Police Cybercrime Training: Strategies, Delivery and Perceptions

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

Context

- Funded by Police Knowledge Fund (College of Policing/HEFCE)
- Sought to explore every aspect of the investigation of cyber crime in a large regional force
- 12 workstreams developed (on the basis of a Needs Analysis) and this presentation pertains to one
    - 'Assessment of Cybercrime Training'

Background

- Police training/education is of perenial interest (Bryant et al 2013)
- Concerns over everything from level of learning to pedagogic strategies
- From "*acquisition* and *transfer*" to " 'participation' and 'becoming' " (Heslop, 2011, p. 327)
- Tension between 'theoretical' and 'real knowledge' (Chan et al, 2003, p. 304)

LEEDS BECKETT UNIVERSITY

Specific Issues Pertaining to Cyber Training

- Success relies on skilled/motivated staff, not just high quality training (Marcum et al, 2010)
- Skills/confidence of front line staff (Holt and Bossler, 2012)
- Differentiation between local/national responses
- Lack/absence of appropriate in-service training Cummins-Flory (2016)
- 'Hyper-connectivity' and mundane offences (Wall and Williams, 2013, p. 410)

Specific Issues Pertaining to Cyber Training (continued)

- Cyber knowledge as 'Core' or 'Specialised' knowledge (HMIC 2015)
- The need for 'general digital awareness' (PA Consulting Group (2015, p. 16)
- "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" (HMIC, 2015, p. 30)

LEEDS BECKETT UNIVERSITY

Key Themes Identified in the Literature

- Evidenced Knowledge V Experiential Knowledge
- Quality of Training
- Resources
- Positioning of Knowledge within the Organisation
- E-learning

LEEDS
BECKETT
UNIVERSITY

Method

- Questionnaire circulated to all officers who had undertaken cyber training in the organization (circa. 600)
- Compared experiences of Online, Face to Face, Workshop and Q and A.
- Included some free text options to generate qualitative data

- Aimed to Answer these Questions
- i. What are the characteristics and differences between training styles, in terms of
  the Format, Satisfaction, Relevancy, Usefulness of knowledge, Increase of knowledge,
- and Increase of skills and Increase of job performance?
- ii.   Is there a training style preferred by the participants?

Findings

- Quantitative
  - Face to Face (i.e. Traditional) training methods were significantly favoured over e-learning packages

- Qualitative
  - Online learning (advantage) 'Flexible'
  - Online learning (disadvantages) 'Superficiality of learning', 'Complexity', 'Questions', 'Lack of interaction'

  - Face to Face learning (advantages) 'Clarification', 'Interaction', 'Knowledge/Skill of Trainers', 'Ease of Learning', 'Sharing of Experiences'
  - Face to Face learning (disadvantages) 'Nothing/NA', 'Time to Travel/ Participate', 'Mixed Ability of Learners', 'Too Long/Too Intense', 'Relevance to Role'.

Discussion

- Evidenced Knowledge V Experiential Knowledge
- Quality of Training
- Resources
- Positioning of Knowledge within the Organisation
- E-learning

Conclusion

- Cyber training, in this organisation, presented a real mix of practical, strategic and cultural challenges.

- Practical issues including estate, capacity, hardware issues

- Strategic issues included that of about where to situate cyber skills in the organization

- Cultural resistance to adding cyber skills to the generic officer role.

LEEDS
BECKETT
UNIVERSITY

References

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

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

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): 7–38

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

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

PA Consulting Group (2015). Digital Investigation and Intelligence: Policing Capabilities for a Digital Age. London: PA Consulting. http://www.npcc.police.uk/doc uments/reports/Digital%20Investigation%20and%20Inte lligence%20Policing%20capabilities%20for%20a%20digit al%20age%20April%202015.pdf (accessed 9 March 2018).

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.

LEEDS BECKETT UNIVERSITY