Police Cybercrime Training: Perceptions, Pedagogy and Policy

Cockcroft, T. W.; Shan-A-Khuda, M.; Schreuders, C.; Trevorrow, P.

Abstract

Cybercrime has become one of the most pressing developments for police organisations to engage with over recent years. One of the key challenges here is to understand how best to effectively impart relevant skills and knowledge about cybercrime throughout the organisation to enable police officers to react appropriately to such illicit behaviours. This paper is drawn from mixed-methods research undertaken as part of a major study into the effectiveness of cybercrime investigation within a large UK police force funded by College of Policing/Hefce. The research found that officers perceived some modes of training as considerably more effective than others and, similarly, highlighted some of the organisational contexts that impact negatively on the delivery of effective cyber training to police officers. The authors believe that the findings will have relevance to police training policies both in the UK and in the wider international context.

Introduction

Police education and training issues remain an area of interest to practitioners, managers, policy-makers and academics. In particular, the substantial growth in prevalence of cyber crime has, over recent years, led to challenges for police organisations in responding effectively to the new demands made on their resources by this relatively new phenomenon. In the United Kingdom, this development has emerged in parallel with an increasingly resource limited post-austerity policing landscape. Increasingly, therefore, there is a need for cyber training delivered within police

organisations to be as efficient and effective as possible in providing staff with the skills to effectively engage with this contemporary crime issue. The aim of this study, funded by College of Policing/Hefce, was to assess, via questionnaire, the perceived effectiveness of different styles of cyber training amongst police officers who had undertaken cyber training in a regional police force over a 30 month period. Simultaneously, the project drew on data from two in-depth semi-structured interviews to contextualise the data generated through the questionnaire. The resulting research, the authors believe, will have relevance to police cyber training strategy and policy at the national and international level.

Literature Review

Police training and education has long been a subject that stimulates discussion (Bryant et al, 2013). Whilst substantial debates in this area, such as the impact of Higher Education (Mosaliuk and Cress, 2013), are unlikely to be resolved soon, there remain several pressing issues. One of these pertains to the increasing orientation and responsiveness of the police to threats posed by digital crime and the most effective ways in which to prepare police organisations for the specific training needs around responding to these specific challenges. What is of note here, however, is that there is a very limited amount of existing research and knowledge surrounding this specific area of police operations.

Many of the recommendations for the improvement or enhancement of police training (in a generic and non-cyber context) are also relevant to training needs surrounding cybercrime. For example, Griffith (2015) notes that, increasingly, police training needs to make greater use of blended learning, encourage practitioners to prepare more detailed reports/outputs, be based on evidencing proficiency and draw from knowledge rather than ‘received wisdom’. The latter point raises an

important issue regarding what constitutes knowledge in policing. Not least, despite the rise of the Evidence-Based Policing (EBP) agenda there remains some scope for arguing that the variety of policework, coupled with the inherent discretion of the police role, necessitates the acknowledgement of experiential learning as being an important driver for effective police practice (see Wood et al, 2017 forthcoming). Notwithstanding Griffith's work, Mastrofski (2007) notes that there are some areas where we quite simply have insufficient knowledge surrounding police training and education.

One of the most practical concerns in this regard is in understanding the relationship between training and quality of police investigations. Marcum et al (2010) noted that, in the context of investigations focusing on policing possession of child pornography, training alone would not improve the quality and success of investigations. Successful investigations also depended upon appropriately skilled and motivated personnel being available in addition to the availability of high quality training. Existing literature also focuses on the orientation of non-specialist patrol officers to cybercrimes. For example, Holt and Bossler (2012) note that cybercrime has created substantial challenges for law enforcement, particularly at the local level, because whilst front line officers are usually first responders to cybercrimes, it is not known whether these staff are sufficiently trained, or confident, to do so. A broad range of evidence therefore points to the need for patrol officers to become more effective first responders to cybercrime calls. The evidence illustrates that many patrol officers are neither prepared nor sufficiently interested in taking an active role in addressing cybercrime at the local level. Holt and Bossler's (2012) work is helpful, therefore, in that it examined the factors that predicted patrol officer interest in cybercrime training and investigations in two South East U.S. cities. They found that officer views of policing cybercrime, the extent to which they valued cybercrime investigations and the extent of their computer skills

were the strongest predictors of patrol officer engagement with cybercrime efforts. The authors concluded that more needed to be done to focus officers on the value of investigating these types of crime.

Other sources also confirm that local responses to cybercrime are under-developed in relation to national responses. For example, the Police Executive Research Forum (2014) noted that cybercrime awareness and investigation skills needed to be embedded within local police officers so that they are able to identify crime situations as having a cyber element and are able to secure them until expert assistance becomes available. Similarly, they noted that local prosecutors and judges needed to be trained to increase understanding of this particular crime type.

It is perhaps unsurprising to note that law enforcement agencies have been slow, in some cases, to engage with and adapt to the newly emerging synergies between technology and crime. As a result, Wydra (2015) highlights the need for doing more to recruit a technologically literate workforce within the criminal justice sector. This in itself, raises wider questions about the role of secondary education in teaching technological skills to those who will become the law enforcement officers of the future. Similarly, Nice (2016) suggest that ICT needs to be more systematically embedded in formal education. Accordingly, Leal (2008) suggests, for example, that one way to deal with the threat of cybercrime is to recruit law enforcement officers with existing technical skills. This, in itself, impacts upon the responsiveness of police staff to new forms of training such as those which are delivered electronically. This is an important issue as, increasingly, police organisations are drawing on electronic forms of learning delivery as a way of reducing the costs associated with training. Monett and Elkina (2015) warn that e-learning delivery should not be viewed as a means of producing cut price training, and that it needs to be underpinned by technological and pedagogic expertise.

Despite the limited information in this area, it is possible therefore to identify five key themes in the literature. These are the *Tension between Evidenced Knowledge and Experiential Knowledge*; *Quality*; *Resources*; *Positioning of Knowledge within the Organisation*; and *Online Learning*.

Methodology

The aim of this project was to assess the perceived effectiveness of different styles of cyber training amongst staff in a large regional police force in the United Kingdom. This was achieved by a) assessing police officers' experiences of cybercrime training and b) understanding the issues of delivering cybercrime training by those involved in training delivery and strategy. A mixed-method strategy (semi-structured interview and questionnaire) was used to allow for 'expansion' (Burke Johnson and Christensen, 2014) whereby different approaches are utilised to explore different research aims within the same project. The use of a questionnaire was adopted to gather quantitative and qualitative data, in a neutral and systematic manner with a more wide-reaching scope than that of a more time intensive method, with the ultimate aim of gathering information for statistical analysis (Buckingham and Saunders, 2004). In addition, interviews were employed in order to gather a more in-depth, smaller scale and subjective viewpoint and to provide for clarification and explanation of themes that may have arisen in the survey element of the data collection phase (Cohen and Manion, 1994; Maykut and Morehouse, 1994).

According to Kilpatrick (1979) there are four general levels at which to evaluate training, regardless of the format. These are 'Reaction'; 'Learning'; 'Transfer'; and 'Results'. The first three points were addressed via the survey and were broken down into specific types of questions. For

this project, ‘Reaction’ focused on participants’ subjective feelings about the training, their satisfaction with their learning and the perceived relevance of the learning to their job (Strother, 2002). ‘Learning’ explored officer perceptions of how the learning had led to changes of skills, knowledge and attitude and ‘Transfer’ (the extent to which learning leads to changes in behaviour), whilst normally collated via customer satisfaction results (see Strother, 2002), was elicited in this study from the participants using the questionnaire. These elements were incorporated into the design of the survey and were covered by seven questions (referred to throughout as ‘items’) repeated for each of the training types (the questions covered: Format, Satisfaction, Relevancy, Useful of Knowledge, Increase of Knowledge, Increase of skills and Increase of job performance). The level of ‘Results’ (Kilpatrick, 1979) was not incorporated as it focuses on the impact on the organisation of changes in behaviour and was beyond the scope of the research project and, therefore, this paper.

The questionnaire was circulated, by the police force, to approximately 600 police officers who had attended a cybercrime training course, attracting 128 responses. The questionnaire had been designed, in conjunction with staff members from the organisation, to collate information on the four identified training methods used within the organisation for cyber training, namely: Online (i.e. delivered remotely and electronically), Face to Face (i.e. traditional classroom-based training), Workshop (i.e. loosely structured training events), and Q&A (i.e. informal exchanges between colleagues where specific questions are asked and responded to). The quantitative data was analysed using primarily some basic frequency analysis, although exploratory factor analysis (utilising the Kaiser-Meyer-Olikin measure for verification), cluster analysis and t-tests were also

conducted. The qualitative data generated through the free text option of the survey was analysed using a manual thematic analysis (Braun and Clark, 2006).

Further qualitative data was generated through two semi-structured interviews (with two members of police staff involved in the strategic and operational delivery of police training). These semi-structured interviews were based on questions derived from the findings of a Needs Assessment conducted in cyber needs within the organisation as part of a major funded study, and from a literature review conducted into police cyber training The semi-structured interview format allowed for themes to emerge during the course of the interview which were not pre-empted by the interviewer's knowledge of the field. The interviews were then transcribed by a reputable transcription company and then subjected to a thematic analysis (Braun and Clark, 2006) using Nvivo 10. Given the constructivist framework adopted in this piece of small scale qualitative research no claims are made in respect of the 'transferability' of findings (see Guba and Lincoln, 1994).

Findings

Quantitative findings from the questionnaire

The quantitative analysis addressed the following two research questions:

i. What do the seven items (Format, Satisfaction, Relevancy, Useful of Knowledge, Increase of Knowledge, Increase of skills and Increase of job performance) of perceived effectiveness of each cyber training style tell us? Is

there any unique characteristic of a training style that differentiates it from other training styles?

ii. Is there a training style preferred by the participants?

There are considerable debates around analysing Likert Scale data such as averaging the numbers, treating as interval data and carrying out parametric statistics (Westland, 2014). Consequently, a non-parametric test such as Wilcoxon matched-pair signed-rank test was conducted. However, the results were similar to those generated by a parametric test.

The cyber training style of 'Q&A' received only 4 responses in the questionnaire which is too small for any statistically significance testing, hence was removed from the quantitative analysis of the results. The analysis thereby focuses on Online, Face-to-Face and Workshop style of cyber training.

Research question i focuses on assessing the overall reliability of participants' scores in all seven items in each training style. All three training styles: Online, Face to Face and Workshop have high reliabilities with Cronbach's α = .882, .918, .989 respectively.

However, a high value of Cronbach's α in each training style does not indicate one-dimensionality (Grayson, 2004). A statistical procedure such as Factor Analysis confirms any underlying dimension in the data (Field, 2013).

Online cyber training style

A principal component factor analysis was conducted on the seven items with varimax rotation. The Kaiser-Meyer-Olkin measure verified the sampling adequacy for the analysis, KMO = .76

('middling' according to Hutcheson & Sofroniou, 1999). An initial analysis was run to obtain eigenvalues for each factor. Two factors had eigenvalues over Kaiser's criterion of 1 and explained 76.51% of the variance. The scree plot was ambiguous and showed inflexions that would justify retaining 2 or 3 factors. Two factors were retained because of the convergence of the scree plot and Kaiser's criterion on this value. Table 1 shows the factor loadings after rotation.

[INSERT TABLE 1]

Table 1 reveals two components or factors where several items loaded highly (>.73): Format, Satisfaction and Increase of skills are related to *Component 1* and Relevancy to job role, Usefulness of knowledge, Increase of Job Performance are related to *Component 2*. Conceptual meaning of the factors is discussed under 'Characteristics of Each Training Style'.

A paired-samples t-test revealed that participants scored more highly for *Component 2* (M=10.13, SD=2.433) than *Component 1* (M=9.10, SD=2.702), a statistically significant higher mean of 1.03, 95% CI [.402, 1.663], t (61) =3.274, p<.001.

Face to face cyber training style

Table 2 shows the factor loadings after rotation. All the seven items of perceived effectiveness do not indicate any dimension of Face to Face cyber training.

[INSERT TABLE 2]

Workshop cyber training style

Table 3 below does not indicate any underlying dimension in Workshop training.

[INSERT TABLE 3]

In summary, the above reliability analysis and factor analysis indicated that online training style has two dimensions, however, Face to Face and Workshop training style have no such dimensions. The characteristics are discussed in detail under 'Characteristics of Each Training Style'.

Statistical tests to assess perceived preference to any training style

Research question ii about preference to any training style is addressed in three ways. Firstly, a comparison is made *within* the seven items of each training style. Secondly, a comparison is made *between* each training style based on the seven items. For example, we have compared the measure of appropriate format of Online and Face to Face training styles. Finally, a comparison is made *between* the overall score of seven items for each participant in each training style.

Paired-samples t-test was conducted to determine whether a statistically significant mean difference exists within the seven items. Because of small sample size (n=8), we have excluded Workshop training style. A summary result is presented below:

Differences within the seven items of each training style

Online

Results from the t-test suggest that participants of Online training have preferred the relevancy of the training to the appropriateness of the format. For example, participants scored considerably less for 'format was appropriate' (M = 2.89, SD = 1.069) than for 'the training was relevant to the job role' (M = 3.76, SD = 0.912), a statistically significant decrease in average score of 0.87 on a scale of 1 to 5, 95% CI [-1.129, -.598], t(65) = -6.498, $p < .001$, d = 0.8.

Face to Face

Results from the t-test suggest that participants of Face to Face training have preferred the appropriateness of the format to the improvement in job performance. For example, participants scored considerably highly for 'format was appropriate for training delivered' (M = 4.46, SD = 0.718) than 'Job performance has improved' (M = 3.75, SD = 1.101), a statistically significant higher mean of 0.71 on a scale of 1 to 5, 95% CI [.518, .892], t (121) = 7.472, $p < .001$, d = 0.7.

Comparison between each training style based on seven items using paired t-test

Paired-samples t-test was conducted to determine whether a statistically significant mean difference exists between all three training styles. Because of the small sample size (n=8) in Workshop training style, the Wilcoxon Matched-pairs Signed-ranks Test (nonparametric equivalent to paired samples t-test) has been conducted in comparing Online and Workshop; Face to Face and Workshop. A summary result is presented below:

Online and Face to Face

Results from the t-test suggest that overall participants' perception between Online and Face to Face training style differ significantly in all of the seven items of perceived effectiveness of a training style. For example, participants scored considerably less for 'Online format was appropriate' (M =2.94, SD = 1.140) than 'Face to Face format was appropriate' (M = 4.60, SD = 0.629), a statistically significant decrease in average score of 1.66 on a scale of 1 to 5, 95% CI [-1.97, -. -1.33], t (66) = - 10.26, $p < .001$, d = 1.66.

Online and Workshop

A Wilcoxon signed-rank test determined that there was no statistically significant ($p > .05$) median difference in any of the seven items between Online and Workshop training style.

Face to Face and Workshop

A Wilcoxon signed-rank test determined that there was no statistically significant ($p > .05$) median difference in any of the seven items between Face to Face and Workshop training style.

Comparing the overall score

A method of assessing the preferred training style by the participants is to compare the overall score in each training style.

[INSER FIGURE 1]

[INSERT FIGURE 2]

[INSERT FIGURE 3]

We can see from **Figure 1** (13.33% of overall score is 21) and **Figure 2** (22.22% of overall score is 35), that the Face to Face training style is preferred to the Online training style by the participants in terms of overall score. A paired-samples t-test was conducted to determine whether a statistically significant mean difference existed between the preferences.

Participants' overall score for Face to Face cyber training (M =30.72, SD = 4.811) is considerably higher than for Online cyber training style (M =22.36, SD =5.275), a statistically significant higher mean of 8.36, 95% CI [6.673, 10.047], t (49) =9.956, $p < .001$, d =1.4.

Consequently, there is enough statistical evidence to suggest that participants preferred the Face to Face cyber training to the Online cyber training. However, because of the small sample size (n=8), no comparison has been conducted between Online and Workshop and Face to Face and Workshop.

Summary of the quantitative findings from the questionnaire

The overall discussion focuses on the two research questions: 'what does each of the seven items measure of perceived training effectiveness tell us about a training style?', and 'is there a training style preferred by the participants?'

Characteristics of each training style

The two latent factors in Online training are *Component 1* and *Component 2* and relate to different levels of understanding of the impact of training. The former represents Kirkpatrick's (1979) level of 'Reaction' (How well the learners liked the training session)'. The latter, represents Kirkpatrick's (1979) level of 'Transfer' (How well learners changed behaviour).

The first factor, *reaction*, relates to perception of format (whether the format was appropriate for the training delivered), satisfaction (with what was learnt), and skills (whether participants believe their skills have increased or improved after the training). This factor represents how well the

learners accepted the training session, which is related to the concept of "reaction" proposed by Kirkpatrick (1979).

The second factor, *'Transfer'*, relates to relevance (participants' perception of whether training received was relevant to job role), use (whether they will use knowledge gained in the job role), and performance (whether job performance has been improved). Continuing Professional Development (CPD) relates to competency requirement of roles and further enhancement of job performance. Hence, it could be argued that 'Transfer' might relate to CPD in Online training.

Analysis indicates that both factors contribute to the perceived training effectiveness, where 'Transfer (M=10.13, SD=2.433)' has a higher impact in perceived effectiveness of online training than 'Reaction (M=9.10, SD=2.702)'. Therefore, any CPD courses in Online training might consider relevancy, use of knowledge gained in the job role and improvement of job performance.

The quantitative results have not revealed any such factor within Face to Face and Workshop training style. This lack of patterned relationship might indicate that all of the seven items "go together" (DeCoster, 1998, cited in Yong and Pearce, 2013, p.80) in measuring the perceived effectiveness of training style in Face to Face and Workshop.

Preferences to any training style by the participants

The results strongly suggest that participants perceived the Face to Face training style to be more effective than the Online and Workshop styles. The effectiveness of Face to Face was significantly higher in terms of every one of the individual measures, and also in terms of the total score comparison. The quantitative data does not indicate any situation where Online or Workshop was

more effective than Face to Face. The qualitative analysis presented below, provides further insights, including the view that Face to Face delivery is appropriate for all types of training with more nuanced responses identifying its particular strengths in relation to cyber with practical elements.

Qualitative findings from the questionnaire (summary)

These findings refer to the thematic analysis of the free text qualitative data generated by the questionnaire.

Online learning was viewed as accessible and unconstrained in terms of pace of learning. Likewise, it cut down on logistical issues of attending a training event at somewhere other than a member of staff's regular workplace. However, it was viewed as not encouraging a particularly deep level of learning, as the degree of interaction was limited. It was viewed as appropriate for basic or refresher training, or as a learning stage to be delivered prior to attendance on a classroom-based session.

Face to Face learning was viewed very positively due to the interactive elements of it. The presence of skilled and knowledgeable trainers was valued by those attending sessions and the ability to seek clarification on complex issues was likewise perceived very positively. Similarly, the group nature of such events allowed for learning and clarification through the sharing of experiences with other participants. A significant proportion felt that this mode of delivery was appropriate for all

training with more nuanced responses identifying its particular strengths in relation to complex subject areas (such as cyber) and those with a practical element.

Respondents asked to identify the characteristics of their ideal training session suggested that it would be Face to Face, involve a classroom environment and have relevance to practice. They also suggested that a combination of online and Face to Face training could work well.

Qualitative findings from the semi-structured interviews

These findings refer to the thematic analysis of the semi-structured interviews held with two stakeholders. Three substantive themes emerged from the thematic analysis - 'Modes of Delivery', 'Resources' and 'Strategic Positioning of Cybercrime Training'.

Modes of Delivery

Substantial reference was made to 'e-learning' in the interviews and it was acknowledged by one of the interviewees that, '...with a lot of people, e-learning doesn't resonate. They cannot understand what it is that they're actually learning. They need somebody to actually explain it in layman's terms to them' (Interview 2). The same interviewee noted that such people prefer interactive modes of learning because it allows them to ask questions and to have the implications of the issues articulated to them. E-learning appears to be more positively perceived when combined with a more traditional delivery format. Of interest here is that the interviewees saw e-learning approaches working in both a post-interactive learning format or in a pre-interactive learning format. For example, in respect of the latter, one interviewee noted that, '...there are a

number of courses now where we do run pre-course learning, which is distance learning, e-learning, which then allows us to shorten the course and then build on the learning that's done from the e-learning' (Interview 1).

Interviewees also referred to 'classroom' styles of teaching delivery. It was noted that, given the technological nature of the information being presented in cyber training, those with limited information technology skills might have less positive experiences of cyber training initiatives. Similarly, it was stated that the traditional classroom approach did not always have to be adhered to, with one respondent suggesting that the main requirement was that students were in an interactive learning environment where they could ask questions.

Whilst 'mixed capability groups' were not seen as a substantial issue by the interviewees, one did note that this could impact on learning. He did feel. ultimately, that all those who attended training would, regardless of ability, learn how to undertake their role more efficiently. It was also stated, by one interviewee, that the mainstream cyber course was viewed by the College of Policing as a 'dual trainer course' (i.e. using two trainers) which would allow for support to be given to those who finding it difficult to engage with the material. However, in reality, it was unfeasible for such courses to be delivered with two trainers given resource issues.

Resources

It was acknowledged by both interviewees that there existed 'training gaps' and that the increasing prevalence of cyber issues meant that training would struggle to cover all relevant areas and subjects. Similarly, it was difficult to identify and train all appropriate staff and this meant that some elements of cyber training were 'diluted' and 'rushed'. Furthermore, one interviewee noted

that lengthy procurement procedures meant that by the time software was usually adopted (a decision often based on whether software was free or not) it was often obsolete.

Resource limitations impact across all dimensions of cyber training and will impact on all dimensions of the discussion. One interviewee noted, for example, that prioritization meant that some subject areas would fall by the wayside to accommodate newer and more acute issues that were considered of more pressing importance. Such resource pressures mean that there is increased focus on the potential for regional collaboration in terms of resource provision between neighbouring forces. One of the key themes to emerge from the interviews was around 'human resources', in respect of the limited human capacity to deliver all training to the preferred standard and in respect of the difficulties for individuals to relinquish their workload to make themselves available for training. In respect of the former, there were seen as being insufficient trainers in post to deliver the training requirements of the organisation which has 8,000 staff. One interviewee noted that the large amount of time spent delivering learning meant that there was little scope to develop new materials or to approach work strategically. He noted that he spent over 90% of his deployed time in the classroom and, beyond that, responded to ad hoc requests for help from individual officers presenting issues of a technical nature.

Changes to shift patterns have resulted in the loss of scheduled training days for staff making it ever harder for officers to engage with training sessions. This absence of protected learning time was seen as a particularly negative impact on learning. This in itself causes further inefficiencies due to courses subsequently running, because of these issues, with less than the anticipated student numbers.

'Estates' also provided some issues in respect of resources. Given the larger numbers of new police

recruits coming through, much of the dedicated space for learning is being taken up by new recruits on the Initial Police Learning and Development Programme (IPLDP). This had resulted in insufficient training facilities for classroom-based learning delivery. Resource limitations were noted as having an impact on the format of cyber training. Whereas, previously, a three-day training block might previously have been stretched out into five days, now training was liable to be of shorter duration and more intense meaning that desirable elements of training were being pared back to those considered essential.

Strategic positioning of cybercrime training

A number of issues emerged which could be categorised under this broad heading. One contextualising factor that emerged in the interviews was that much police learning is experiential. As such learning is therefore generated through officers' work-based experiences rather than their training there was a perceived need for formal training to complement informal processes of knowledge acquisition.

The first identified theme is termed '*Tension between General and Bespoke Training*' and refers to ideas expressed in the interviews regarding the extent to which generic cyber training was considered appropriate. One of the views suggested that bespoke cyber training for particular roles was the favoured approach and these have been developed and delivered, for example for PCSOs and those with crime reduction roles, where investigative and evidential elements would not be required. Of interest here, however, is that a counter view also emerged. The police is an organisation where individuals take on new roles on a regular basis and where certain elements, such as the preservation of evidence, cut across particular roles. One interviewee suggested that

general training was helpful as it allowed staff to develop institutional knowledge around cybercrime as it impacted on policework beyond the trainees' immediate role and that this could be positive for the organisation.

Data from the two interviewees also touched on the ways in which negativity about cyber training might, in part, be caused by the different ways in which members of the organisation come to undertake training. As part of the Personal Development Review a member of police staff might identify a training event they wish to attend or be recommended to attend by their line manager. Outside of this process, there are other ways in which staff can ask to be supported in an application to do a particular training course. However, some of the cyber training takes place within other training packages. One such example is that the cyber training which takes place within the detective training programme was met with reluctance by some attendees who failed to appreciate the relevance of the cyber input.

The issue of '*Role of Assessment*' also arose during the interviews. Assessment was not seen as necessary for lower level basic cyber training, for example that which might be appropriate for PCSO roles. For those with a more in-depth knowledge requirement, such as subject matter experts who might be giving advice and who will need to prove understanding of, for example, evidential issues, assessment would be more appropriate.

Interviewees also spoke about the issue of '*Refresher Training*'. This is an important area as it refers to the need to update practitioner knowledge over time. Concern was raised by one interviewee that for those who had taken the cyber training in 2014 there had been no refresher training despite developments in the field progressing substantially over that period. However, providing widespread refresher training, in a traditional format, to the force's 4,000 police officers

would prove to be difficult logistically. Two alternatives were provided. One, that refresher training could take the form of directing officers to online information (as opposed to online training) or, alternatively, using subject matter experts within the organisation informally to cascade information.

'*Probationer Training*' was referred to by one of the interviewees who was keen to address the basic core cyber knowledge that every police officer should possess. It was originally envisaged that the week-long mainstream cyber course would be replicated in full on the IPLDP. This system worked for three or four cohorts. However, when recruitment increased substantially the resource constraints around cyber training ensured that only two days of this training now make it onto the probationer programme. This raises questions about the possibility that the baseline level of cyber knowledge amongst police is now insufficient.

'Areas of Potential Development' also arose as a subject within the interviews. Two particular issues were mentioned. The first was of '*Subject Matter Experts'* and were referred to by both interviewees. This idea suggests that the organisation should look to develop expert high level knowledge in particular individuals who then become a resource to lessen the reliance solely on formal training. In practice this would mean that, whilst officers might have basic skills in an area, if they felt out of their depth they could engage with an expert and get appropriate information for their immediate needs. That said, questions were raised about what would constitute an appropriate number of such individuals.

Discussion

The literature review highlights a number of important themes around the effective delivery of cyber training. These can be summarised as the tension between *Evidenced Knowledge* and *Experiential Knowledge*; *Quality*; *Resources*; *Positioning of Knowledge within the Organisation*; and *Online Learning*. '*Pace of Technological Change*' emerged as substantive area within this project but one that had not been explicitly articulated in the existing literature. It should be noted that these thematic categories should not be considered as discrete and that they can and do overlap at times.

The tension between *Evidenced Knowledge* and *Experiential Knowledge* is important. Traditionally, police work has been viewed as being underpinned by a corpus of experiential, as opposed to evidenced knowledge. That is to say, the knowledge needed to undertake efficient police work has largely been viewed as being driven by experience, be it either personal or informally from other officers (Shearing and Ericson, 1991). Increasingly literature (perhaps driven by the EBP agenda) is seeking to position tested knowledge as the key driver of good police practice. However, one of the key findings of the survey was that many police officers very much value those modes of cyber training that allow for interaction and clarification and which are based on practical situations or scenarios. These tend to reinforce the idea that police officers may value the experiential elements of learning which may not be surprising given the large degree of discretion at their disposal. Likewise, it might suggest that evidence-based knowledge might have less impact on learners dealing with more complex areas of police work. That said, officers still did tend to see value in training based on the presentation of evidential knowledge, for example in respect of procedural training or refresher training where prior learning had already been successfully undertaken.

The theme of *Quality*, likewise, emerged in the research (see Marcum et al 2010). Respondents drew attention to the fact that training was more likely to be effective if it was delivered by quality trainers, if the content/format was viewed as appropriate or relevant and if the composition of the class cohort was appropriate. Trainers who were knowledgeable and receptive to questions were highly thought of but this needed to be supported by a course that was relevant and appropriately structured. A theme that emerged through the findings that was not identified in the existing literature was that of the negative impact, perceived by some, of having classes of varying ability. Whilst this reflects broader and ongoing pedagogic debates (see, for example, Boaler et al, 2000), it appeared that the technical element of cyber training could alienate those officers who were less confident with technology. This issue may, however, be exacerbated by resource issues. One of the interviewees did note that some of the College of Police cyber training was envisaged as being delivered by more than one trainer and that this would help to ameliorate this particular issue. However, due to financial constraints such delivery models could not always be utilised.

The issue of *Resources* appears to have a substantial impact, both in the literature (see Leal, 2008) and in the present study. One interviewee referred to how training was becoming 'diluted' and 'rushed'. This might be unsurprising in the context of an increasing restriction on police funding in recent years, estate restrictions on appropriate teaching spaces, restricted numbers of training staff, a growing focus on the training of 'essential' (as opposed to 'desirable') subjects, shortened courses and the need to make difficult choices around the prioritisation of different needs. These major issues have also been apparently impacted by changes to staff rotas which have made it harder to free up time for training in staff work time. What is apparent, therefore, is that formal traditional training models appear at present to be leading to real questions of sustainability.

Increasingly, a shift to exploring options of informal training, delivered by subject matter experts, appears to be one area from which new strategies might evolve.

Positioning of Knowledge within the Organisation is an important strategic challenge facing police organisations and was previously identified by the Police Executive Research Forum (2014). The Police Executive Research Forum research suggested that knowledge of cyber issues needs to be spread across all areas of police organisations, not just in silos of expert knowledge. One of the key reasons for this is to ensure that the integrity of evidence at crime scenes attended by first responders is not compromised (Holt and Bossler, 2012). Such a strategy poses issues for police organisations as it means that technical knowledge has to be made integral to the work of those police staff with very broad-ranging roles. Such staff may feel that they have insufficient technical knowledge to engage effectively with such training. Likewise, again echoing Holt and Bossler's findings, this research found that some people attending cyber courses failed to see the relevance of such training to their work role. Data from the semi-structured interviews drew attention to this issue and suggested that more needed to be done to explain the importance of cybercrime (and cybercrime training) to those working throughout the organisation, and not just in cyber specific roles.

The issue of *Online Learning* emerged as a major element of this research. As noted by existing literature in this area (see Monett and Elkina, 2015), there are concerns that such a mode of delivery can be seen as a means of providing inexpensive training and that this raises issues surrounding the technological and pedagogic underpinnings of the approach. The quantitative data suggests that, in a general sense, Online learning was significantly less well perceived than Face to Face learning. However, the analysis also suggests that Online learning was viewed positively in respect of how it related to issues that we would equate with Continuing Professional Development (CPD).

Therefore, it could be suggested that online learning was not viewed particularly positively as a means of general training provision but that it was viewed as having a positive contribution to make in some more focussed areas. In terms of basic procedural training, refresher training or as a means of providing background knowledge prior to a traditional classroom–based training event, it tended to be viewed more positively. It also allowed training to take place at a time and place of the trainee's choosing. However, it was viewed as less helpful for training where more complex concepts were being communicated or where there was a need for practical application or shared experience to embed knowledge.

One theme which was not clearly identified in the existing literature was *Pace of Technological Change*. In some respects, it is very much linked to the issue of *Resources* and refers to the extent to which technological change tends to raise pronounced issues for cyber training in respect of training packages becoming obsolete more quickly than for other areas of police work and also raises challenges in respect of the form and frequency of refresher training. It also can create a technology lag in which, after lengthy procurement processes, an organisation's technological resources quickly become outdated in comparison to the technologies being used within the communities that they serve.

Conclusion

This project aimed to assess the experiences and perceptions of cybercrime training of staff in a large UK police force. It drew on a mixed methods design to explore, via an online questionnaire, quantitative and qualitative data drawn from 128 respondents. It also drew on two semi-structured interviews with one strategic and one operational stakeholder. This data provided a valuable set of contextualising qualitative data.

The research began with a literature review. Whilst there is limited literature in the area of cybercrime training in police organisations a number of themes were identified. These reflect a tension between experiential and evidence-led learning, the scope for blended learning, the need for high quality training materials and delivery, the challenges of successfully integrating e-learning packages for this form of training and the need for first responders to cybercrimes to have sufficient skills in (and engagement with) cyber investigation techniques and protocols. The findings largely support the themes that emerged from the literature review. They also suggest that the pace of technological change has a negative impact on the perceived effectiveness of training in the absence of a strategic direction on refresher training. The findings of this project could be enhanced by extending it to undertake a more expansive sample for the questionnaire (from more than one police organisation) and to extend the use of focus groups and semi-structured interviews.

References

Boaler, J., William, D., and Brown, M. (2000). 'Students' Experiences of Ability Grouping – Disaffection, Polarisation and the Construction of Failure', *British Educational Research Journal,* **26**(5), 631-648.

Braun, V. and Clark. V. (2006). 'Using thematic analysis in psychology', *Qualitative Research in Psychology,* **3**(2), 77-101.

Bryant, R., Cockcroft, T., Tong, S. and Wood, D, (2013), 'Police Training and Education: Past, Present and Future.' In J. Brown (ed), *The Future of Policing*, Abingdon: Routledge, pp. 383-397.

Buckingham, A. and Saunders, P. (2004). *The Survey Methods Workbook*. Cambridge: Polity Press Ltd.

Burke Johnson, R. and Christensen, L.B. (2014), *Educational Research: Quantitative, Qualitative, and Mixed Approaches (5th edition)*. London: Sage.

Cohen, L. and Manion, L. (1994). *Research Methods in Education (4th edition)*. London: Routledge.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences (2nd ed)*. Hillsdale, NJ: Lawrence Erlbaum Associates.

DeCoster, J. (1998). *Overview of Factor Analysis*. Available from: <http://www.stat-help .com/notes.html> [Accessed 1st May 2017].

Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics (4th ed).* London: SAGE Publications Ltd.

Grayson, D. (2004). 'Some Myths and Legends in Quantitative Psychology.' *Understanding Statistics,* **3**(1): 101-134.

Griffith, D. (2015). '25 Ways to Make Police Training More Effective', *Police: The Law Enforcement Magazine*, http://www.policemag.com/channel/careers-training/articles/2015/04/25-ways-to-make-police-training-more-effective.aspx (last accessed on 31/10/16).

Guba, E.G. and Lincoln, Y.S. (1994). 'Competing Paradigms in Qualitative Research.' In N. K. Denzin and Y. S. *Lincoln* (eds), *Handbook of Qualitative Research*, London: Sage, pp. 163-194.

Holt, T.J. and Bossler, A.M. (2012). 'Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments.' *Cyberpsychology, Behavior, and Social Networking*, **15**(9), 464-472.

Hutcheson G. and Sofroniou N. (1999). *The Multivariate Social Scientist: Introductory Statistics Using Generalized Linear Models*. London: Sage.

Kirkpatrick, D. (1979). 'Techniques for Evaluating Training Programs.' *Training and Development Journal*, **33**(6): 78 – 79.

Leal, J. (2008). *E-Learning and Online Education: Implications for the Future of Law Enforcement Training*. Sacramento: California Commission on Peace Officer Standards and Training.

Marcum, C.D., Higgins, G.E., Freiburger, T.L. and Ricketts, M.L.(2010). 'Policing Possession of Child Pornography Online: Investigating the Training and Resources Dedicated to the Investigation of CyberCrime.' *International Journal of Police Science and Management*, ***12***(4): 516-525.

Mastrofski, S. (2007). 'Police Organization and Management Issues for the Next Decade.' *Paper Presented at the National Institute of Justice (NIJ) Policing Research Workshop: Planning for the Future*. Washington, DC, November 28-29, 2006.

Maykut, P. and Morehouse, R. (1994). *Beginning Qualitative Research. A Philosophical and Practical Guide*. London: The Falmer Press.

Monett, D. and Elkina, M. (2015). 'E-Learning Adoption in a Higher Education Setting: An Empirical Study', *Proceedings of the Multidisciplinary Academic Conference*, Prague, October 2015.

Moskaliuk, J. and Cress, U. (2013). 'Impact of Virtual Training Environments on the Acquisition and Transfer of Knowledge', *Cyberpsychology, Behavior and Social Networking*, **16**(3): 210-213.

NICE (2016). *National Institute for Cybersecurity Education Strategic Plan 2016*, Washington, DC: United States Department of Commerce.

Police Executive Research Forum (2014). *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime*. Washington, DC: Police Executive Research Forum.

Shearing, C.D. and Ericson, R.V. (1991). 'Culture as Figurative Action', *British Journal of Sociology*, **42**(4): 481-506.

Strother, J.B. (2002). 'An Assessment of the Effectiveness of E-learning in Corporate Training Programs*.' The International Review of Research in Open and Distributed Learning 3 (1)*. Available: http://www.irrodl.org/index.php/irrodl/article/view/83/160

Westland, S. (2014). *The Dangers of Likert Scale Data* [ONLINE]. Available from: < http://colourware.org/2014/02/18/the-dangers-of-likert-scale-data/> [Accessed 30th April 2017].

Wood, D, Cockcroft, T, Tong, S. and Bryant, R. (2017 forthcoming). 'The Importance of Context and Cognitive Agency in Developing Police Knowledge: Going Beyond the Police Science Discourse.' *The Police Journal: Theory, Practice and Principles*, (Sage Journals).

Wydra, C. (2015), 'Educating the Technology Officer of the Future: A Needs Analysis.' *Issues in Information Systems*, **16**(4): 224-231.

Yong, A.G., Pearce, S. (2013). 'A Beginner's Guide to Factor Analysis: Focusing on Exploratory Factor Analysis.' *Tutorials in Quantitative Methods for Psychology*, **9** (2). Available from:

< http://www.tqmp.org/Content/vol09-2/p079/p079.pdf> [Accessed 1st May 2017].

---

[1] The seven areas are: 'Format was appropriate for training delivered'; 'Satisfaction with what was learnt from training'; 'Training received was relevant to job role'; 'Will use any knowledge gained in job role'; 'Knowledge has increased as a result of training'; 'Skills have increased/improved as result of training' and 'Job performance has improved as a result of training'.

[2] Effect size, d=M (mean)/SD (Standard Deviation). According to Cohen's d (Cohen, 1998), 0.8 means a large effect.

[3] 0.7 means medium effect.

[4] Large effect

[5] Large effect

[6] http://www.college.police.uk/What-we-do/Development/professional-development-programme/Pages/CPD---what.aspx

Table 1 Factor loadings after rotation (Online)

Rotated Component Matrix[a]

	Component	
	1	2
Format was appropriate for training delivered	**.901**	.109
Satisfaction with what was learnt	**.887**	.164
Training received was relevant to job role	.228	**.739**
Will use any knowledge gained in job role	.091	**.951**
Knowledge has increased as a result of training	.692	.443
Skills have increased/improved as result of training	**.758**	.433
Job performance has improved as a result of training	.446	**.756**

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 3 iterations.

Table 2 Factor loadings after rotation (Face to face)

Component Matrix[a]

	Component 1
Format was appropriate for training delivered	.696
Satisfaction with what was learnt	.851
Training was relevant to job role	.835
Will use any knowledge gained in job role	.785
Knowledge has increased as a result of training	.879
Skills have increased/improved as result of training	.876
Job performance has improved as a result of training	.835

Extraction Method: Principal Component Analysis.

a.1 components extracted.

Table 3 Factor loadings after rotation (Workshop)

Component Matrix[a]

	Component 1
Format was appropriate for training delivered	.997
Satisfaction with what was learnt	.997
Training was relevant to job role	.997
Will use any knowledge gained in job role	.954
Knowledge has increased as a result of training	.997
Skills have increased/improved as result of training	.954
Job performance has improved as a result of training	.954

Extraction Method: Principal Component Analysis.

a 1 components extracted.

Figure 1 Percentages of overall score of 7 areas in Online training

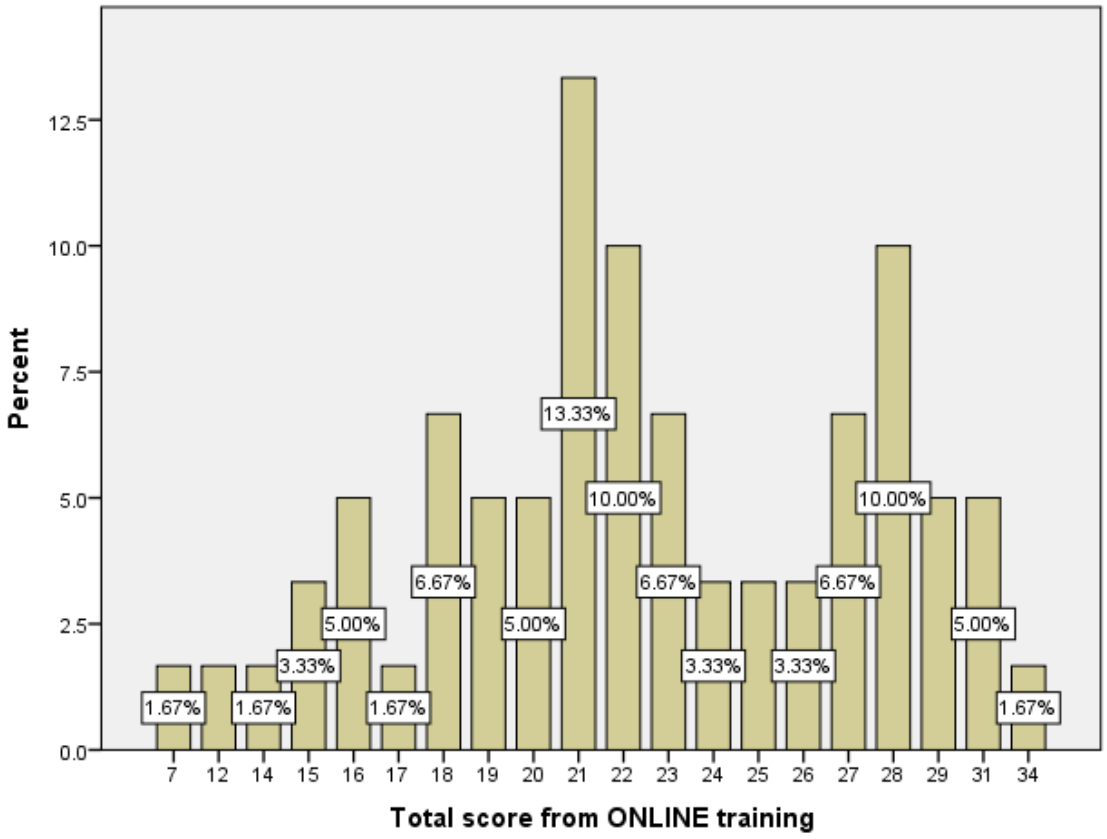

Figure 2 Percentages of overall score of 7 areas in Face to Face training

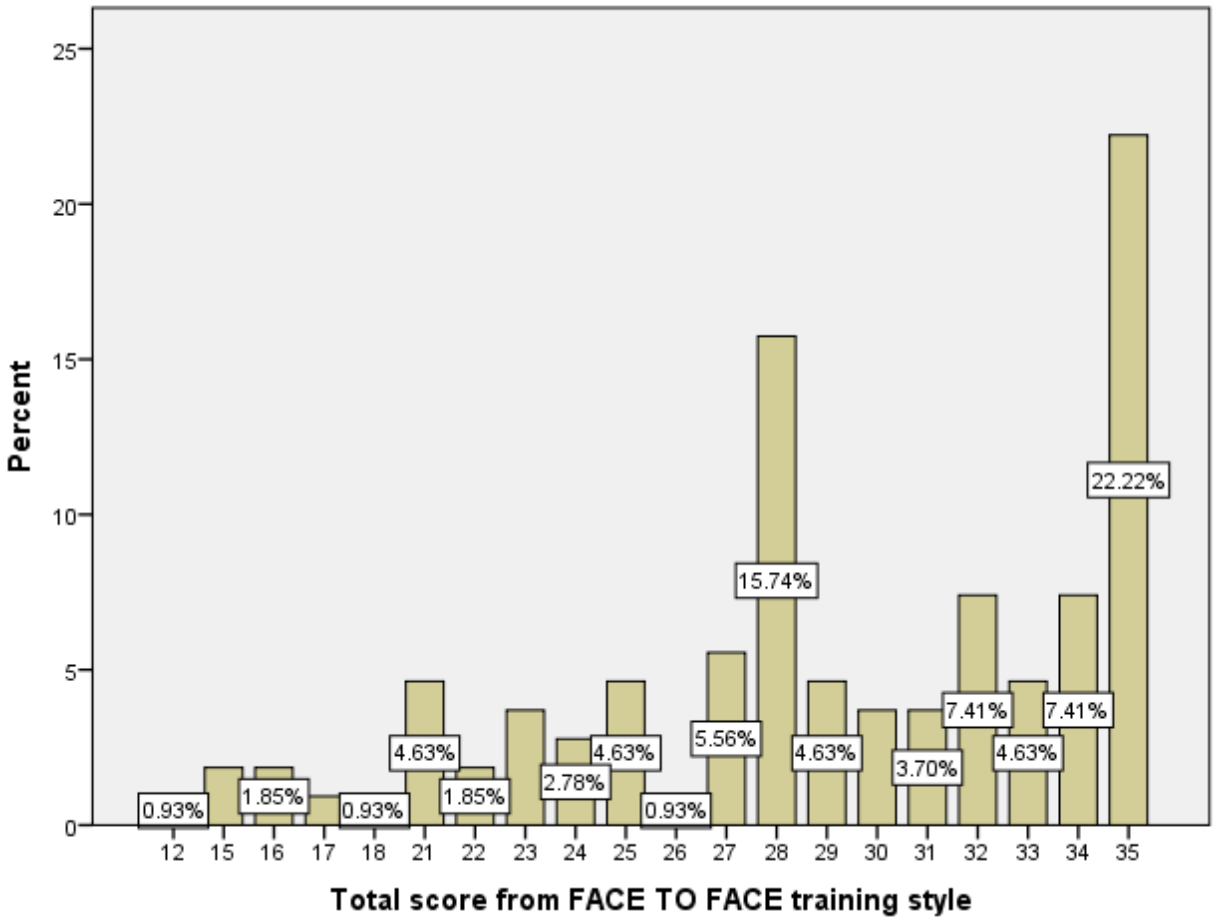

Figure 3 Percentages of overall score in Workshop training style