Improving Cybercrime Reporting in Scotland: The Victims' Perspective

Juraj Sikra

[a] *Affiliation (University of Strathclyde, Computer & Information Sciences, juraj.sikra@strath.ac.uk).*

Keywords: *Cybercrime, Victims, Reporting, Policing, Scotland.*

People victimised by cybercrime can feel excluded within their communities due to shame, which results in underreporting cybercrime. This research builds on earlier work by Sikra, Renaud and Thomas (2023), which used a systematic literature review to establish a theoretical foundation for improving economic cybercrime reporting in Scotland. Using the paradigms from the latter, this research focuses on three types of Scottish victims of cybercrime (SVC): Individuals, Private institutions and Public institutions. It analyses their reporting experiences via the taxonomy of Human-to-human (H2H), Human-to-machine (H2M) and Machine-to-machine (M2M). Importantly, it adds value to the research subject by using victims' own views on what is required to improve cybercrime reporting in Scotland. In doing so, it is addressing a research gap whereby there is currently no research with victims on how to improve cybercrime reporting in Scotland.

This study used a qualitative semi-structured interview design to collect information from SVC about their background, the cybercrime they had to endure as well as their experiences of reporting and suggestions for improvement.

Participants were recruited using several methods. Firstly, in cases of Private and Public institutions, news coverage was followed-up for news of prominent cybercrimes based on which potential interview candidates were contacted. Secondly, all researchers' private connections were explored. Thirdly, snowballing participants was used. Fourthly, recruitment was done via social media. There was a total of 10 SVC (9 males, 1 female): 3 Individual SVC who incurred cybercrime harm of £1000, £5240, and £20. 2 Private institution SVC who incurred cybercrime harm of over £20,000 and non-monetary harm. 5 Public institutions, represented by various functions, which suffered technological and psychological harms. All the cybercrimes were from the years: 2012 (1), 2015 (2), 2017 (1), 2020 (1), 2021 (3) and 2022 (2), where the number of interviewees is in brackets.

Approval for the study was granted by the CIS Departmental ethics committee 7 times from 22 April 2022 – 09 January 2023. Most of these were extensions to the original application due to substantial problems with participant recruitment. The analysis was carried out with 'NVivo 1.3 Release software' in three stages which were: Stage 1: Initial coding, Stage 2: Focused coding, Stage 3: Thematic coding.

Individual SVC were attacked via an E-Bay Scam, HMRC Scam and Credit card details theft. Individual SVC link improved reporting to aftercare and returned finances. Individual SVC link impeded reporting to anxiety and frustration with the Police. All individual SVC reported via H2H approaches. Private institution SVC were attacked via .ru ransomware. Private institution SVC link improved reporting to having a unified phone number, awareness raising and a possibility to report online. Private institutions

SVC link impeded reporting to unpreparedness of the local Police as well as not knowing who to report to. Private institution SVC reported via H2H approaches, but only one reported to the Police. The other reported to their IT company. Public institution SVC were attacked via fraudulent invoices, ransomware, and a vendetta-motivated cybercrime. Public institution SVC link improved reporting to following procedures and taking a multistakeholder approach among others. Public institution SVC link impeded reporting to Police being unhelpful and terminological confusion. All Public institutions SVC reported via H2H approaches both to the Police and multiple other interested agencies in most cases.

Since all SVC reported via H2H approaches this suggests that it is the dominant mode of reporting currently utilised in Scotland implying a proclivity towards a socially inclusive preference, which suggests that the way to improve cybercrime reporting should be social rather than purely technical.

References:

Sikra, J., Renaud, K. V. and Thomas, D. R. (2023) 'UK Cybercrime, Victims and Reporting.' *The Commonwealth Cybercrime Journal*, 1(1), pp. 28-59.

Room No: TL329 (Zoom), Wednesday 14th of June, 11:15

Go back to the full list of presentations

Go back to the full schedule