CARI Project

Police Cybercrime Training: Perceptions, Pedagogy and Policy

Tom Cockcroft, Pip Trevorrow, Mohammad Shan-A-Khuda, and Z. Cliffe Schreuders

The Cybercrime and Security Innovation (CSI) Centre
Leeds Beckett University

2018

This is a *pre-print*, in the process of undergoing academic publication.

The CARI Project

The CARI Project is a large-scale collaboration between West Yorkshire Police and the Cybercrime and Security Innovation Centre (CSI Centre) at Leeds Beckett University. The CARI Project aims to improve and incorporate an evidence-based approach into the policing of digital forensics and cybercrime investigations. An extensive needs assessment of UK policing and cybercrime and digital evidence was conducted to understand the current situation, and to identify needs across the force. The CARI Project also involved implementing a training and research programme that has impacted the capability of the digital forensics and cyber units within West Yorkshire Police to engage in research. This needs assessment and research training led to the development of a set of research proposals, which were scored and selected. Subsequently, academics and police staff co-produced 9 research and development workstreams: a framework for seizure, preservation and preservation of cloud evidence; automated forensic analysis; image linkage for victim identification and framework for image fingerprint management; automated grooming detection; frontline officer awareness development and decision support mobile app; assessment of methods of cyber training; an evaluation of the role of the Digital Media Investigator within WYP; and characteristics of victims of cybercrime. Each of these projects were designed to address needs within law enforcement and outputs include evidence-based procedures, new capabilities such as software/algorithms, and actionable intelligence.

This work was supported by a Police Knowledge Fund grant, administered by the Home Office, College of Policing, and the Higher Education Funding Council for England (HEFCE).

LEEDS BECKETT UNIVERSITY

WEST YORKSHIRE POLICE

Abstract

Cybercrime has become one of the most pressing developments for police organisations to engage with over recent years. One of the key challenges 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 the CARI Project, a major study into the effectiveness of cybercrime investigation within a large UK police force funded by the Police Knowledge Fund[1]. As part of the needs assessment for the above project, concerns were raised about the effectiveness of existing training arrangements in facilitating the development of cyber skills within police officers. The present research, based on survey data, sought to explore the effectiveness of different training styles as perceived by those who had undertaken cyber training. The research found that officers perceived some modes of training as considerably more effective than others and highlighted some of the organisational contexts that impact negatively on the delivery of effective cyber training to police officers. Analysis of survey responses indicated that whilst eLearning is perceived as having some utility, such as in delivering refresher training, it is not perceived as effective as other forms of learning delivery. The findings are presented within a context, informed by existing literature, that acknowledges wider debates surrounding the pedagogy of police learning and the organisational challenges of developing cyber skills within police officers.The authors believe that the findings will have relevance to police training policy both in the UK and in the wider international context.

[1] The CARI Project was supported by a grant from the Police Knowledge Fund, which was administered by the College of Policing, Higher Education Funding Council for England (HEFCE), and the Home Office.

Introduction

Cybercrime is a growing and global phenomenon, which police need to be trained to respond to, and refers to incidences where a computer is used in the commision of a crime or as a target of crime. The UK Home Office (2013) categorises cybercrime into cyber-dependent crime (or 'pure cybercrime'), forms of crime that only exist digitally, and cyber-enabled crime, crimes that can be conducted with or without digital devices, but that are carried out with digital devices. The substantial growth in prevalence of cybercrime 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. 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. Police cybercrime education and training issues remain an area of interest to police leaders, think tanks, policy-makers and academics (e.g. PA Consulting Group, 2015, HMIC, 2015, Cummins-Flory, 2016, and Reform, 2017). At the same time, the UK Government openly acknowledges the role played by businesses, individuals and, indeed, the market in ensuring that the security risks posed by cyber crime are minimised (HM Government, 2016). In doing so, they rightly identify the complexity of the cyber crime problem and the role played by a variety of actors in any crime prevention strategy. Despite this, however, as with any crime related phenomena, the pressure brought to bear upon the police to respond effectively is substantial.

This work was motivated by a wide-scale needs assessment conducted within one of the largest forces in England and Wales, involving focus groups and interviews with police staff

and strategic leads across key units and roles. The most prevalent theme of need across the entire needs assessment study was the issue of training and knowledge. Results indicated that there was reason to assess the value in alternative training methods as many of the police officers interviewed suggested that online eLearning may may not be particularly effective (Schreuders *et al.*, 2017).

The aim of this study, therefore, was to assess the perceived effectiveness of different styles of cyber training within the police force. A questionnaire was delivered to police officers who had undertaken cyber training in a regional police force over a 30 month period. The results, the authors believe, 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). These discussions cover a wide range of topics ranging from those relating to the level of learning and the nature of institutional learning providers (for example, the impact of Higher Education [see Mosaliuk and Cress, 2013]) to the appropriate pedagogic approach with which to underpin learning delivery (e.g. Griffith, 2015). At a wider level, there are moves towards developing a more rigorous evidence base for knowledge in policing (see Sherman, 1998, Fleming and Wingrove 2017) and this will further impact on the direction of content and delivery of police education as the tension between evidential and experiential bases of police occupational knowledge is explored further. And, despite the ongoing increase in published academic work on the subject of police training and education, Mastrofski (2007) notes that our knowledge base remains underdeveloped in a number of

areas. For the purpose of this section, two such areas can be identified: *How police officers learn* and *Cyber knowledge and the police organisation*.

How Police Officers Learn

One aspect of the literature which has helped us to develop our understanding of police training is that which addresses, simply, how police officers learn. Police learning has traditionally been premised upon notions of "*acquisition* and *transfer*" (Heslop, 2011, p. 327 italics in original) and this perspective has become viewed as the standard 'paradigm' underpinning police training. Heslop (2011) notes, however, that, increasingly, pedagogic research is drawing on different ideas of " 'participation' and 'becoming' " (Heslop, 2011, p. 327) as a means of explaining how knowledge is developed. Accordingly, he argues that learning is simultaneously an individual and a participatory process and, as a result, proposes that learning is also linked to the process whereby individuals 'become' police officers. In doing so, he draws on Chan's (1997) depiction of field (the structural arrangements of policing) and habitus (cultural knowledge of policework). Crucially, the process of police learning, Hislop suggests, is dependant upon a reciprocal relationship with habitus and changes to either variable have potential to impact on the other. The idea of learning as acquisition has largely been discredited, despite its continuing popularity in police training. The opposing participatory paradigm of learning sees knowledge as being generated through participation in practices, in this case, within the organisational and cultural milieu. Whilst neither approach is without problems, there is a case, argues Heslop, to look towards a holistic integration of these two paradigms. In conclusion, Heslop notes that learning is situated socially and culturally and not just in terms of individual processes of knowledge acquisition. The implications of such ideas are that traditional forms of training (based on

knowledge acquisition) might have a limited positive impact on learning and that, conversely, participatory learning may be more effective.

Heslop's work parallels that of Chan, Devery and Doran (2003), not least in its application of 'field' and 'habitus' to the organisational context of police learning. Both pieces of work show a distinction between different stages of initial police training with initial training packages more likely to be based on social context and community awareness and later packages on the core 'apprenticeship arrangement' (p. 304). Of interest here, as Chan et al identify, is that the latter sits somewhat uncomfortably with the ongoing professionalisation agendas that are implicitly contained within the former. In respect of which approach was perceived as more effective by recruits, Chan et al tellingly note that recruits "distinguish between the theoretical knowledge taught in the academy and what they regarded as 'real' knowledge" (2003, p. 304).

However, integral to many explanations that draw on identity and the notion of what it means to be a police officer is that the context pertains to initial police training and the increasingly potent professionalisation agenda. The issue of cyber training presents some challenges in this regard, most notably around the extent to which it is considered a core or non-core element of the police role. As a relatively new phenomenon, knowledge around cybercrime enjoys a somewhat ambiguous status within policing. Whilst ostensibly a specialist knowledge, HMIC (2015) made it very clear that they considered that knowledge of digital crime should no longer be the preserve of specialist squads but be integrated fully within public facing police roles.

Cyber Knowledge and the Police Organisation

Loveday (2017) suggests that fraud and cybercrime represent one of the most substantial threats to security in England and Wales. However, what information we have, globally, regarding police capacity to effectively deal with this threat is limited but generally points to substantial challenges in delivering an appropriate response. One of the biggest factors, in this respect, concerns the level of cyber knowledge within the organisation and the positioning of such knowledge in respect of particular police roles.

Some of this knowledge has been generated through studying the relationship between training and quality of police investigations. For example, Marcum et al (2010) noted that, in the context of investigations focusing on policing possession of child pornography, high quality training alone would not improve the quality and success of investigations. Successful investigations, they suggested, also depended upon appropriately skilled and motivated personnel being available. Existing literature also focuses on the orientation of non-specialist patrol officers to cybercrimes. The work of Holt and Bossler (2012) examined the factors that predicted patrol officer engagement with cybercrime training and investigation in two South Eastern U.S. cities. They highlighted 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 deal with such instances. 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 effective patrol officer engagement with cybercrime situations. 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. Overall, a broad range of evidence therefore points to the need for patrol officers to become more effective first responders to cybercrime calls as existing evidence illustrates that some patrol officers are insufficiently prepared or interested in embedding cyber skills within their everyday role.

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. Such an approach to recruitment would presumably impact upon the effectiveness of 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. On this point, Monett and Elkina (2015) warn that eLearning delivery risks becoming viewed as a means of producing cut price

training, adding that it is imperative that such methods that be underpinned by technological and pedagogic expertise.

Reporting on the police cyber training provision available in the US state of Indiana, Cummins-Flory (2016) identifies that, within that jurisdiction, digital crime is not covered within any initial or in-service training. Police officers who wish to train in digital investigation have to do so through attending courses provided by an external provider (such as an HEI). Whilst lack of funding explains some of this lack of provision, according to Cummins-Flory, the need for cyber skills is such that initial police training should include a course on digital evidence and more advanced training should be made available for appropriate officers.

Similar issues have been identified within the UK as crimes with cyber elements become increasingly prevalent and this points to evidence of systematic shortfalls globally. This has been a result of, according to Wall and Williams (2013), both the rise in professional and organised criminals who undertake attacks on systems and the people that use them and the 'hyper-connectivity' (p. 410) that has facilitated a substantial increase in more mundane cyber offences. However, within the UK context, what limited commentary exists has suggested that there remain some substantial discussions to be had regarding the strategic response to this threat. The first of these pertains to the issue of whether cyber skills should be viewed as specialist or non specialist skills within the policing context. Substantial opinion points to the need for cyber skills to be viewed as non specialist and integral to the roles of police and civilian workers alike, a set of skills articulated by PA Consulting Group (2015, p. 16) as 'general digital awareness'. The position was further clarified through HMIC (2015, p. 30) when it declared, "We recognise, however, that bringing the handling of digital crimes

within the general skillset of every police officer and member of police staff means that it is essential that they, in turn, have the necessary understanding of the technology". The second key area of discussion relates to training provision and effectiveness. Whilst, some arguments, such as those forwarded by Reform (2017), have suggested that future responsibility for training cyber provision might fall between Higher Education providers and a mooted Home Office digital academy, more immediate questions surround the effectiveness of existing provision. The review conducted by HMIC (2015) into digital crime and police response highlighted the effectiveness of existing provision for non specialist staff, which included an online programme and a classroom based course for first responders. And despite the fact that eLearning packages were seen as effective when engaged in as a group exercise, their effectiveness was compromised through being undertaken on low quality PCs. Furthermore, the reduction of training days within the organisation meant that there was often insufficient time to complete the packages in a meaningful way. Instead, time pressures led to a 'tick box' approach focussing on completion of the package rather than engaging with the contents. Obviously, cyber training has emerged as a considerable strategic and operational issue, raising substantial concerns around the ability of police organisations to provide training and, when it is provided, the extent to which it allows for the development of appropriate skills and competencies within those members of the organisation who require them.

Despite the limited information in this area, it is possible to identify five key themes in the above literature which pertain to the effectiveness of training in respect of police cyber skills and knowledge. These are the a) *Tension between Evidenced Knowledge and Experiential Knowledge*; b) *Quality*; c) *Resources*; d) *Positioning of Knowledge within the Organisation*; and e) *eLearning*. These themes also relate to the broader conceptual advances surrounding

police knowledge and learning. For example, the tension between 'evidenced' and 'evidential' knowledge is central to the debate surrounding 'Evidence-Based Policing' in which academic and professional opinion has divided along the lines of what criteria define appropriate evidence and knowledge in the police occupation (see Fleming and Rhodes, 2016). The application of this to the area of cyber crime training raises important questions about the roles that evidence and experience might play in facilitating the development of appropriate cyber knowledge and skills within police officers. The linked themes of quality, resources and positioning of knowledge within the organisation all appear to link to the concept of 'field'. If the field represents the structural context of policing, such themes suggest that the concept of cybercrime knowledge is not fully being integrated at that level. This would then account for the fact that such knowledge does not appear to be fully incorporated within the habitus of officers. Whilst this knowledge fails to be unambiguously incorporated into the wider field of policing, the habitus, or cultural knowledge of officers, will fail to afford it particular prominence. If cyber knowledge remains the domain of police specialists the wider field and the habitus of non specialist officers will accordingly fail to recognise its importance. The work of Rowe and Garland (2013) demonstrates (with reference to police diversity training) how such cultural and structural barriers need to be overcome for training to be fully effective. If an area of police knowledge is seen as a passing fashion or fad, it will not be engaged with regardless of the mode of content delivery. Finally, the issue of online learning draws us back to Heslop's useful distinction between knowledge as acquisition and knowledge as participation. In an era where attempts to impart new knowledge often use remote and electronic means (derived from acquisitional models of police learning) our ability to effectively satisfy the participatory needs of the learner may be limited.

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 exploring police officers' experiences of cybercrime training. 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 (Buckingham and Saunders, 2004) and thematic (Braun and Clark, 2006) analysis. The choice of research method was driven by a number of factors. As May (2011) highlights, questionnaire research allows researchers to minimise bias within a research project and, correspondingly, to create a research strategy that is replicable by others. Similarly, Francis (2000) identifies how the method also satisfies requirements of 'feasibility, practicability and validity' (p. 42). In respect of the second benefit outlined by Francis, the method allowed for the most logistically viable option of gathering data from a substantial number of respondents. Furthermore, the use of questionnaires has proved to be a popular research method for research attempting to elicit the views of police officers, as it affords participants a degree of anonymity which, it is hoped, will generate more accurate responses.

A questionnaire was designed to evaluate police perceptions of modes of training. 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 levels were addressed via the survey and were broken down into questions addressing aspects of these levels. The level of 'Results' was not incorporated as it focuses on the impact on the organisation with regard to a change in behaviour, and was beyond the scope of the research.

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. ‘Transfer’ explored the extent to which participants perceived that their learning had led to changes in behaviour. 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 questionnaire was circulated, by the police force, to approximately 600 police officers and staff, 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 descriptive statistics, such as frequency analysis, to explore the basic features of the data. Inferential statistics were used to test the relationships between variables by conducting exploratory factor analysis, cluster analysis and t-tests. The quantitative analysis addressed the following two research questions:

i. What are the characteristics and differences between training styles, in terms of the Format, Satisfaction, Relevancy, Useful of knowledge, Increase of knowledge, and Increase of skills and Increase of job performance?

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

The qualitative data generated through the free text option of the survey was analysed using a manual thematic analysis, and aimed to explore police perceptions of the effectiveness and appropriateness of approaches to training (Braun and Clark, 2006).

Findings

Quantitative Findings from the Questionnaire

The cyber training style of 'Q&A' within the questionnaire was completed by only 4 respondents which is too small for any statistical significance testing, hence was removed from the quantitative analysis of the results. The statistical analysis therefore focuses on comparing Online, Face-to-Face and Workshop styles of cyber training.

Cronbach's alpha was used to measure the internal consistency (reliability) of the scale made up of the seven items in each training style. Results from all three training styles were found to have high reliability across the seven items: Online, Face to Face and Workshop with Cronbach's $\alpha = .882, .918, .989$ respectively. These results enable us to use the seven items to calculate and compare overall scores for each training style. Furthermore, a high value of Cronbach's α in each training style does not indicate one-dimensionality (Grayson, 2004). Therefore in the following sections, we apply factor analysis to test for underlying dimensionality in the data (Field, 2013), and test for significant differences between factors.

Online cyber training style

Principal component factor analysis was conducted on the seven items for Online cyber training 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 make up *Component 1* and Relevancy to job role, Usefulness of knowledge, Increase of Job Performance relate to *Component 2*. Conceptual meaning of these 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 for Face to face after rotation. All the seven items of perceived effectiveness do not indicate any dimensionality of Face to Face cyber training;

that is, there was no structure detected in the relationships between seven items making up the overall score.

[INSERT TABLE 2]

Workshop cyber training style

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

[INSERT TABLE 3]

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

Perceived preferences for training styles

The preferences for training styles is explored in three ways. Firstly, a comparison is made *within* the seven items of each training style, to understand the perceived strengths and weaknesses of each training style. Secondly, a comparison is made *between* each of the training styles for each of the seven items, to test whether training styles have an effect on each level. Finally, a comparison is made *between* the overall score made up of the seven items for each participant in each training style.

Differences *within* the seven items of each training style

A 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. The results from this analysis is presented in the sections below.

Online

Results from the t-test suggest that participants of Online training have scored the relevancy of the training higher than the appropriateness of the format. Participants scored considerably lower 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 scored the appropriateness of the format higher than the resulting improvement in job performance. Participants scored 'format was appropriate for training delivered' considerably higher (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

A 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 in the sections below.

Comparison between Online and Face to Face styles

Results from the t-test showed that overall participants' perception between Online and Face to Face training style differed 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.

Comparison between Online and Workshop styles

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.

Comparison between Face to Face and Workshop styles

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 *between* approaches

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

[INSERT 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 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 for Workshop (n=8), no comparison has been conducted between Online and Workshop and Face to Face and Workshop.

Qualitative findings from the questionnaire

In this Section we present findings from the thematic analysis of the free text qualitative data generated by the questionnaire.

The quantitative survey findings draw attention to the marked difference in perceptions of online and face to face training. This section provides a commentary based on the qualitative data drawn from the surveys.

What did you like about the online training?

In response to this question, 43 positive responses (33.5% of sample) were recorded which were categorised under the thematic headings of 'Flexible Learning' (58.13%), 'Ease of

Understanding' (16.27%), 'Format' (11.62%), 'Quality of Information' (9.30%), and 'Reference Tool' (4.65%). 'Flexible Learning' represents the views of a majority of respondents who answered positively to this question. In particular, respondents cited the importance of this mode of delivery in ensuring that training could be conveniently accessed and that learning could take place at the trainee's preferred time and their preferred pace and therefore fit in more easily with their operational duties. The 'Ease of Understanding' category was used to cover those responses which suggested this mode of delivery allowed for material to be presented in an easily understandable format. Respondents suggested that the training provided in this format was, relevant and concise. Under 'Format' respondents suggested that the structure of the learning packages was helpful, for example in respect of their interactive nature. A small number of respondents referred to the 'Quality of Information' contained in the packages and the way in which it was helpful in providing basic information to help with the acquisition of new knowledge. Finally, a very small number of respondents drew attention to the fact that the online learning could be returned to, post-training, and used as a reference tool.

Under this question, seven negative responses were also recorded and five of these did not refer to specific issues. However, those that did referred to the perception that online packages did not facilitate the retention of new knowledge, were impersonal and suitable only for refresher training or shorter basic introductions to areas. One respondent suggested that, in respect of cybercrime, online packages might work better in conjunction with traditional training techniques.

What did you NOT like about the online training?

In response to this question, 64 responses (50% of sample) were recorded which were

categorised under the thematic headings of ‘Superficiality of Learning’ (28.31%), ‘Questions’ (28.12%), ‘Complexity’ (15.62%), ‘Lack of Interaction/Lack of Feedback’ (14.06%), ‘Environment’ (7.81%), ‘General’ (6.25%), ‘Positive’ (4.68%) and ‘Miscellaneous’ (3.12%)’. Over a quarter of respondents raised the issue of ‘Questions’; that is, the lack of ability, when using online learning packages, to ask questions. This was seen as the most substantial weakness, as the ability to ask questions was seen as a very important means of clarifying complex issues and concepts. This ties in closely with the allied category of ‘Lack of Interaction/Lack of Feedback’ that encapsulates those views that articulate a preference for more interactive modes of learning. Under this category responses highlighted the impersonal nature of online learning packages, the lack of opportunity for explanation/clarification and the lack of opportunity to share experiences with other attendees. A substantial proportion of respondents drew attention to issues around the ‘Superficiality of Learning’. This refers to responses that suggest online training does not lead to a thorough understanding of knowledge or to retention of knowledge. Those responding under this category also suggested that this mode of learning was not sufficiently an active learning process and that there was little chance to consolidate knowledge. Overall, two distinct sets of experience seemed to emerge. First, that for those with little experience in cyber matters the training could be ‘boring’, ‘lengthy’ and ‘complicated’. Second, one respondent articulated the problem of using online training with more experienced learners. They suggested;

> “By its nature online training has to be very linear and by default operates in a black and white universe. Unfortunately police investigation is the very opposite of this, neither linear or black and white with simple decisions quickly spiralling into a complex spaghetti of consequences and the opening up of future options. This is impossible to convey in an online training environment and therefore I find it doesn't

work with police investigation training as it is too simplistic."

The issue of 'Environment' was also raised by five respondents. The majority of these responses suggested that learning was compromised by the fact that online learning usually took place in one's normal place of work. This meant that respondents were likely to be pulled away from training packages and asked to undertake work tasks, leading to a fragmented learning experience which impacted poorly on focus, engagement and, ultimately, understanding.

What type of training do you believe ONLINE training is best suited for?

In response to this question, 62 responses (48.4% of sample) were recorded which were categorised under the thematic headings of 'Basic/Procedural/Legislation Training' (35.48%), 'Refresher' (14.51%), 'Cyber'(11.29%), 'Consolidation' (8.05. %), 'Miscellaneous'(6.45%), 'Don't Know' (6.45%), 'No Use' (6.45%), 'Face to Face Training' (4.83%), 'Any' (3.22%) and 'Advanced' (3.33%). 'Basic/Procedural/Legislation Training' was used to categorise responses that drew attention to the potential for online training to be used effectively in respect of certain forms of content/subject. A large majority of these responses advocated online training as a way of delivering content of a basic or introductory nature. Two responses suggested that it was appropriate for delivering training regarding legislation, whilst one other suggested it was appropriate for training in processes/procedure but not, however, those pertaining to cyber training. A significant number of responses drew attention to the fact that online training could be an effective means of delivering 'Refresher' as opposed to 'Initial' training. It was suggested by a number of respondents that online training could be used for pre course preparation to make the face to face element more streamlined.

What did you like about the face to face training?

In response to this question, 114 responses (89.0% of sample) were recorded which were categorised under the thematic headings of 'Clarification' (58.77%), 'Interaction' (13.15%), 'Knowledge/Skill of Trainers' (8.77%), 'Ease of Learning' (6.14%), 'Sharing of Experiences' (4.38%), 'Miscellaneous' (3.50%), 'Environment' (1.75%), 'Practice Methods' (0.87%), 'Practical Examples' (0.87%) and 'N/A' (0.87%). By far the largest group of responses were those pertaining to the issue of 'Clarification' whereby face to face training was seen as valuable because of the opportunities it gave for attendees to receive clarification over the concepts being taught as and when they required. Furthermore, 86.56% of these respondents (i.e. those whose responses pertained to 'Clarification') specifically mentioned the extent to which they considered the ability to ask questions as integral to their favouring of this mode of delivery. A separate but related category relates to responses that referred to 'Interaction'. This referred to responders' preference for modes of delivery that allowed for them to interact with other people, especially other learners. For example, one respondent referred to, "Interaction with a knowledgeable trainer and other students in checking comprehension, discussing examples, ideas, and sharing best practice in practise" whilst another noted that, "The interaction and the chance to ask questions and receive the experience from a trainer who has utilised what they are delivering in real life policing. Having face to face training allows for interaction regarding real life working scenarios etc". 'Knowledge/Skill of Trainers' was considered important by a number of respondents. Such responses draw attention to the impact of trainers who have specialised knowledge or whose communication skills facilitate engaging learning experiences. In particular, reference was made to the importance of trainers who could gauge the engagement/learning of individuals and group and deliver input at the appropriate level. A small number of respondents referred to the

'Ease of Learning' that they experienced under this mode of delivery. These responses tended to be subjective opinions regarding respondents' own preferred learning styles/formats. Five respondents made reference to issues which could be categorised as 'Sharing of Experiences' whereby the interactive nature of the format allowed for engagement between peers and which allowed for understanding of practical contexts to be enhanced.

What did you NOT like about the face to face training?

In response to this question, 108 responses (84.3% of sample) were recorded which were categorised under the thematic headings of 'Nothing/NA' (52.77%), 'Time to Travel/Participate' (11.11%), 'Mixed Ability of Learners' (8.33%), 'Too Long/Too Intense' (6.48%), 'Relevance to Role' (4.62%), 'Pace' (3.70%), 'Miscellaneous' (3.70%), 'Design ' (1.85%), 'Clarification' (1.85%), 'Environment' (1.85%), 'Brevity' (1.85%), 'Delivery' (0.92%) and 'Insufficient Practical Component' (0.92%). A majority of respondents stated that there were no elements of face to face training that they did not like. The largest substantive issue raised as a negative with this mode of training was 'Time to Travel/Participate'. A number of issues converged under this category and included concern over a protracted extraction from the workplace, the time taken to reach the training venue and the fact that the training lasted longer than online training. 'Mixed Ability of Learners' was also perceived as an issue by nine respondents. For these, the varied abilities of students meant that the flow of class content could be disrupted. One forwarded suggestion to resolve this was to stream people attending training sessions with a technological focus into those who were more or less confident with IT. A small number of respondents thought that classroom sessions were 'Too Long/Too Intense'. For some, a week long course on cyber was too difficult to fully engage with because of the use of technical language, the

complexity of the subject matter and the amount of information to be assimilated. For five respondents, there were concerns over the 'Relevance to Role' of the training that they engaged with in that they felt the training bore little relevance to their work. For the four respondents who had issue with the 'Pace' of the training half complained of the training being too fast and the other two complained that it was too slow.

What type of training do you believe FACE TO FACE training is best suited for?

In response to this question, 104 responses (81.2% of sample) were recorded which were categorised under the thematic headings of 'All' (25%), 'Complex' (21.15%), 'IT/Cyber' (19.23%), 'Practical' (15.38%), 'Most Training' (4.80%), 'Miscellaneous' (4.80%), 'Longer Sessions' (1.92%), 'Where Skills Deficits Occur' (1.92%), 'For Those with Existing IT Skills' (1.92%), 'Short Training' (0.96%), 'Systems Training' (0.96%), 'Continuing Development' (0.96%), 'New Topics' (0.96%) and 'Investigative' (0.96%). A quarter of respondents suggested that all training would benefit from being conducted through a face to face mode of delivery. One such respondent noted, "We do an important job and we should be given the time to learn the ever changing role". However, one respondent was a little more cautious by adding the caveat that whilst face to face training is preferred, there needs to be a cohort of the same, or similar, skill level. A substantial proportion of survey respondents suggested that face to face training works well with 'Complex' training or where the subject matter is in-depth. One reason given for this was the ability to raise queries whilst learning. A slightly smaller proportion of respondents suggested that face to face training is suited to the delivery of 'IT/Cyber' training. The rationale for such views was explained, largely, by the complexity of this form of training and as such does connect with the 'Complex' category. A significant number of respondents highlighted the view that face to face training works with

'Practical' subject matter. Five respondents were of the opinion that face to face training was the preferred mode of delivery for 'Most' training.

Discussion

Discussion of the quantitative findings

Characteristics of each training style

The two latent factors in Online training, *Component 1* and *Component 2*, 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.

Discussion of the qualitative findings

The findings, derived from the qualitative data elicited by the survey, provide scope for discussion in the context of both the research questions and the literature presented in the literature review. The qualitative findings provide insight into the quantitative component of the survey, which identified a pronounced difference in respondents' perception of the

effectiveness of styles of learning delivery with Face to Face delivery being viewed significantly more positively than Online learning. The qualitative data identified some of the positively perceived factors with this form of delivery and which may have motivated these responses. The most commonly cited factors were categorised as 'Clarification', 'Interaction', 'Knowledge/Skill of Trainers', 'Ease of Learning' and 'Sharing of Experiences'. Conversely, Online learning was viewed negatively, with the most commonly cited factors being identified under 'Superficiality of Learning', 'Questions', 'Complexity', 'Lack of Interaction/Lack of Feedback' and 'Environment'.

The literature review highlighted a number of important themes around the effective delivery of cyber training and which will be used, in this section, to contextualise the findings of the research. These are *Evidenced Knowledge* and *Experiential Knowledge*; *Quality*; *Resources*; *Positioning of Knowledge within the Organisation*; and *Online Learning*. The first relates to the theme of how police officers learn and the following four to the way in which cyber knowledge is organised, structured and delivered within police organisations.

The first theme, that of the tension between 'Evidenced Knowledge and Experiential Knowledge' does bare some exploration in light of the results. The findings do appear to provide possible support for Heslop's assertion that learning is (or, at least, was viewed by some of this project's participants) as an active social and cultural process. Whilst officers saw some benefits to online learning packages these were viewed, at best, as only a partial solution to the delivery of effective police cyber learning and officers criticised this mode of delivery for its superficiality and its lack of an interactive element. In particular, officers viewed the need for an interactive element as a result of the nature of police work. The complexities of police work therefore, it can be argued, demand strategies for learning

delivery that go beyond what Heslop viewed as the standard paradigm which, in this context, might be most closely associated with eLearning packages. This is especially true given the evolving nature of opportunities and threats in this domain in which, according to Wall and Williams (2013), new developments have signified significant transformations of the level of threat posed to police organisations. Whilst eLearning packages undoubtedly offer scope for efficiencies, it should be argued that police investigatory training in a context as fluid and dynamic as cyber crime demands recognition that some learning takes place against a context of evolving human interaction (with systems, individuals and legislation) that requires a more interactive approach to learning. For officers to appreciate and recognise this, any police cyber learning strategy requires some element that supports interaction and which recognises the field within which policing occurs. Crucially, what is being suggested is that neither approach be favoured over the other but that we seek, as Heslop suggests, to integrate both approaches into future cyber learning strategies. In doing so, it might be hoped that we can bridge the divide between what Chan et al perceived as 'theoretical' and 'real' knowledge whilst utilising the efficiencies that eLearning packages offer.

Measuring the 'Quality' of police cyber learning is an intrinsically difficult task. To do so in a meaningful and objective manner would require a greater array of data than that which fell within the scope of this study. Furthermore, an accurate measure of the quality of such learning would require some understanding of a threshold level of knowledge which constitutes, in the words of HMIC (2015, p. 30), a "necessary understanding of the technology". Understandably, it is difficult to suggest what is, and what is not, an appropriate level given the lack of clarity, thus far, on what level of knowledge should reside in which parts of the organisation. Notwithstanding such caveats, it is possible to infer some general judgements on the quality of training as perceived by the respondents. Overall, respondents

appeared to believe that their perceived needs were more likely to be met by face to face as opposed to online training. These respondents tended to attribute such positive experiences to the opportunity to seek clarity over particular issues. However, other indicators of their positive experiences were elements of interaction, the skill of the trainers and the sharing of experiences between participants. Such factors highlight the perceived importance, to respondents, of the participatory elements of the learning environment and, in doing so, appear to support the work of Heslop who advocates greater recognition of the need for participatory approaches to police learning.

Any discussion of 'Resources' in respect of cyber knowledge inevitably entails a recognition of the previously discussed issue of 'Quality'. Whilst it would be wrong to suggest that the relationship between the two is linear and simplistic, with substantial resources unproblematically leading to substantial levels of quality, it is important to recognise that the austerity agenda has created challenges in delivering quality at all levels of policing. One of the key challenges is that the generic role of the police officer is defined against increasingly wider terms of reference (Millie, 2014) and cyber policing is a substantial element of this. Part of the challenge for the police organisation is undoubtedly that new forms of social behaviour demand new forms of police response, and such widening of roles leads to impacts on front line officers. At the same time, however, these changes lead to practical stresses in respect of organisational capacity in delivering learning and training. In the present research, where negative perceptions were identified in relation to face to face training these were largely due, not so much to the method of delivery itself, but the delivery context and included factors such as the time to travel to, and participate in, the learning and the impact of mixed ability classes. Such findings mirror those of HMIC (2015) where resource issues (be they, for example, hardware limitations or the reduction in number of staff training days)

impact on the effective engagement with the course content regardless of the effectiveness of the learning approach utilised. The recommendations forwarded by Reform (2017) provide a vision of what development is required to create a police force more effectively positioned to deal with the cyber crime issue. What remains unclear, in the post-austerity policing landscape, is the resource available for such infrastructure projects.

The issue of 'Positioning of Knowledge within the Organisation' remains one of substantial strategic significance and one that has attracted commentary from both US and UK commentators (Holt and Bossler 2012, PA Consulting Group, 2015, HMIC, 2015 and Cummins-Flory, 2016). In essence, it refers to whether or not cyber skills should be siloed within specialist groups within police organisations or should represent *core* skills. It is interesting to note that some respondents in the present study criticised the training they received for lacking relevance to their role. The responses suggest two causes: that a mainstream training package may not be best suited to the variety of roles within the force, and that the principle of 'general digital awareness' (PA Consulting Group, 2015, p.16) as a common skill set for all public facing police employees has yet to resonate fully throughout police organisations. Chan et al's use of the concept of 'field' (the structural context of policing) may help us to understand this issue more fully. Resistance to the incorporation of cyber elements into the police officer's role may be explained by the concept of cybercrime not fully being integrated into the 'field' of policework. This would then account for the fact that cyber knowledge (and a will to engage with it) does not appear to be embedded within the police 'habitus'. Whilst such knowledge fails to be unambiguously incorporated into the field of policing, the habitus or cultural knowledge of officers, fails to deem it important. If cyber knowledge remains the domain of police specialists the wider field and the habitus of non specialist officers will continue to fail to recognise its importance. The work of Rowe

and Garland (2013) into the problematic implementation of community and race relations training in the wake of the Macpherson report (1999) is instrumental in demonstrating how cultural and structural barriers need to be removed for effective learning of new skills to take place. Their work suggested that low quality training, a lack of focus on the intended outputs of the training and a failure to understand the relationship between training and work-based practices reflect a lack of strategic implementation. Furthermore, such oversights do little to persuade officers to engage meaningfully with programmes that seek to change how officers engage with new concepts and skills.

'Online learning' provides both opportunities and challenges for the delivery of cyber skills and expertise in police organisations. There remain concerns about it being used as a low cost and expedient means of cyber training (Monett and Elkina, 2015) and these concerns are echoed by HMIC (2015) who found that a lack of suitable equipment undermined this method's effectiveness. Somewhat ironically, the same research found that online cyber packages tended to work most effectively when used as a 'group training tool' (HMIC, 2015, p.32). The present research found that the flexibility of the format was perhaps its most favoured characteristic and that respondents also thought it appropriate for basic or refresher training. This does tend to suggest that eLearning training needs to be utilised *strategically* rather than as a default mode of learning delivery. Three initial reasons for this can be forwarded. First, that online learning is typically based on learning as 'acquisition' rather than learning as 'participation' (see Heslop, 2011) and therefore may have limited impact on the learner. Second, there remains the concern that the use of eLearning is driven by a wish to reduce the costs associated with learning delivery, rather than by an appreciation of this style of learning's pedagogic qualities. Third, and finally, the way in which online training has been presented to police staff has encouraged a mindset that focuses on completing the

training rather than engaging with the knowledge. Without the participatory context that is viewed as crucial to much police learning there remains little scope for "generic digital awareness" (PA Consulting Group, 2015, p. 16) becoming viewed as a core policing knowledge and therefore become embedded in the field of policing or the habitus of the police officer.

In the light of the above discussion it might be possible to propose two recommendations, based on the findings of the research, to inform the future development of cyber training in police organisations. First, significant consideration needs to be given to the substantial benefits associated with incorporating an element of participatory group learning into the delivery of police cyber learning. Evidence suggests that this might encourage deeper understanding of cyber issues, allow officers to explore the application of their skills to a wide range of occupational scenarios and encourage officers to more readily appreciate the importance of cyber skills to the police role. Second, the role that eLearning plays needs to be re-considered in the light of some of the negativity with which it might be perceived by police officers. In particular, concerns that it does not encourage a in-depth level of knowledge acquisition suggests that it might more appropriately be used as a means of imparting pre-course knowledge or refresher training.

Conclusion

This project was undertaken as a result of recommendations generated from a large scale needs assessment undertaken in a large UK police force. It aimed to assess the experiences and perceptions of cybercrime training of staff through an online survey to elicit quantitative and qualitative data from 128 respondents. The survey sought to measure and investigate the characteristics and perceived effectiveness of different training styles, in terms of the following measures - Format, Satisfaction, Relevancy, Useful of Knowledge, Increase of Knowledge, Increase of Skills and Increase of Job Performance.

Whilst there is limited research in the area of cybercrime training in police organisations, two overriding themes were identified in existing literature. The first related to ongoing pedagogic debates surrounding how police knowledge is imparted to members of the occupational group and the tension between acquisitive and participatory modes of police learning. The second was grounded in more practical organisational questions of where in the organisation cyber knowledge should be positioned and the most effective means of delivering it. Both themes proved helpful in contextualising the data generated. The findings contribute to the knowledge base of police cyber training, internationally, through identifying a distinct preference, amongst the participants, to participatory (rather than acquisitional) approaches to police learning of cyber knowledge. Furthermore, existing literature suggests that this may hold a further benefit in respect of breaking down cultural resistance to the incorporation of new forms of knowledge (in this case, cyber knowledge) into police roles. Similarly, whilst it is beyond the scope of this research to determine where such skills should structurally reside in police organisations, policy recommendations more generally are

identifying the need for a generic level of cyber knowledge to be distributed throughout all roles within the organisation. This policy, if adopted, will present some challenges for police training over the coming years. It is against the backdrop of such anticipated needs that the recommendations made in this paper stand. To recap, firstly, to consider those learning strategies that encourage participatory learning as a means of facilitating the development of meaningful knowledge and of legitimising new knowledge into frontline policing. Secondly, to limit the use of acquisitional learning as a standalone strategy and, instead, to encourage it as a means of supporting or augmenting that knowledge which is instilled through more participatory means.

References

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.

Chan, J.B. (1997). *Changing Police Culture: Policing in a Multicultural Society*. Cambridge University Press.

Chan, J., Devery, C., and Doran, S. (2003). *Fair Cop: Learning the Art of Policing*. Toronto: University of Toronto Press.

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

Cummins-Flory, T. A. (2016), Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies, *Journal of Digital Forensics, Security and Law*, **11**(1), pp. 7-38.

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.

Fleming, J. and Rhodes, R. (2016). 'Can experience be evidence?', *Paper to the Public Policy and Administration Specialist Group, Panel 2: Policy Design and Learning, PSA 66th Annual International Conference, 21-23 March 2016, Brighton.*

Fleming, J and Wingrove, J. (2017). *''*We Would If We Could...But Not Sure If We Can': Implementing Evidence-Based Practice*', Policing: A Journal of Policy and Practice,* 11(2), pp. 202-213.

Francis, P. (2000). 'Getting Criminological Research Started.' In Jupp, V.P., Davies, P. & Francis, P. (eds) *Doing Criminological Research*, London: Sage, pp. 29-53.

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).

HM Government (2016). *National Cyber Security Strategy 2016-2021*. London: HM Government.

HMIC (2015), *Real Lives, Real Crimes: A Study of Digital Crime and Policing*, London: HMIC.

Heslop, R. (2011) 'Community engagement and learning as 'becoming': findings from a study of British police recruit training' *Policing and Society* **21**(3): 327-342.

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.

Home Office (2013). *Cyber Crime: A Review of the Evidence*. London: Home Office.

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.

Loveday, B. (2017). 'Still plodding along? The police response to the changing profile of crime in England and Wales'. *International Journal of Police Science & Management*, ***19***(2), pp.101-109.

Macpherson, W. (1999). *The Stephen Lawrence inquiry: report of an inquiry by Sir William Macpherson of Cluny*. London: The Stationery Office.

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.

May, T. (2011). *Social Research: Issues, Methods and Process (4th edition)*, Maidenhead: Open University Press.

Millie, A. (2014). 'What are the police for? Re-thinking Policing Post-Austerity.' In Brown, J. (ed) *The Future of Policing*, Abingdon: Routledge, pp. 52-63.

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.

PA Consulting Group (2015), *Digital Investigation and Intelligence: Policing Capabilities for a Digital Age*. London: PA Consulting. (Accessed 09/03/18) http://www.npcc.police.uk/documents/reports/Digital%20Investigation%20and%20Intelligence%20Policing%20capabilities%20for%20a%20digital%20age%20April%202015.pdf

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

Reform (2017), *Bobbies on the Net: A Police Workforce for the Digital Age*, London: Reform (accessed 09/03/18) http://www.reform.uk/wp-content/uploads/2017/08/Bobbies-on-the-net.pdf

Rowe, M. and Garland, J. (2013). 'Police diversity training: A silver-bullet tarnished?' In M. Rowe, M (ed), *Policing beyond MacPherson – Issues in Police, Race and Society*, Collumpton: Willan, pp. 43-65.

Schreuders, Z.C., Cockcroft, T., Butterfield, E., Elliott, J., Soobhany, A.R., and Shan-A-Khuda, M. (2017). *Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force: Report - CARI Project*, Leeds: Leeds Beckett University Cybercrime and Security Innovation Centre

Sherman, L. (1998). *Evidence-based Policing: Ideas in American Policing.* Washington DC: Police Foundation.

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

Wall, D.S. and Williams, M.L. (2013). 'Policing cybercrime: networked and social media technologies and the challenges for policing'. *Policing and Society,* **23**(4): 409-412.

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

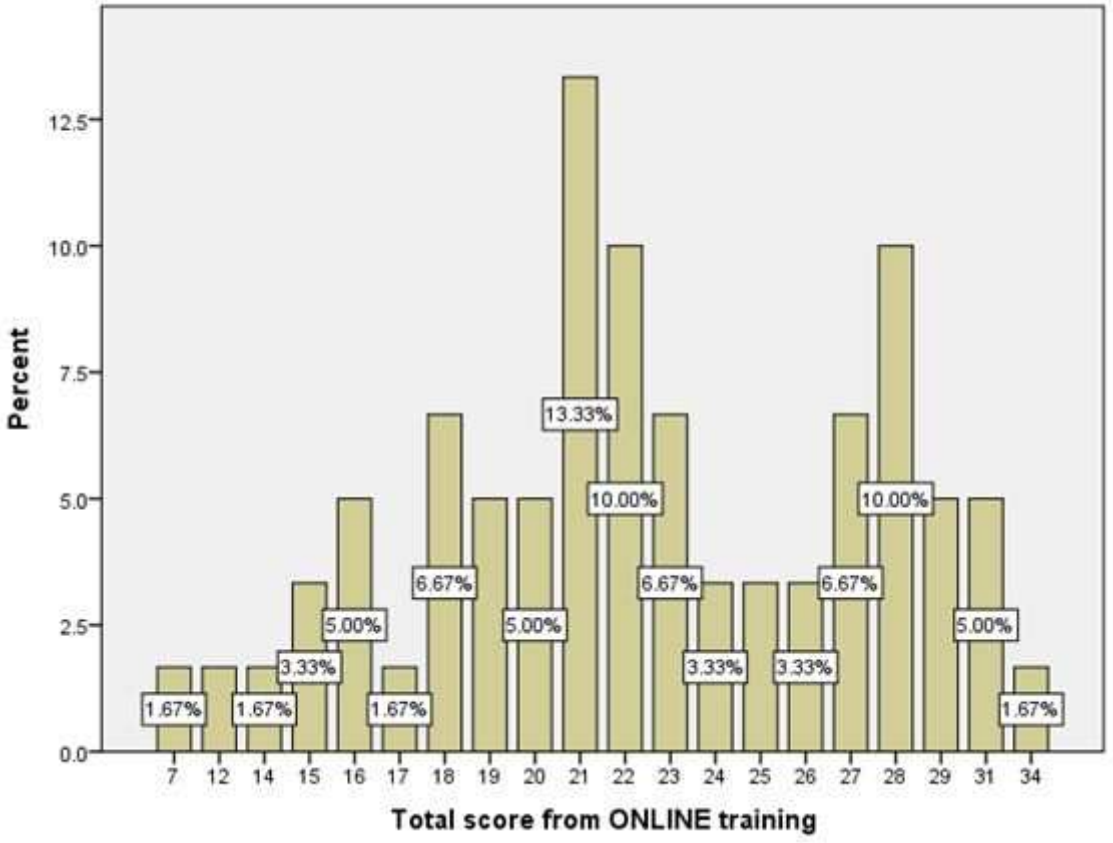


Figure 2 Percentages of overall score of 7 areas in Face to Face training

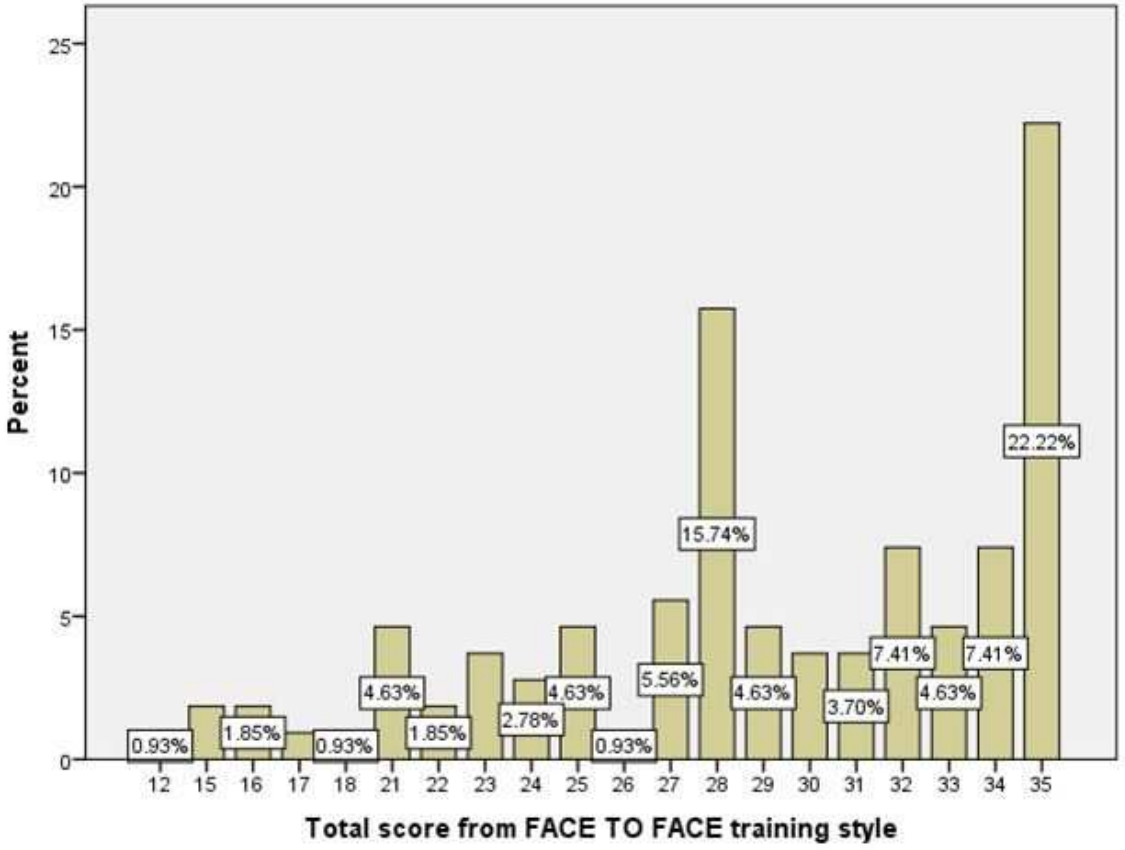
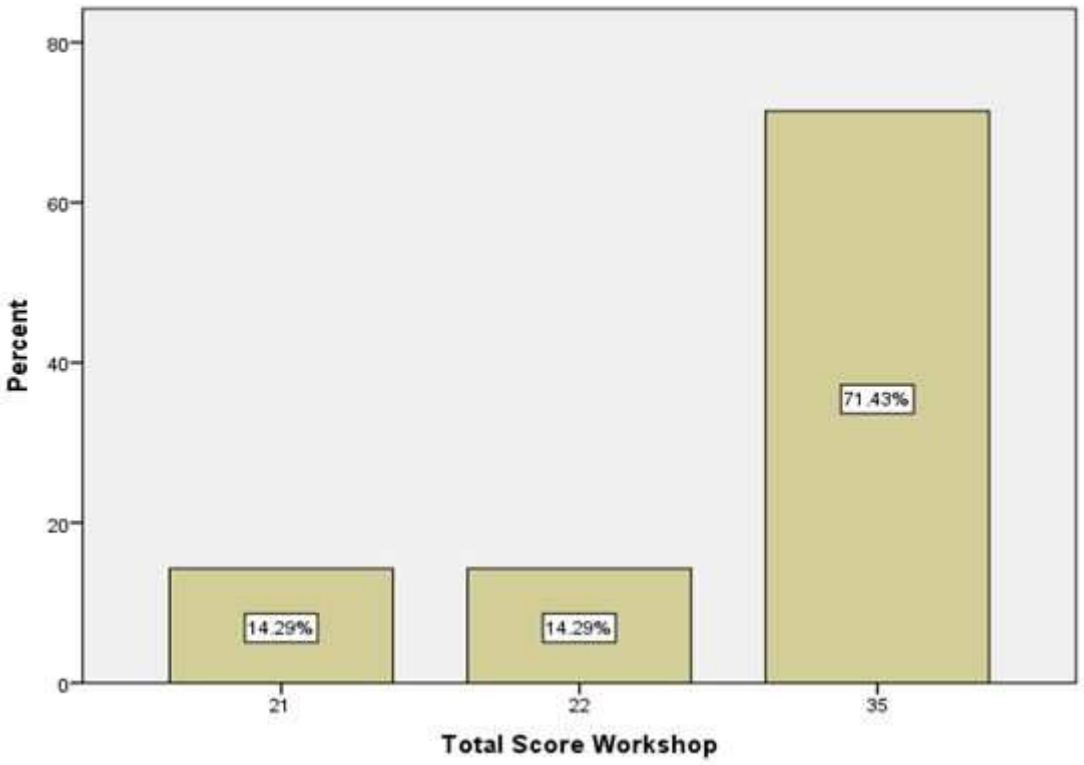


Figure 3 Percentages of overall score in Workshop training style


80
60
40
20
0
Percent
14.29%
14.29%
71.43%
21
22
35
Total Score Workshop