifthly, Payne *et al.* [32] encourage interested readers to freely use their own downloadable materials from Cybersecurity, Technology and Society. Specifically, Module 4: Business and Cyber Security is extremely useful for students entering the job market, which has units focused on leadership, fundamentals in cyber-security as well as other items relevant for SMEs.

Bearing in mind the challenges brought on by COVID-19 research focused on ways to deliver cyber-resilience curricula online in a way that continued to bring value to university students [46]. The researchers delivered on this aim by creating the CLARK (Cybersecurity Labs And Resource Knowledge base). The main purpose of CLARK is to supply a model for building the curriculum, the digital library system and the curriculum collections. Educators have used the CLARK model to build their curricula, which has aided the process of delivery during COVID-19 pandemic. More information on the CLARK project alongside its practical utilisation can be found at the Clark Center. This project offers a wealth of free information for different educational groups, but none that would be especially accessible for SMEs.

Returning to the subject of evaluating curricula previous research has sought to illuminate the best way to achieve this for cyber-resilience courses at business schools [53]. Yang [53] examined ten cyber-resilience frameworks and 380 topics and associated areas. Much like the previous research cited within, it was found that most cyber-resilience curricula favour technical topics over business related ones. Hence, they neglect the social side of developing cyber-resilience and justify the need for our research in the domain of SMEs.

2.3 Industry

Educational institutions struggle to integrate cyber-resilience curriculum into their syllabus, which results in unprepared job seekers entering the workforce thereby compromising their employers' systems. Take for instance the study by Pusey and Sandera [35], which examined teachers' preparedness to teach cyber-resilience subjects to their pupils. It was found that their own skills are inadequate in this area and hence they struggle to impart the knowledge onto their pupils. This points to a systemic problem as it proves that teachers are ill-prepared to teach cyber-security due to their

own gaps in knowledge. Consequently, educational systems will fail to prepare the workforce for being cyber-resilient in SMEs making the latter susceptible to cyber-attacks.

In contrast to the theoretical approach set out above, Knapp *et al.* [29] argue for greater links between academia and the industry that offer cyber-resilience qualifications. In their study they have noted that a substantial amount of people working with cyber-resilience have acquired qualifications via the industry rather than academia and hence they put forward a model, which derives the cyber-resilience curriculum from the industry qualifications. They have also argued that experiential learning and end of term academic projects should play a more prominent role in teaching cyber-resilience. This reflects the views contained within this research as well as its overarching aim to use academia as a part of the solution in the area of client-centred cybercrime training.

According to previous research even the high end specialised cyber-resilience curricula are struggling to keep up with the industry's requirements [25]. To identify the knowledge, skills and attributes for performing in this domain, the researchers conducted 44 interviews with cyber-resilience professionals. Based on the acquired data the researchers found that the participants acquired most of their skills in the industry rather than via the formal educational route. Critically, participants viewed topics such as networks, programming vulnerabilities and interpersonal communication as needing to be prioritised in the cyber-resilience curriculum. As a part of our research and client-centred cybercrime training we have placed a high emphasis on communicating with the participants in as accessible and non-judgemental way as possible.

The next research ties closely into the previously discussed topic. Johnson [24] found that graduates from cyber-resilience courses have acquired theoretical knowledge on the subject but struggled to apply this to their workplace. Hence, she designed a module which would allow students to engage with work placements in the industry. According to preliminary analysis this increased students' preparedness to enter the job market and resolved some of the graduate employers complaints about unprepared graduates. This programme also faced a challenge whereby the internship providers felt challenged by the amount of hand holding that the interns expected them to do. However, it is considered that work placements during a person's degree are good place for students to build their confidence in a place of safety and nurture. We are including this research as it ties closely with the overall research ethos, which is to develop research in close correspondence with industry's needs in Scotland. This research in particular showcases the ability to do outreach work in Scottish communities which are usually forgotten by cyber-resilience specialists.

In considering the context of new employees entering the workplace, Blazic [5] identified several areas that are not currently covered in cyber-resilience curricula, but are expected by employers, nevertheless. The areas required by employers are an insight into computer architecture, data, cryptography, networking, secure-coding principles, operating-systems internals, Linux-based systems, low level programming skills. However, it was also argued that people will be better suited for jobs in cyber-resilience if they are from a multidisciplinary background emphasising the need to recruit people with enhanced social skills. Whilst this work highlights the need for social skills in cyber-resilience professionals, it feels that its recommendation is pro-forma due to their low specificity. Yet, we adapted them when

using social skills when engaging with practice-based professionals in a Scottish SME that lacked a cybersecurity background.

Zhang *et al.* [55] acknowledged that employees entering into the industry are not adequately prepared in terms of cyber-resilience awareness, which is a source of vulnerability for their employer. Nevertheless, most cyber-resilience awareness training cannot meet this demand due to a misaligned focus. To meet this need Zhang *et al.* [55] have developed a framework that will help organisations develop their training. The framework works on a cost and benefit principle. The costs are specified into three categories: constant, complementary and compensatory. The benefits are specified into four categories: negligible, consistent, increasing and diminishing. The authors argued that this framework will aid companies designing cyber-resilience awareness training that will resolve vulnerabilities whilst they are still at the lower end. From the perspective of client-centred cybercrime training, these types of frameworks are mainly good because they read well on paper. In practice, employees are too overburdened to engage even with simple dichotomies never mind matrices. We will discuss this in more depth as we go on because we too have put forward a dichotomous framework believing that it will improve people's learning. However, the feedback suggested that participants viewed this only as a mental exercise.

Blazic [5] considered the European cyber-resilience curriculum and the extent to which it corresponds to industry's needs. In her analysis she identified five pillars of cyber-resilience education, which are: Device-centric security, Network-centric security, Software/System-centric security, Data/Application-centric security and User-centric security. Much like the previous research Blazic [5] suggests that organisational and human-centred aspects of cyber-resilience are neglected in curricula, which are components concretely addressed within.

2.4 Non-Traditional Learning

In a study that concentrated on the techniques of teaching cyber-resilience strategies, Hamman *et al.* [16] investigated the contribution of game theory to teaching cyber-resilience. Using an empirical set-up, the scientists managed to prove that a two-hour training course on strategic thinking improves the reasoning of students about cyber-resilience and helps them anticipate the steps taken by the hackers. Whilst this course does seem to be for the more sophisticated pupils, the principles of game theory could be used to help in educating people reflect on suspicious content such as phishing links. We have done this in the current research using more rudimentary principles and approaches from impactful popular literature.

There have also been suggestions in previous research that innovative out-of-class learning experiences are conducive to acquiring cyber-resilience skills [21]. Here the authors observed the limited effectiveness of classroom teaching methods and used empirical methodology to evaluate students' learning in an out of class environment, which entailed experiences such as an internship with the FBI. They found that out-of-class learning did not only improve cyber-resilience skills, but also made the learning process more appealing to the student. Therefore, the future cyber-resilience curriculum would benefit from integrating components that enable students to solve real world problems in a real-world

context to improve their learning. The real-world context played an important role in this research too as the participants were keen to learn more about the modus operandi of attacks to make sense of their own experience, which was reflected in the learning materials.

In an article focusing on an evaluation of 'Capture the Flag Challenge (CTFC)', Svabensky *et al.* [56] examined the gaps in curricula that the cyber-resilience competitions address as well as those, which they neglect. They found that CTFC addresses skills in relation to technical knowledge such as cryptography and network security. However, it neglects a skills gap in connection to the human components such as social engineering and cyber-resilience awareness. This research lends further support for the current approach where we seek to fill this gap and help our participants understand cybercrime from the perspective of the criminal whilst capitalising on their social skills and critical thinking as important assets.

In addition, Workman *et al.* [50] explored the contribution of educational activities to cyber-resilience behaviours. Their study assumed that whilst traditional modes of classroom learning do not amplify cyber-resilience behaviours, gamified modes of learning do. They have sought to prove this empirically. Based on their results, it was demonstrated that simulations of real-world situations improve cyber-resilience behaviours vs. classroom taught materials. Nevertheless, the most improved performance was evidenced in the cohort, which received structured cyber-resilience simulations combined with live competitive tasks. The interactive nature of the client-centred cybercrime training complies with these findings and ultimately produces modest results.

2.5 People with a Disability

When considering the cyber-resilience curriculum, it is crucial to consider research that pertains to individuals living with a disability [22]. Based on the findings from this research, visually impaired people with more cyber-security knowledge were less likely to use the internet than those with less cyber-security knowledge. This is a good example for the principle that teaching someone cyber-resilience is not enough unless that person is given the tools to apply those principles safely. Hence, the visually impaired participants were dis-empowered from using the Internet by the very same knowledge that would encourage safe use among the visually healthy population. We were guided by this research when we designed the client-centred cybercrime training because we specifically probed the presence of any disabilities that would impede participation and offered extra assistance to anyone who required it.

2.6 A Practical Framework

In making use of what is already out there, Schaeffer *et al.* [38] applied their understanding of the National Institute of Standards and Technology (NIST) to the subject of cyber-resilience education and related their framework as a way of conceptualising the cyber-resilience curriculum. They suggested that students are developed in the areas of: 1) secure provision, 2) operation and maintenance, 3) protection and defence, 4) investigation, 5) collection and operation, 6) analysis and 7) oversight and development. Whilst the NIST is a highly respected cybersecurity framework, Schaeffer *et al.* [38] did little in terms of explaining to the reader how they would apply the seven areas to the cyber resilience

curriculum. Hence, additional effort is required from the reader in terms of accessing the NIST website and applying the material within onto the subject under review. In this research we aim to avoid this type of complexity by co-designing the client-centred cybercrime training in close collaboration with the attacked company to ensure a close alignment with their needs. In our approach, we sampled staff's learning needs by directly asking them what they wanted to learn about, but that was not enough. In addition, we included material in our training that was not reflected in their preferences, but we felt that it was critical for effective asset safeguarding.

Since, the literature review preceding this study revealed only a limited number of pieces for the purposes of upskilling the staff of an attacked SME, a more individualised approach was required. Therefore, we sought to answer the following research questions:

Research Question 1 (RQ1): Will a collaborative and client-centred approach to cybercrime training improve staff's cyber-resilience posture?

Research Question 2 (RQ2): Will a collaborative and client-centred approach to cybercrime training improve reporting?

3 Methods

We used *Well Aware* by Finney [14] as our starting point and it is Finney's [14] theorising about cybercrime education that underlies much of our freely available training materials [43].

This section will commence with the Design of this study. Here, two components are discussed: the Quantitative section and the Qualitative section. The first is concerned with how the pre-training and post-training questionnaires were developed whilst the second pertains to the development of qualitative interviews. Subsequently, information on Participants will be supplied. We will then briefly touch upon the ethics of these studies and finally explain our rationale for analysis. In essence, we wanted to find out people's preferences for the cybercrime training and evaluate its effectiveness against those preferences post-hoc.

3.1 Design

3.1.1 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 Huang [20]. Next, expertise of designing [41] and evaluating [42] 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 naive employees of an attacked SME.

Nevertheless, we did not neglect the empirical component and as can be seen in Appendix D our approach was designed to diligently map out increase in self-rated knowledge over time, but also changes in emotionality in response to new and potentially slightly unsettling material. Lastly, we included the rating of lecturer's supportiveness as an added factor that could be used to make inferences from scores. For example, Participant one in Table 2 in Appendix D gave a low lecturer rating of just 50% and subsequently displayed a dip in confidence and increase in depression, which opens the avenue to explore connections between lecturer supportiveness, learning and affectivity, particularly in cases with larger groups and more engaged members of staff.

Also, research that focused on designing a student-led curriculum to cyber-resilience was utilised [34]. 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. Additional findings were also accessed when envisaging the current training, mainly our emphasis on the use of real-world examples will form an important part of how the material is illustrated [32].

Following on from that, we also made important insights for the questionnaire design by highlighting the influence of computer anxiety as a mediating factor over IT performance [47]. Hence, we integrated three Likert scales measuring depression, anxiety and confidence with respect to preventing cybercrime in the pre-training and post-training questionnaires.

3.1.2 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 three weeks or more. 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. This was supplied in advance to make them more comfortable but in addition there was no added value to spontaneity. In fact, it was useful evidence if participants made some sort of notes prior to the interview to prime their memory accurately. The entire training approach was based around people being able to ask questions, so there was an opportunity to answer those. We advised that we would remain available for follow-up questions about cybersecuring circumstances allowing.

3.2 Participants

3.3 Ethics

This study required two ethics applications, which were approved by the departmental ethics committee.

3.3.1 Quantitative Section - Survey

This part of the study employed an online pre-training and post-training questionnaire which contained the necessary ethical forms. Before the participant could progress from the consent forms, they had to indicate that they have read the piece of documentation. If they did not indicate that they read the documentation, then they could not progress. The ID of the approved application is 2161.

3.3.2 Qualitative Section - Interview

This section employed a semi-structured interview which contained the necessary ethical forms. 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 questions. The ID of the approved application is 2213.

3.4 Analysis

3.4.1 Survey

The data were analysed with Qualtrics by comparing pre-training (Appendix A) and post-training questionnaires (Appendix B), which is rooted Bunge *et al.*'s [9] methods, 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 for visual rather than statistical purposes as depicted in the summary Tables 1 and 2 in Appendix D.

3.4.2 Interview

The data were analysed in accordance with Braun and Clarke's [8, 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 [8] theorising, our themes are best understood as summaries of particular topics, mainly in connection to the training effectiveness and improved cybercrime reporting. In identifying our TA approach, we have also followed the best practices guidelines by Braun and Clarke [7, p.335] who urged all researchers to "clearly demarcate which TA approach they are using."

4 Results: CCCT for Private institution Victims

4.1 Development of Training Materials

As already mentioned, the SME resides in an area with a higher level of deprivation. This meant that staff's level of cybercrime awareness was likely to be even lower than in an SME from an affluent suburban region. Therefore, we sought to ensure a particularly supportive approach, which was informed by psychotherapeutic theory. One might ask:

"Why engage with psychotherapeutic theory outside of a clinical setting?" This is based on life experiences within communities faced with deprivation. In our experience, there is a much greater chance of anxiety and suspicion towards people coming from an academic background.

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. The chances of increased negative emotions resulted in the need to assess their emotional states (i.e., anxiety, depression and confidence), which were rated using a Likert scale as captured in the pre-training questionnaire.

The latter ties into the post-training questionnaires which are contrasted against each other as an indicator of progress more broadly discussed in the evaluation (§4.3). 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*."

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 delivery section, which also showcases photographic evidence in the forms of Figure 1, Figure 2 and Figure 3.

In summary, the literature review was of limited use for developing a training for an attacked Scottish SME that resides in an area of higher deprivation. Hence, additional resources were utilised alongside various sampling techniques to design a bespoke training booklet as well as customised pedagogical approaches.

4.2 Delivery of Training Materials

Contracting: This term should be understood as derived from a counselling and psychotherapy contract [19]. This is separate from either the research consent forms which were the necessary requisites for the ethical delivery of this study. Rather, psychotherapy contracts, in this sense of the word, pertain 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 [19, 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 draft 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 5.-10. open for inclusion based on staffs' preferences. We explained to them that in order to learn effectively everyone needed to feel to able to

express what they thought or did in with regards to cyber-resilience without the fear of being judged, which covered points 1. and 2. Point 3. related to the fact that the session would last for 60 minutes after which it would be completed. Point 4. regarding confidentiality noted that the SME allocated an open physical space for the training which offered some but not complete confidentiality as cleaners and clients were able to pass through now and again. In addition, confidentiality was limited by the fact that the training data would be published in a study. Then, we provided the SME's staff with an opportunity to add five more points to the contracts if it made them feel more comfortable. After a short pause, they stated that they were comfortable with the current contract and did not wish to make further additions.

Self-disclosure: This term should be understood as derived from psychotherapeutic practice, namely as a tool for building connection and increasing transparency [51]. 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. Nevertheless, Yalom and Lescz [52, p. 343] warn that self-disclosure comes at a risk: "Every self-disclosure involves some risk on the part of the disclosurer—how much risk depends in part on the nature of what is disclosed. Disclosing material that has previously been kept secret or that is highly personal and emotionally charged obviously carries greater risk." Self-disclosure is a useful addition to the existing research by Cross [12], which focuses on simplifying cybersecurity training materials but neglects the importance of the human connection during the delivery of those materials.

We felt that it would be suitable to proceed with self-disclosure even before the session to show the lay audience the human side of what it means to work in this field. The example we selected also served another important purpose. It was used to illustrate that you must be able to control for the dangers in your immediate environment before you escalate to protecting it from "exciting things" like Russian hackers or foreign spies.

Our researcher disclosed an incident from a conference during his PhD. He related a story about how he was going over his private e-mails on the phone without paying attention to what was happening in the background. He then heard a colleague engage him in conversation from behind whilst clearly and brazenly tying his questions into the content of the author's e-mails. This was used as a way of highlighting how easy it is for a breach to happen.

We used self-disclosure as a way of explaining to the SME staff that we can also become careless which results in the leakage of sensitive communication. It was not his colleague's responsibility to safeguard his private e-mails, but the said researcher's. We also wanted to get them thinking about their physical space and how they were securing it when processing the data of their clients. It was a successful strategy as it prompted them to provide a very honest account of how wholly cyber insecure their company actually was. This in turn enabled us to formulate ideas for improvement based on the actual situation.

Dialectic approach: This term 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 dialectic approach was most apparent in the group interactive exercises, which reflected Finney's [14] applied and extended

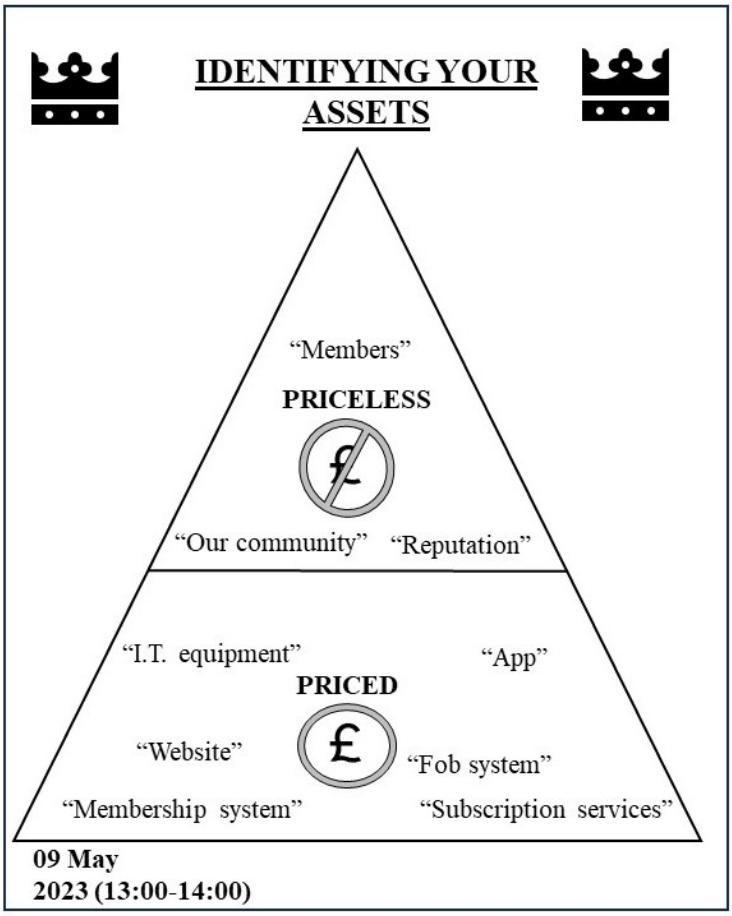

Figure 1: Identifying your assets

theory which remains captured in our published materials. 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 transfixed the latter onto a computer generated version for easier reading.

Exercise 1 Understanding harm to your assets: This interactive exercise was derived from Finney's [14] 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.

The reader can appreciate that the 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. This speaks to the community orientation of Scottish SMEs in deprived areas and the need for their enhanced protection from the side of the government as they are a source of jobs and services where there is a relative scarcity of both. In hindsight, there could have been more discussion about the connection between the priceless and priced assets because the damage to priced assets (e.g., website defacement) can trigger a negative reaction in the

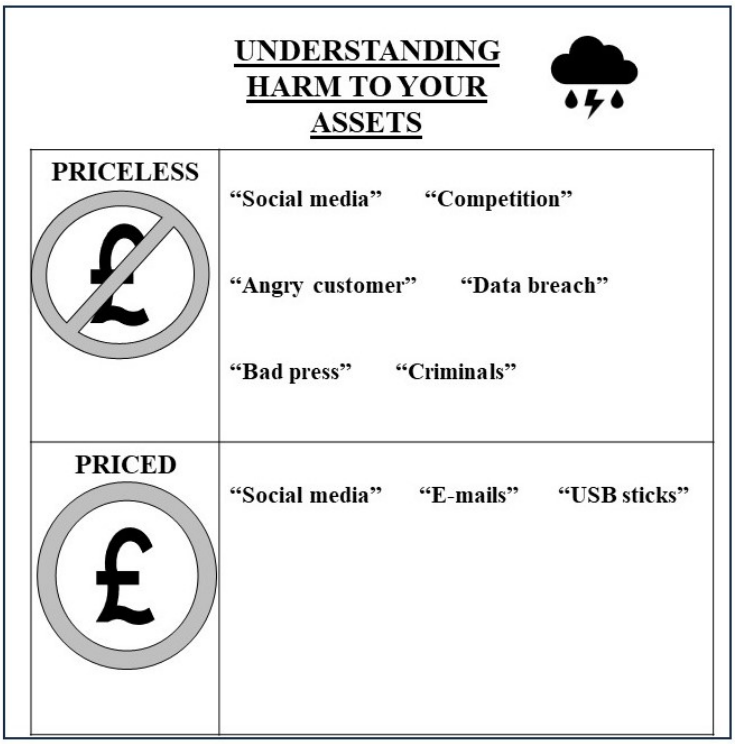

Figure 2: Understanding harm to your assets

members who will be prompted to unsubscribe. Likewise, the priceless asset of "Reputation" can be connected to how technology is embedded within formal and informal managerial decision-making [2].

On pages 8–10 of the training booklet [43] we present our own ideas and justification for priceless and priced assets. However, in line with the dialectical approach, we have advised staff to adjust these to their situation or simply prioritise the ones from Figure 1. if it suits them.

Exercise 2 Understanding harm to your assets: As before, we used an adapted version of Finney's [14] 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.

As shown in Figure 2, 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 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 the 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. Lastly, their experience of "Data breach" was connected to the cyber-attack that prompted the current collaboration on the client-centred cybercrime training.

Figure 3: Safeguarding your assets

On pages 11–14 of the training booklet [43] we present a scientific understanding backed up by referenced terminology that helps people understand harm to their assets. However, in line with the dialectical approach, we have advised staff to adjust these to their situation or simply prioritise the ones from Figure 2. if it suits them.

Exercise 3 Safeguarding your assets: This exercise is a theoretical extension of Finney's [14] 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 were 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 Figure 3. 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. Nevertheless, it was an important exercise to trigger thought on the subject and future replications can consider how to make the process more effective so that, for example, if staff list "Social media" as a "CYBER WORLD" THREAT" there is a matching solution "CYBER WORLD SAFEGUARD."

This could also be a derivative of the Memory card game (also referred to as Concentration or Pexeso) where 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?" Another pair of cards with "Data breach" on one side could contain sequence of advisory steps to the effect of "1. Report to management, 2. Report to Police Scotland, 3. Request an incident number for insurance" on the other side and so on. Then, just like with the classical Memory card game these cards would get mixed up so that each card from the pair is displaying a different side and staff would have to compete based on who pairs the most cards until no cards are left. We believe that this is will be a valuable pedagogical avenue as other current work in this domain that utilises games is designed for experts [15].

On pages 14–17 of the training booklet[43] we present a more technical and analytical synopsis of how to best safeguard the SME's assets. However, in line with the dialectical approach, we have advised staff to adjust these to their situation or simply prioritise the ones from Figure 3. if it suits them.

4.3 Evaluation of Training Materials

Self-evaluation: The ability to be reflective practitioners in this domain is of the essence as trainees will pick up on implicit emotions and thoughts. In line with Yalom's [51] recommendations about self-disclosure we commence with a reflection of our own processes during the training.

Firstly, it is important to note that delivering this training and interacting with the audience was somewhat anxiety-provoking. We felt very self-conscious about not being perceived as arrogant due to our professional background.

Secondly, we should disclose our own experience of responsibilised self-rhetoric. Getting the training up and running proved arduous and despite the manager's best efforts took a lot longer than we felt it should have done. We felt that the SME's staff should take on our advice or face the consequences of another attack if they do not. This is exactly the type of counterproductive attitudes that Renaud *et al.* [37] have warned against in their critique of the responsibilization agenda.

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 are implicitly included.

Their full pre-training and post-training scores are found in the Tables 1 and 2 in Appendix D as Participants 1–5 Within, we are supplying a short commentary on the progress of individual participants alongside a selection of appropriate quotes from their returned forms. Some participants did not answer all of the questions on one or either forms.

Participant 1: In this case, the participant rated their knowledge of cybercrime 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.

Here, it is evident that the participant underwent some internal process that they did not feel comfortable in sharing as their negative affectivity increased incrementally and their score for the lecturer's supportiveness was 50%, but they did not specify why. This could be because, as according to Participant 3, some members of the group preferred to have their questions answered instantly as opposed to being told to wait. Alternatively, the training may have triggered unpleasant feelings connected to the cybercrime, which became transferred onto the trainer [18].

Participant 2: In this case, the participant rated their knowledge of cybercrime 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 cybercrime 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, the 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 discoveries along the way. The reason why we respectfully asked them to wait was in order to maintain coherence in to the material, but it was perceived as unhelpful. Instead, we could have highlighted that it was a really good point and that they were ahead of the game.

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 cybercrime 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 [33]. According to Peytchev [33, 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 as per questions listed in the qualitative interview in Appendix C. However, participants did not respond to questions regarding the demographics and, in line with the ethics of the study, only submitted answers pertaining specifically to the training were included. Rather than supplying an answer to each question the general theme will be interpreted alongside representative quotes within the context of participants' questionnaire scores. The purpose of the qualitative interview was also to chart the participants' learning and retention over time. Hence, 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, which is nearly four months after the training.

The interviewed participants highlighted the importance of training as an awareness raising tool, which has shed light on an important topic. Hence, training as an awareness raising exercise was the dominant theme in their thinking.

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 as we have exemplified in Figure 1. We have specifically probed whether the participant was able to glean any benefit from this exercise to which they responded that:

> "'*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 from Figure 1. 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.

An important take home message is that both participants feel that if the SME gets attacked, then it is first and foremost the company's responsibility to fix it. This is a way of saying that the private sector should look after itself. In cases, where people get attacked, it should be the banks (i.e., private sector) who looks after them. On a subconscious level, the state is out of the equation, the training did not alter the responsibilized mindset.

5 CCCT Discussion

The purpose of this case study [11] was to answer the following research questions:

5.1 Research Question 1 (RQ1):

Will a collaborative and client-centred approach to cybercrime training improve staff's cyber-resilience posture?

We devoted focused resources into co-designing the training in partnership with the staff of an attacked private institution (§4.1). Based on research on co-authored online education into the Ukrainian war-zone [41, 42], we felt that these

approaches would be transferable into work on an attacked SME as well. This assumption was only partially accurate. In truth, the enthusiasm for this training felt thin from the start and the collaborative nature of co-authorship did not seem to override staff's other priorities. Eventually, 9 members of staff compiled the pre-training questionnaires, which enabled us to design a series of interactive exercises as showcased in the results as well as the booklet, which was distributed among staff in printed and bound format.

When it came to the delivery (§4.2) of the training, finding an appropriate time slot proved once again tricky due to the pressures faced by the business and despite the best efforts of management and staff. Once an appropriate slot was identified and we commenced with training delivery, we significantly drew from the mental health background of one of the authors. We felt that by practising self-disclosure [52, 51] about our own carelessness in data security we would level the power imbalance and enable people to open up. This was successful and we were able to understand the extent to which the company was truly vulnerable. We tried to work with this knowledge thoughtfully throughout the training by helping people connect the material from the discussions with the theory we were presenting. We were curious to see whether our self-disclosure would be reflected in the feedback that was collected after the training, but there was no mention of it. This suggests that it if it affected people's sharing of information, then it did so on a subconscious level.

We could see that the interactive exercises, which we exemplified via Figure 1, Figure 2 and Figure 3 activated the group and even the inactive individuals became more engaged. One male attendee suggested that the group is subdivided into "boys versus girls", which signalled a competitive element. Future studies that build on our findings can include an element of competitive games since the ones discussed by Kayali *et al.* [27] in the introduction were not described as competitive. Whether or not they should contain a gendered component is up to the future authors or, more precisely, up to the client SME's staff. If ours were competitive and gender-divided, the women would have overwhelmingly won because of two highly motivated individuals.

We were very interested to see how the subdivision of assets into priced and priceless would help inform the company's defence strategy. Whilst the participants spoke about it in a complimentary way, they did not exemplify how this dichotomy informed their defence strategy. Thereby, making it more of an awareness raising exercise rather than a tool that they could take with them into the field and implement. This makes us return to the various concepts and frameworks discussed in the related research (§2). If such a basic dichotomy is of little use to the hands-on people, then more effort is required to translate cyber-resilience knowledge into a language that is relatable. That extends to the language that is being used because, as we revealed in the aforementioned section, it is far too technical and specialist.

5.2 Research Question 2 (RQ2):

Will a collaborative and client-centred approach to cybercrime training improve reporting?

In the contexts of countries with a high level of responsibilization, this requires to be accounted for. 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 the evaluation (§4.3). 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. Hence, anyone that is interested in building upon our findings needs to do so with the realisation that they will come up against a mixture of factors affecting people's perceptions some of which are connected to responsibilization whilst others may be connected with an assimilation to online and offline criminality.

6 Limitations

The generalizability of the population sample in this case study is reflective of the regional variation found in Scottish areas with higher levels of deprivation rather than Scotland or SME research as a whole. Further research into the cybersecurity needs of SMEs in areas of low socioeconomic status is warranted as these constitute government income via taxation.

7 Conclusion

Within, we have rejected an exposé approach that would showcase our knowledge against the naivete of non-academic SMEs 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. This was developed and delivered despite temporal constraints and high dropout rates. The main contribution of the training was in awareness raising whilst some shift in working practices and behaviours was evidenced. Academia should collaborate more closely with the government in informing the education of attacked SMEs because documents such as the SBSS 2022-23 underline the entrenched problems of cybersecurity responsibilization in Scotland. Indeed, if the SBSS 2022-23 highlights that SMEs require regular external financing but omits cybersecurity obstacles, then one is left to wonder how much of that borrowed money goes towards rectifying cybersecurity incidents. This is why it remains the government's role to use research know-how for the purposes of developing qualified cybersecurity trainers and supporting vulnerable SMEs.

Acknowledgements

The first author would like to thank the University of Strathclyde for the grant of £56,154.89 as well as the Scottish Institute for Policing Research (SIPR) for the grant of £38,154.92. Importantly, the first author thanks Dr Jean Carletta for her expertise and additional grant (£2,559.06) via the University of St Andrews in Scotland.

References

[1] Bada, M., Furnell, S., Nurse, J.R.C., and Dymydiuk, J. 2023. "Supporting small and medium-sized enterprises in using privacy enhancing technologies," In *HCI for Cybersecurity, Privacy and Trust*, pp. 274–289.

[2] Barney, J. 1991. "Firm resources and sustained competitive advantage," *Journal of Management*, (17:1) pp. 99–120.

[3] Batchelor, S.A., and Gormley, C. 2023. "Repeat Violence in Scotland: A Qualitative Approach," *Scottish Centre for Crime and Justice Research University of Glasgow*, *CRIME AND JUSTICE*.

[4] Bjorge - Ulven, V., and Wangen, G. 2021. "A systematic review of cybersecurity risks in higher education," *Future Internet*, (13:2) pp. 39.

[5] Blažič, B. 2021. "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training." *Technology in Society*, (67:1).

[6] Bolun, I., Bulai, R., and Ciorbă, D. 2021. "Support of Education in Cybersecurity," *Pro Publico Bono - Magyar Kozigazgatas*, (1) pp. 128–147.

[7] Braun, V., and Clarke, V. 2021. "One size fits all? What counts as quality practice in (reflexive) thematic analysis?," *Qualitative Research in Psychology*, (18:3) pp. 328–352.

[8] Braun, V., and Clarke, V. 2022. "Conceptual and design thinking for thematic analysis," *Qualitative Psychology*, (9:1) pp. 3–26.

[9] Bunge, E., Williamson, R., Cano, M., Leykin, Y., and Muñoz, R. 2016. "Mood management effects of brief unsupported internet interventions," *Internet Interventions*, (5) pp. 36–43.

[10] Cabaj, K., Domingos, D., Kotulski, Z., and, Respício, A. 2018. "Cybersecurity education: Evolution of the discipline and analysis of master programs," *Computers & Security*, pp. 75–24.

[11] Chetty, S. 1996. "The case study method for research in small-and medium-sized firms," *International Small Business Journal*, (15:1) pp. 73–85.

[12] Cross, C., and, Kelly, M. 2016. "The problem of "white noise": Examining current prevention approaches to online fraud," *Journal of Financial Crime*, (23:4) pp. 806–818.

[13] Dragoni, N., Alberto, L.L., Massacci, F., and Schlichtkrull, A. 2021. "Are we preparing students to build security in? A survey of European cybersecurity in higher education programs [education]," *IEEE Security & Privacy*, (19:1) pp. 81–88.

[14] Finney, G. 2020. *Well Aware - Master the nine cybersecurity habits to protect your future*. Greenleaf Book Group, 1st. edition.

[15] Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., and Naqvi, S. A. 2019. "The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game," *IEEE Transactions on Software Engineering*, (45:5) pp. 521–536.

[16] Hamman, S., Hopkinson, K., Markham, R., Chaplik, A., and Metzler, G. 2017. "Teaching game theory to improve adversarial thinking in cybersecurity students," *IEEE Transactions on Education*, (60:3) pp. 205–211.

[17] Harris, M., and Patten, K. 2015. "Using Bloom's and Webb's taxonomies to integrate emerging cybersecurity topics into a computing curriculum," *Journal of Information Systems Education*, (26:3) pp. 219–234.

[18] Horwitz, L. 1964. "Transference in training groups and therapy groups," *International Journal of Group Psychotherapy*, (14:2) pp. 202–213.

[19] Hough, M. 2006. *"Counselling Skills & Theory,"* Hodder Arnold, 2nd. edition.

[20] Huang, R.-T. [2015.] "Overcoming invisible obstacles in organizational learning: The moderating effect of employee resistance to change," *Journal of Organizational Change Management*, (28) pp. 356–368.

[21] Hwee-Joo, K. and, Katerattanakul, P. 2019. "Enhancing student learning in cybersecurity education using an out-of-class learning approach," *Journal of Information Technology Education. Innovations in Practice*, (18) pp. 29–47,

[22] Inan, F., Namin, A., Pogrund, R., and Jones, K. 2016. "Internet use and cybersecurity concerns of individuals with visual impairments," *Educational Technology & Society*, (19:1) pp. 28–40.

[23] Ivy, J., Kelley, R., Cook, K., and Thomas, K. 2020. "Incorporating cyber principles into middle and high school curriculum," *International Journal of Computer Science Education in Schools*, (4:2).

[24] Johnson, C. 2019. "University of South Wales National Cyber Security Academy – creating cyber graduates who can 'hit the ground running': An innovative project based approach," *Higher Education Pedagogies*, (4:1) pp. 300–303.

[25] Jones, K., Namin, A., and Armstrong, M. 2018. "The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals," *ACM Transactions on Computing Education*, (18:3) pp. 1–12.

[26] Kappe, M., Härting, R.-C., Karg, C., and Deffner, D. 2023.. "Cybersecurity in SMEs - drivers of cybercrime, insufficient equipment and prevention," In *Procedia Computer Science*, (225), pp. 3631 – 3640.

[27] Kayali, F., Schwarz, V., Purgathofer, P., and Götzenbrucker, G. 2018. "Using game design to teach informatics and society topics in secondary schools," *Multimodal Technologies and Interaction*, (2:4) pp. 77.

[28] Khader, M., Karam, M., and Fares, H. 2021. "Cybersecurity awareness framework for academia," *Information*, (12:10) pp. 417.

[29] Knapp, K., Maurer, C., and Plachkinova, M. 2017. "Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance," *Journal of Information Systems Education*, (28:2) pp. 101–113.

[30] Liu, F., and Tu, M. 2020. "An analysis framework of portable and measurable higher education for future cybersecurity workforce development," *Journal of Education and Learning (EduLearn)*, (14:3) pp. 322–330.

[31] Marquardson, J., and Gomillion, D. 2018. "Cyber security curriculum development: Protecting students and institutions while providing hands-on experience," *Information Systems Education Journal*, (16:5) pp. 12–21.

[32] Payne, B., He, W., Wang, C., Wittkower, D., and Wu, H. 2021. "Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course," *Journal of Information Systems Education*, (32:2) pp. 134+.

[33] Peytchev, A. 2009. "Survey breakoff," *Public Opinion Quarterly*, (73:1) pp. 74–97.

[34] Pike, R., Brown, B., West, T., and Zentner, A. 2020. "Digital badges and e-portfolios in cybersecurity education," *Information Systems Education Journal*, (18:5) pp. 16–24.

[35] Pusey, P., and Sadera, W. 2012. "Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference," *Journal of Digital Learning in Teacher Education*, (28:2) pp. 82–88.

[36] Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., and Peersman, C. 2018. "Scoping the cyber security body of knowledge," *IEEE Security & Privacy*, (16:3) pp. 96–102.

[37] Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P, and Orgeron, C. 2018. "Is the responsibilization of the cyber security risk reasonable and judicious?," *Computers & Security*, (78) pp. 198–211.

[38] Schaeffer, D., Olson, P., and Eck, C. 2017. "An interdisciplinary approch to cybersecurity curriculum," *Journal of Higher Education Theory and Practice*, (17:9) pp. 36–40.

[39] Schatz, D., Bashroush, R., and Wall, J. 2017. "Towards a more representative definition of cyber security," *Journal of Digital Forensics, Security and Law*, (12:2) pp. 8.

[40] Scottish Government 2020. "Scottish index of multiple deprivation 2020."

[41] Sikra, J. 2022. "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.

[42] Sikra, J. 2023. "Evaluating a university curriculum delivered during Russia's invasion of Ukraine," *The Bulletin of Taras Shevchenko University of Kyiv Social Work*, (8:1) pp. 78–80.

[43] Sikra, J. 2023. "Client-centred cybercrime training for Scottish small-to-medium sized enterprises (SMEs) [delivered as part of PhD research]."

[44] Smith, S.C. 2023. "Toward a scientific definition of cyber resilience," *Proceedings of the 18th International Conference on Cyber Warfare and Security*, (18:1).

[45] Tagarev, T. 2016. "A Generic Reference Curriculum on Cybersecurity," *Information & Security*, (35:1) pp. 181–184.

[46] Taylor, B., Kaza, S., and Zaleppa, P. 2021. "CLARK: A design science research project for building and sharing high-quality cybersecurity curricula," *IEEE Security & Privacy*, (19:5) pp. 72–76.

[47] Thatcher, J.B., and Perrewe, P.L.2002. "An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy," *MIS Quarterly*, (26:4) pp. 381–396.

[48] Vain, J., and Kharchenko, V. 2016. "Enhanced Education for Cybersecurity and Resilience," *Information & Security*, (35:1), pp. 5–8.

[49] van de Weijer, S., Leukfeldt, R., and Moneva, A. 2024. "Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands," *Computers and Security*, (139).

[50] Workman, M., Luevanos, J., and Mai, B. 2022. "A study of cybersecurity education using a present-test-practice-assess model," *IEEE Transactions on Education*, (65:1) pp. 40–45.

[51] Yalom, I.D.2011. *"Staring at the sun - Overcoming the dread of death,"* Clays Ltd, St Ives plc, 2008 and 2011 edition.

[52] Yalom, I.D. and Leszcz, M.2005. *"The theory and practice of group psychotherapy,"* Basic Books, 5th. edition.

[53] Yang, S. 2021. "A meta-model of cybersecurity curriculums: Assessing cybersecurity curricular frameworks for business schools," *Journal of Education for Business*, (96:2) pp. 99–110.

[54] Yang, S., and Wen, B. 2017. "Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the united states," *Journal of Education for Business*, (92:1) pp. 1–8.

[55] Zuopeng, J.Z., Wu, H., Li, W., and Abdous, M. 2021. "Cybersecurity awareness training programs: a cost–benefit analysis framework," *Industrial Management & Data Systems*, (121:3) pp. 613–636.

[56] Švábenský, V., Čeleda, P, Vykopal, J., and Brišáková, S. 2021. "Cybersecurity knowledge and skills taught in capture the flag challenges," *Computers & Security*, (102:1).

CCCT Appendix

A CCCT Pre-Training Questionnaire

Age:

Gender:

Date:

Position:

Client-centred cybercrime 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

Age:

Gender:

Date:

Position:

Client-centred cybercrime 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.

C CCCT Qualitative interview

Demographics

Age Range (18-24; 25-34; 35-44; 45-54; 55-64; 64+):

Gender:

Date:

Position:

Educational attainment (Select the highest applicable):

a) Certificate of Higher Education – Advanced Higher/ Higher National Certificate

b) Diploma of Higher Education – Higher National Diploma

c) Bachelors Degrees – Graduate Diplomas and Certificates

d) Bachelors Degrees with Honours – Graduate Diplomas and Certificates

e) Masters Degrees (including all Postgraduate Degrees)

f) None apply, please specify in your own words your level of educational attainment.

Client-centred cybercrime post-training qualitative interview

1. Looking back at the time you spent at the client-centred cybercrime training, how helpful was it for your role in the company and why?
2. Looking back at the time you spent at the client-centred cybercrime training, how helpful was it for your personal life and why?
3. Has the client-centred cybercrime training affected your confidence in the realm of cybersecurity? If so, how, what changes to your confidence have you observed?
4. Has the client-centred cybercrime training affected your skills in the realm of cybersecurity? If so, how, what changes to your skills have you observed?
5. Since the time you have attended the client-centred cybercrime training, have you shown leadership/initiative in making your company more cybersecure? If so, what have you done that was an act of leadership/ initiative?
6. Since the time you have attended the client-centred cybercrime training, have you shown leadership/ initiative in making your personal life more cybersecure? If so, what have you done that was an act of leadership/ initiative?
7. Since the time you have attended the client-centred cybercrime training, how has your perception of the company's priceless assets evolved in cybersecurity?
8. Since the time you have attended the client-centred cybercrime training, how has your perception of the company's priced assets evolved in cybersecurity?
9. Since the time you have attended the client-centred cybercrime training, how has your understanding of the need to report cybercrime evolved?
10. If you or your company became a victim of a cyberattack how would you proceed with reporting this offence? Please supply a real or theoretical example for each.

D CCCT Table 1 and 2

Table 1. depicts the calculation of knowledge improvement via the client-centred cybercrime training based on subjective ratings. Improvement was measured as the positive increase in score from "Desired" score.

Participant no.	Knowledge		Knowledge	
	Pre-training		Post-training	
	Current	Desired	Achieved	Improvement
1.	4	8	6	Yes.
2.	5	8	6	Yes.
3.	2	6	5	Yes.
4.	5	8	5	No.
5.	2	3	2	No.

Table 2. displays the changes in emotionality prior and after the client-centred cybercrime training. Additionally, expressed as "%" participants supplied a rated assessment of the lecturer's supportiveness which can be further used to gauge insights from their scored ratings.

Participant no. (Lecturer supportiveness)	Emotions			Emotions		
	Pre-training			Post-training		
	Anxiety	Depression	Confidence	Anxiety	Depression	Confidence
1. (50%)	2	0	4	2	1	3
2. (100%)	2	0	8	3	1	9
3. (80%)	4	0	1	5	0	5
4. (100%)	5	0	4	0	0	0
5. (100%)	0	0	0	0	0	10