The Scottish Institute
for **Policing Research**

First responder guide for cybercrime and digital forensics

Evaluation of training pilot

Miranda Alcock

Associate of the Scottish Institute for Policing Research

October 2017

First responder guide for cybercrime and digital forensics
Evaluation of training pilot

Key findings

Six pilot training days held – 98 participants completed questionnaires

89% had **not any previous training** in cybercrime/ digital forensics

79% were **not at all or not very confident** in dealing with operational incidents involving cybercrime/digital forensics

but... 56% had **some experience** of dealing with these incidents

Before the training

Droman Solutions

After the training

76% agreed or strongly agreed that they **now had more confidence** in dealing with operational incidents involving cybercrime/ digital forensics

74% agreed or strongly agreed that they **found it an easy way to learn** about this topic

81% agreed or strongly agreed that they **found it easy to navigate** through the game

60% would **like more training in this format**

> "The training has been very beneficial and it has given me an understanding on how to approach incidents involving cybercrime"

First responder guide for cybercrime and digital forensics
Evaluation of training pilot

Introduction

1. Cybercrime is a growing and evolving threat, both nationally and internationally. Recent figures indicate that fraud and computer misuse now comprise nearly half (47%) of all crime in England and Wales.[1] There is an urgent need for relevant and accessible training for non-specialist police who carry out the initial response in dealing with this crime area.

2. The First Responder Guide (FRG) was designed as an innovative approach to a number of challenges facing the police in dealing with cybercrime and digital evidence:
   - how to train large numbers of people and keep them up-to-date with an evolving operational challenge,
   - how to provide front line officers with relevant information as and when they need it, and
   - how to reduce the cost and abstractions from duty incurred by traditional classroom training.

3. The FRG has been developed through a three-way partnership comprising Droman Solutions Ltd, Police Scotland and Abertay University, building on the strengths of each. The development work has been funded by Droman Solutions with support from Scottish Enterprise and Interface (Innovation Scotland).

4. The game aspect of the guide is intended to make training more engaging and encourage frequent interaction with the training materials, so that skills are not just learned but practised. The guide was initially developed through a students' 'game jam' organised by Abertay University, and a subsequent prototype trial with police officers in Dundee. This resulted in the development of a game with three scenarios – a reactive patrol call, a pre-planned house search and a spontaneous office call. The game is designed to be used on a tablet or other mobile device, reducing the need for abstractions, but can also be used on corporate desktops.

5. Following the development of the three scenarios, the partnership organised a more extensive trial with front-line police officers and staff from across Scotland. Droman Solutions asked the Scottish Institute for Policing Research to undertake an independent evaluation of this larger trial. This report describes the findings from that evaluation.

Methodology

6. Six pilot training events were run in Edinburgh (2), Fife, Glasgow (2) and Irvine. Participants were asked to attend without any prior briefing as to the nature of the event beyond being told that it was related to cybercrime. All those invited to participate had some responsibility for initially responding to incident calls. Each pilot day typically comprised four sessions, with about six participants in each session, and each session lasted 90 minutes.

7. Participants were briefed on the background to the project, the nature of the training and the feedback and evaluation process. They were then left to themselves (in a group) for an hour to work through the scenarios. They were allowed to confer and discuss their experiences during this time.

8. As part of the evaluation, participants were asked to complete a short questionnaire anonymously (Annex 1); the first few questions were completed before they started on the training and the rest after completing the game. This report is based on an analysis of the responses to those questionnaires. Analytical data on technical aspects of how participants were using the game was also collected electronically and is being analysed by the developers.

---

[1] *Crime in England and Wales: year ending March 2017*. Office for National Statistics, 2017 (Hyperlink)

9. It is important to note that the pilot environment was not typical of how the guide will be used in real life. Normally, officers would access the training in short bursts, at a time convenient to them, and they would have more time to practice navigation. The findings from this evaluation should be seen in this context. In particular, the pressure of time people experienced in the pilot (which was frequently commented on) would not be the same in real-world use.

10. The organisation of five of the pilot days went smoothly and as planned. Unfortunately, the organisation for one session (Day 4) was less well organised and this appears to have affected how participants experienced the training.

Demographics

11. Ninety-eight participants completed questionnaires, 89% of whom said they had received no previous training in cybercrime or digital forensics.

12. Of the people who completed questionnaires, 61% were police constables, 11% were detective constables, 7% were police staff and 3% were sergeants. The remainder didn't specify their rank.

13. Respondents were fairly evenly split by age with roughly a third in each of the main age groups - 31% in the 26-35 age group, 27% were 36-45, and 33% were 46-55; 5% were younger and the rest didn't specify.

14. Nearly half of the respondents had less than 10 years service (with 24% having 1-5 years and 23% having 6-10 years); 16% had 11-15 years. There were small numbers in the other categories or not specified.

Quantitative findings

Prior experience and levels of confidence

15. More than three quarters of the respondents had little or no confidence in dealing with operational incidents involving cybercrime/digital forensics, prior to completing the training. This was split between 24% being not at all confident and 54% not very confident. Of the remaining respondents, 20% were fairly confident and one was very confident.

16. Over half the respondents had some experience of dealing with operational incidents involving cybercrime/digital forensics (56%). Most of the rest had no experience (39%), while a few (5%) described themselves as experienced in dealing with it.

17. Based on the sample participating in this trial training, these findings indicate that many officers may be attending operational incidents involving cybercrime with little or no confidence in how they should be dealing with them. This has implications for how victims and members of the public may experience police handling of this type of crime (now approaching half of all crime in England and Wales), creating a reputational risk for the police service and consequent damage to public confidence.

Overall views after completing the training

18. Respondents were generally positive about the training after completing the game:

    - 81% agreed or strongly agreed that they found it easy to navigate through the game
    - 74% agreed or strongly agreed that they found it an easy way to learn more about cybercrime/digital forensics
    - 76% agreed or strongly agreed that they now had more confidence in dealing with operational incidents involving cybercrime/digital forensics

Perceptions about different features of the game

19. Participants were asked what they thought were the best features of the game and to rank these. About 10% of the respondents didn't clearly rank their responses to this question. Of those that did (n=86), the feature most often ranked as no. 1 was that it was simple to use (36% of respondents) and length of time to complete was the least liked feature (ranked 7, also by 36% of respondents).

20. Figures 1 shows how many people ranked each of the seven features as most important and least important to them and Figure 2 shows the features which respondents ranked in their top three.

Figure 1:

Number of respondents ranking individual features of the game as most important

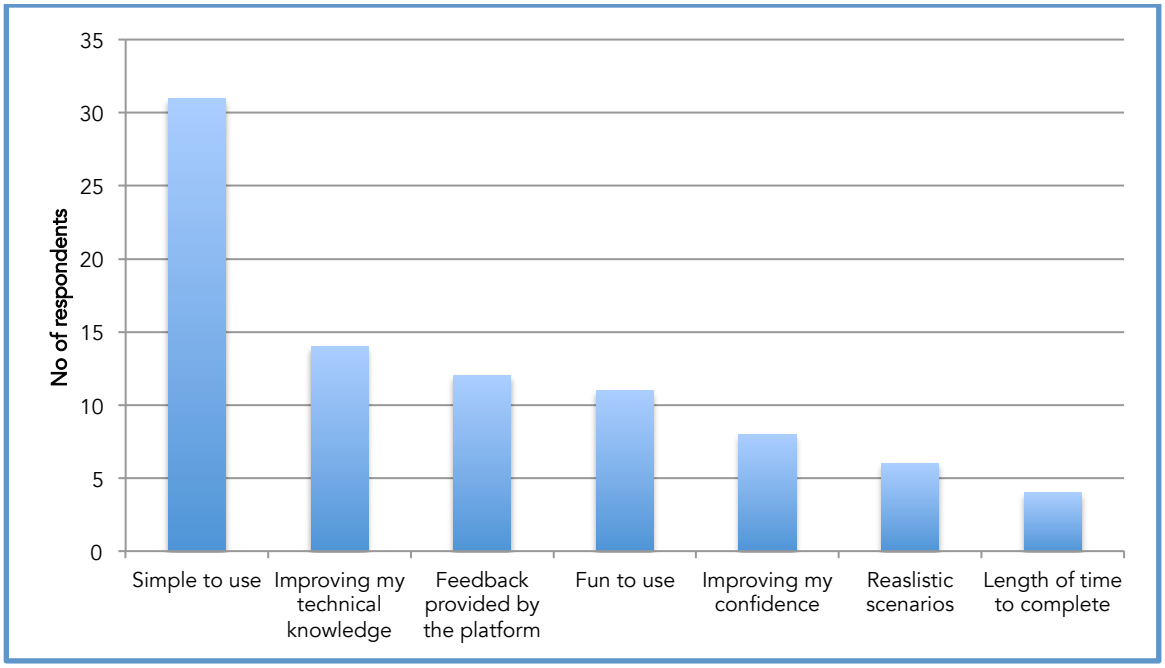
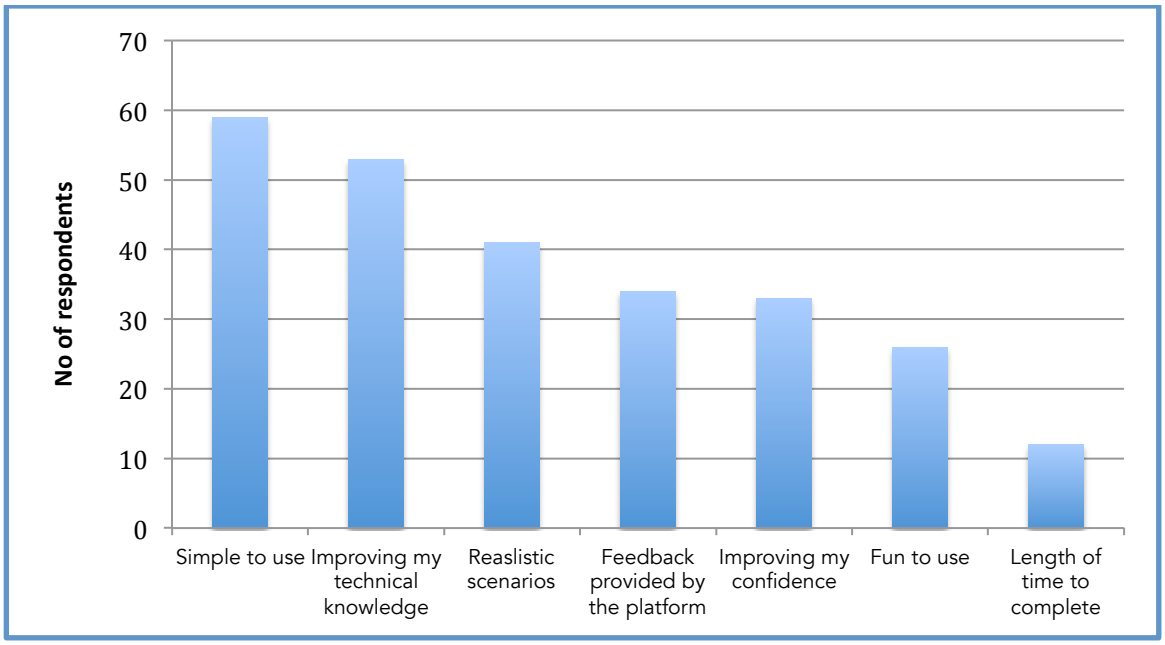


Figure 2:

Number of respondents ranking individual features of the game in their top three



21. Figure 2 shows that realistic scenarios, while rarely ranked as the most important feature, was in the top three of over half of the respondents.

22. Notable in these figures is the unpopularity of the length of time to complete. The artificial conditions under which participants were trying out the game is likely to have been a factor here. The pilot required participants to sit down for an hour and go through the whole package. If the guide was being used as intended, users would be able to browse some notes and try a scenario, allowing more time to get used to the navigation, before returning to complete it. The different scenarios could be completed at different times, giving users flexibility over when they completed the training.

Qualitative analysis

23. The questionnaire included two free text questions about the training: one asking participants what they liked least about this type of training; and the other asking for any further comments on the usefulness of the training method or any suggestions for improving knowledge of dealing with operational incidents involving cybercrime and digital forensics.

24. There was considerable overlap in how respondents answered these two questions and variation in the number of comments and suggestions they made. As a result, the analysis of the two free text boxes was combined. Multiple comments and suggestions from individual respondents were separately identified and grouped into common themes.

25. As participants were allowed to discuss the game during the training, there was some commonality of suggestions from individual sessions.

Comments on the overall approach

26. There were over 50 generally positive comments on this training, from participants across the range of age and experience covered by the sample. Several respondents specifically mentioned their preference to this approach over the current Moodle training (a proprietary e-learning system). Some typical quotes were:

    "A fun, easy to use, interactive training programme. So much better than the current Moodle training and much better suited to my personal learning style. Definitely a step in the right direction."

    "Excellent way of providing training. Interactive learning with realistic scenarios enables you to take in the points that are significant to enquiries."

    "I found I actually knew very little about cybercrime, this certainly highlighted those areas."

    "It is an interesting way to learn. It makes you think, but is different from just reading and answering questions."

    "The training has been very beneficial and it has given me an understanding on how to approach incidents involving cybercrime. The feedback following the questions was very useful. I feel that I will be able to attend incidents as such with more confidence."

27. A significant minority of participants (22) made negative comments on the game. A common theme in their comments was related to the time taken to complete the game, but several participants just felt that this kind of learning didn't suit them: they weren't 'gaming' people, they didn't like using tablets, they preferred Moodle or classroom training. Some typical examples:

    "I would rather have a document to read or attend a training session speaking to cybercrime experts. Alternatively prefer Moodle training."

    "I feel this platform is not right for my learning style and believe a class room based input would be beneficial"

    "I felt that the training was difficult to navigate and disrupted the learning experience. This lead to frustration which was detrimental to learning"

    "Simpler layout on SOP/Intranet negates need for game. The game will not develop operational experience"

    "I started to get dizzy going round all the rooms, started to get bored, sorry."

28. It is important to note that over half of those making negative comments (13) had attended the training day (Day 4) where there were problems in the organisation of the event.

Comments about the game itself

29. Comments on the game itself can be grouped into three categories:

    - aspects of the game that respondents said they liked,
    - what they liked least about using the game (often linked to what could be improved), and
    - comments on the content of the game.

30. What respondents liked included the feedback from the questions and the information provided during the game:

    "The feedback from the questions was really helpful, whether you got it right or wrong."

    "Scenarios seem straightforward and likely to happen in the real world."

    "Info provided at start and end of scenarios good."

31. Aspects of the game that respondents liked least can be further grouped under a number of common themes - locating items, navigation, graphics and length of time to complete the game. There were 10-15 comments around each of these areas.

32. The question '*what did you like least?*' was specifically designed to gather information to help improve the game. The wording wasn't neutral but had an intended negative bias to encourage participants think about what they had found difficult or frustrating when using the game.

33. Many of the comments are inter-related, for example, people may have had difficulty navigating, and therefore found the game time-consuming. Typical quotes under the four categories identified above included:

    Locating items
    "I was unable to see how many items still to find on the room scenario. A little countdown would be useful"

    "Unable to find some of the items. Could be improved if there was a function that takes you to the devices if you are unable to find them"

    "May need 'clues' in the pre-planned scenarios when the player is searching to save frustration"

    Navigation
    "A floor plan type of window would be a good addition which could run in the bottom corner showing your relative position in the property"

    "Difficult to navigate in house search. Got stuck in house not knowing some items were questions"

    "The navigation was a little sticky, adding to the time required to complete a task that could be halfed (sic) without all dragging etc."

    Graphics
    "Graphics could be slightly better, for instance the CD stack looked like books" (a number of people commented on this).

    "Realistic search would have included facilities to open drawers, etc."

    "Should be able to move items / pick items up as with real search"

    Length of time taken to complete the game
    "Gaps between questions were sometimes longer than necessary to due to location of productions within the game"

    "Very time consuming. May help to be able to open cupboards, etc. to look inside. Same for bins and books etc." (Also, see comments above on graphics…)

34. A number of comments concerned the pre-planned house search scenario. Analysis of the data collected automatically by the system indicates that the average time taken by participants to complete this scenario

(19 minutes) was longer than the other two scenarios. The reactive patrol call took participants 12 minutes on average to complete and the spontaneous office call only five minutes.

35. Three respondents commented that while they felt they improved their knowledge through completing the game, 'failing' the scenarios left them with an overall negative experience. While this is only a small minority of participants, developers may wish to consider how to mitigate these experiences, for example through more positive feedback. Much of the rationale for the gaming approach is to encourage people to learn through experience in a 'safe' virtual environment, where mistakes or errors of judgement don't matter. Users need to feel positive about completing the scenarios to realise the full potential of the training.

36. In addition, three respondents found the sounds annoying and there were a few miscellaneous comments with too little detail to categorise.

Comments on the content of the game

37. A minority of comments related to the content of the game. A few people felt the wording of the questions was a bit ambiguous or they could have been worded more clearly. A few people also commented on the reference to Faraday bags, which they weren't familiar with. Comments in this category tended to be more critical:

    "Some answers were not entirely accurate, depending on the users experience and knowledge. Faraday bags are not commonly used."

    "Items such as printers which are updated frequently, advising not to seize items such as this may soon be incorrect as new models may have internal storage. This should be highlighted."

    "Some of the feedback was contradictory, for instance, not seizing routers or printers despite the feedback stating that these sometimes had internal memories."

    "Some answers were not realistic i.e. phone would not be seized if it had threatening facebook message. Print outs only."

38. The game is now being further developed, following this pilot, with developers taking on board many of the comments and suggestions. For example, a floor plan is being added to assist navigation, and the graphics are being improved. One of the advantages of this approach is that a facility to allow users to give immediate feedback or report errors/problems (similar to those captured through the questionnaire) can be integrated into the game. The developers plan to include this feature in future versions of the game.

Overall views on the guide

39. In order to get an indication of respondents' overall view of the game (and this approach to training), each completed questionnaire was assigned to one of three possible categories - positive, mixed (ie respondents liked some aspects but not others) and negative. This was done by weighting the responses to the questions answered following completion of the game (apart from the ranked one) and making a judgement on the nature of the comments in the free text boxes.

40. From this analysis, 63% respondents were generally positive about the guide and this approach to training, 22% were negative and 14% were mixed[2].

41. Using these results, there was no correlation either between the age of the participant and their overall view of the guide or their length of service and their overall view. So, it doesn't appear that younger officers particularly prefer this type of training, as might have been assumed.

42. As previously mentioned (paragraph 8), one of the pilot days was poorly organised and this had an impact on participants' overall view of the game. Annex 2 shows the breakdown of overall satisfaction according to the different pilot days. This clearly demonstrates the untypical negativity towards the game experienced by respondents on Day 4.

[2] NB Doesn't add up to 100% because of rounding

Enhancing the effectiveness of the training

43. Eight participants felt that they (and others) would get more out of the game if they had received some pre-training and five participants thought it would be useful to have an aide memoire, either as well as, or instead of, the game:

    "It is useful but I think it would have been more beneficial following some structured training on cybercrime."

    "This is a unique process for training however there is a need to know the legislation first as such this seems to be a knowledge check"

    "With a rise in incidents involving cybercrime a booklet with the key feedback points would be beneficial as a reference point."

44. In fact, the guide includes both briefing material for reading before starting the game and supporting material for reference during the game. So these comments are perhaps more about better signposting to the existing supporting material rather than a fundamental change in approach. The developers are currently working to improve this.

Interest in more training in this format

45. The partnership developing this game has a long-term vision for building a suite of training modules in a similar format, which students will be able to access on a device issued to them personally. Participants were therefore asked if they would like to see more training in this format, and if so, in what subjects. Just over half (60%) of respondents said they would like to see more training, and a just over a quarter (27%) said they wouldn't (15% didn't answer).

46. Not all the participants who said they would like more training made suggestions for topics. Of those that did, the commonest response was that it could be applied to all training areas. Other topics suggested were crime scene management, drugs and major incidents. Figure 3 is a word cloud showing the frequency different topics were suggested.

Figure 3:
Word cloud of suggestions of topics for future training using this approach[3]

[3] The bigger the letters reflect the more frequent the topic was mentioned.

47. Other suggestions for training in this format included

    - drug searches of houses to show assets held by the drug dealer (eg high value jewellery, foreign bank accounts, shares, etc.)
    - scenarios about taking witness statements, involving search powers for drugs and offensive weapons etc.
    - adaptation of the game to suit different roles, for example, dealing with cybercrime over the telephone for service advisers.

Conclusion

48. The findings in this evaluation suggest that:

    - there is a widespread need for training in cybercrime and digital forensics;
    - that an interactive game-based approach using mobile devices could be a cost-effective way of delivering this training. Such an approach has the potential to reduce pressure on training personnel and associated budgets;
    - there is potential to develop this approach to other areas where immersive scenario-based training, of the kind typified by large fixed-site facilities such as Hydra, would be beneficial.

49. Cybercrime and digital forensics is a fast moving and continually evolving area. Any training approach must therefore be flexible enough to accommodate new threats and technological developments quickly and effectively. This type of immersive learning, using a virtual environment, allows frequent updates as subject matter experts can quickly alter the content to reflect the most recent changes in technology.

Annex 1: Participant questionnaire

Biographical information

Please complete this short anonymous questionnaire prior to starting the training course.

URN:	Rank:
Age Range - please circle one option - 18-25 26-35 36-45 46-55 56+	Service Range- please circle one option: 1-5 6-10 11-15 16-20 21-25 26-30 30+

Have you had previous training in cyber/digital forensics? Yes / No – if 'yes' please enter details below

Further Details:

Please circle your answer

Current confidence in dealing with operational incidents involving cybercrime/digital forensics ?

Not at all confident Not very confident Fairly confident Very confident

Experience of dealing with operational incidents involving cybercrime/digital forensics ?

No experience Some experience Experienced Highly experienced

To be completed following the training – please circle one answer

I found it easy to navigate my way through the game –

Strongly disagree Disagree Agree Strongly agree

I found this an easy way to learn more about cybercrime/digital forensics –

Strongly disagree Disagree Agree Strongly agree

I now have more confidence in dealing with operational incidents involving cybercrime/digital forensics –

Strongly disagree Disagree Agree Strongly agree

Where were the best features about this training platform?
(Please rank in importance: 1 being the most important to 7 being the least important)

Simple to use	
Fun to use	
Improving my technical knowledge	
Improving my confidence	
Length of time to complete	
Realistic scenarios	
Feedback provided by the platform	

What did you like least in this training?

Do you have any further comments about the usefulness of this training or this training method, in improving your knowledge of how to deal with operational incidents involving cybercrime/digital forensics or how it could it be improved?

Would you like more training in this format? If yes, in what subjects? Yes / No

This exercise is anonymised. However, if you are willing to be contacted later by an independent researcher for any follow up questions, please provide your work email address, at the bottom of this sheet. This questionnaire will be destroyed once the evaluation is complete.

We would be very grateful of your input.

Work Email Address:

Annex 2: Overall views of participants for each pilot training day

Number of respondents on each of the pilot days who were positive, had mixed views, or were negative about the first responder guide.