View metadata, citation and similar papers at core.ac.uk

brought to you by CORE
provided by Leeds Beckett Repository

LEEDS BECKETT UNIVERSITY

The Cybercrime & Security Innovation Centre (CSI)

Cybercrime Policing: Needs Analysis & Building a Research Culture

Z.C. Schreuders, T. Cockcroft, E. Butterfield, J. Elliott, M. Shan-A-Khuda, A.R. Soobhany

Cybercrime and Security Innovation Centre, Leeds Beckett University, Leeds, LS6 3QS, UK

csi@leedsbeckett.ac.uk

Progress

Collaborating with university academics, a research training programme has been initiated to build a research culture and capacity within the Cyber Crime Team (CCT) and Digital Forensics Unit (DFU) of one of the largest police forces in the UK. An evidence-based approach is employed to improve the effectiveness and efficiency of investigating cyber enabled crime. The needs assessment has been completed and areas of needs identified.

Aims

- Cybercrime is not exclusively a technical problem
- This research will analyse the cyber-investigation lifecycle:
  - from the experience of the public when reporting cybercrime, to the call taker, the attending officer, investigator, and the various support units,
  - to identify key knowledge gaps and needs in the policing of cyber enabled crime
- Deploy evidence-based solutions with the Police force
- Enable force personnel to engage in research

Stages of the project

Perform needs analysis
Identify priority areas and projects

Develop research & cyber investigation potential
Perform secondary research

Facilitate research within HTCU
Engage in primary research

Evaluation of the collaboration
Formally evaluate overall outcomes

Dissemination
Organise conferences and publish papers

References

- Kaufman Roger A., and Fenwick W. English. 1979. *Needs Assessment: Concept and Application*. Educational Technology.
- T. J. Holt and A. M. Bossler. 2014 . *An Assessment of the Current State of Cybercrime Scholarship*,. **Deviant Behaviour**, vol. 35 (1), pp. 20–40.

Abstract

- The needs assessment was conducted using:
  - Kaufman's Organizational Elements Model (OEM), and SWOT
  - Individual and group interviews involving a wide range of police specialist units and strategic leads
- Academics are currently working with force personnel to perform secondary research

Areas of needs

Training/ Knowledge
- Raising awareness of cybercrime / digital evidence
- Bespoke and evidence awareness training
- Access to knowledge and training

Procedures
- Triage practices
- Practices across districts
- Action Fraud delays
- Flagging of cyber cases

Communication/ Structures
- Communication between specialist units
- Feedback loop with Action Fraud
- Clarity of roles and units
- Non-technical summaries in reports

Software/ Hardware resources
- Tools to support strategic focus
- Standalone PCs
- Automation of manual work

Legal issues
- Lack of clarity over RIPA application
- Insufficient legal training

What next

- Academics and force personnel will:
  - jointly conduct primary research
  - explore ways to maximise the efficacy and efficiency of cyber investigations
- Postdoctoral research fellows and “research champions” will be embedded within the force
- Propose and evaluate process, practice and solutions based on the outcome of the Needs Assessment
- Train and equip the force to engage in research and professional development
- Dissemination of findings