*This is a pre-copyedited, author-produced version of an article accepted for publication in Policing:A Journal of Policy and Practice following peer review. The version of record* ***Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2018). A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime. Policing: A Journal of Policy and Practice, 1–10; doi.org/10.1016/0038-1098(79)91043-3*** *] is available online at: https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay090/5233865.*

# A Qualitative Exploration of Police Officers Experiences, Challenges, and Perceptions of Cybercrime

Dr Lee Hadlington

Division of Psychology

De Montfort University

The Gateway, Leicester. LE1 9BH

Email: lhadlington@dmu.ac.uk

Telephone: 0116 207 8626

Dr Karen Lumsden

Department of Criminology
University of Leicester
The Friars
154 Upper New Walk
Leicester LE1 7QA

Dr Alexandra Black

Department of Law and Criminology,

Sheffield Hallam University, Sheffield, UK

Dr Fenia Ferra

Faculty of Technology

De Montfort University

The Gateway, Leicester. LE1 9BH

**Abstract**

Victimisation from cybercrime has increased exponentially over the past decade. Frontline police officers are dealing with a variety of crimes different than those existing in an era before the advent of digital technology. Frontline officers are expected to encourage members of the public to report such crimes, to investigate them, as well as keeping up-to-date with the latest developments in this ever-changing landscape. This study explored the issues that frontline officers are dealing with on a daily basis when it comes to cybercrime. 16 front line police officers took part in focus groups exploring key questions around aspects of cybercrime. The key themes discussed in this article include the difficulty of defining what is cybercrime, the contrast between the speed of developments in cybercrime and the speed of investigation, and the ineffectiveness of current training. The results are discussed in the context of a need for clearer training information to be delivered to all officers and staff who come into contact with aspects of cybercrime.

**Keywords:** cybercrime, internet, policing, victims, victimisation



## Introduction

The current level of reported cybercrimes in the UK for adults stands at approximately 4.7 million incidents in the year ending September 2017 (British Crime Survey, 2017). The level of victimisation from cybercrime has a respective knock-on effect for individual police forces around the UK, who are expected to provide an effective and agile response to victims (Holt & Bossler, 2012). In an effort to maintain such a response, a variety of assumptions in relation to frontline officers' knowledge and understanding of an ever-changing and complex environment

are made (Holt & Bossler, 2012). These assumptions include all officers having a full understanding of key definitions and terms related to cybercrime, having knowledge of the required routes for investigation and evidence gathering, and of there being effective training in place which supports officers in advising (potential) victims as to the best course of action (Holt & Bossler, 2012). This study aimed to explore frontline officers' current knowledge in relation to cybercrime. It also shed light on their key concerns and perceived issues which included frustrations related to lack of knowledge and power to deal with cybercrime, The contrast between the speed at which cybercrime develops versus the speed of investigation, and a perceived lack of specialist resources. Officers also drew attention to the ineffectiveness of current training provision.

## Literature Review

### *Defining Cybercrime*

The concept of cybercrime has evolved in a number of distinct ways over recent years, particularly in the light of technological developments (Holt, Bossler, & Seigfried-Spellar, 2015; Wall, 2001). Aligned with this, the way in which the concept has been defined has also gone through a number of reiterations, in turn creating potential confusion for both law enforcement and the public alike (Wall, 2007). Cybercrime has been frequently dichotomized into different categories, based on the motives and target(s) of the attack. The most frequently used classification distinguishes between two main categories, these being ' cyber-dependent' and 'cyber-enabled' (HM Government, 2016; McGuire & Dowling, 2013; Wall, 2008). Cyber-dependent crimes are those that can only be committed using computers or computer-related technology, such as the spreading of malware or denial of service (DDoS) attacks. In contrast, cyber-enabled crimes can be conducted both on and offline, with online aspects serving to

increase both the speed and scale of such crimes (National Crime Agency, 2016). Research has noted at that a lack of agreement related to how cybercrime is defined has generated a degree of confusion in the public, particularly in relations to which crimes fall under which categories (Wall, 2008a, 2008b). There is often an assumption that those in law enforcement who deal with aspects of these crimes on a daily basis have a clearer understanding of these categories and crime inclusion. However, as will be discussed in the next section, such an assumption may be misplaced.

***Police Officers' Views and Knowledge of Cybercrime***

Whilst the investigation and prosecution of cybercrime has received a lot of attention there has been a limited number of studies looking directly at police officers' perceptions of cybercrime (Bossler & Holt, 2012; Hinduja, 2004; Holt & Bossler, 2012). Often, police therefore it is important for them to have adequate knowledge and understanding of the area (Holt & Bossler, 2012). Although police officers understand the complexity and seriousness of cybercrime, their perceptions are often outside of the empirical evidence (Senjo, 2004). Senjo (2004) noted that police officers often based their perceptions of cybercrime on mass media depictions, something that Wall (2008a) also noted in terms of the public's perceptions. The research also noted that perceptions of cybercrime were heavily influenced by age, level of experience of these crimes, political pressures on investigation priorities, and a lack of relevant information (Senjo, 2004).

A perceived lack of specialized training provision has also been mentioned in previous studies (Davis, 2011; Hinduja, 2004). Law enforcement staff often present feelings of inadequacy and of being ill-equipped to deal with crimes related to digital technologies and the Internet. The

general consensus from research findings suggests that police officers desire more training and guidance when it comes to investigating cybercrime (Hinduja, 2004). They also recognise a need for more specialized training when it comes to the collection and processing of digital evidence (Hinduja, 2004). Burns, Whitworth, & Thompson (2004) also draw attention to a lack of resources, including staff and training. Burns et al. (2004) note that a persistent societal preoccupation with traditional offline crime puts more pressure on devoting essential resources to these types of offences rather than those involving cybercrime. This work focuses directly on US law enforcement, while studies of the UK policing of cybercrime are still in their infancy.

The research discussed above highlights a number of challenges which frontline officers encounter when dealing which cybercrime on a daily basis. This includes dealing directly with members of the public and advising them on a best course of action, and also aspects related to investigation and evidence gathering. At present, scarce research has been conducted into how frontline officers in the UK (in the case of this study – in England) view the concept of cybercrime, the challenges they face, and their perceptions related to the effectiveness of training. The aim of this study was therefore to delve into this issue deeper by asking a group of frontline officers, who come into contact with aspects of cybercrime on a daily basis as part of their operational roles, about their experiences. By gaining a deeper understanding of the issues these officers face, it is envisaged that areas of potential weakness can be identified, with the aim of developing more innovative and effective routes for training and awareness.

**Methods**

***Participants***

The study was a qualitative exploration of frontline police officers' perceptions of cybercrime at a mid-sized police force in England. A purposive sampling technique was employed, with a total of 16 actively serving police officers were recruited to take part in the study. The officers in question were all part of the same regional force, with the region covering predominately large urban conurbations, but also included considerable rural areas. In the context of cyber crime, the force deals with a significant portion of crimes involving a cyber enabled element, as well as having an Economic Crime Unit (ECU) dealing specifically with online fraud. Each officer had a minimum of 18 months' service within the force and they were recruited from various operational backgrounds. Drawing on participants from wide variety operational responsibilities was deemed important to ensure as many experiences were explored. The breakdown of the focus groups according to operational background is presented in table 1 below.



Table 1: Focus group break down according to operational background

| | Participants Operational background |
|---|---|
| Focus Group 1 (Female) | Respondent 1 (RS1) Control Room Operations; Respondent 2 (RS2) Control Room Operations; Respondent 3 (RS3) Investigations Management Unit; Respondent 4 (RS4) Incident Response |
| Focus Group 2 (Male) | Respondent 3 (RS3) Control Room Operations, Respondent 4 (RS4) Control Room Operations, Respondent 2 (RS2) |

| | |
|---|---|
| | Investigations Management Unit, Respondent 1 (RS1) Control Room Organisation Team |
| Focus Group 3 (Female) | Respondent 2 (RS2) Investigations Management Unit, Respondent 1 (RS1) Call Management Team, Respondent 3 (RS3) Managed Appointment Unit, Respondent 4 (RS4) Managed Appointment Unit. |
| Focus Group 4 (Male0 | Respondent 1 (RS1) Managed Appointment Unit*, Respondent 2 (RS2) Patrol and Resolution Officer, Respondent 3 (RS3) Investigation Management Unit, Respondent 4 (RS4) Investigation Management Unit. |

**Managed Appointment Unit* – members of the public can arrange to meet a police officer within a specific time period for non-emergency matters

***Focus Groups***

A focus group schedule was designed to explore: officers' knowledge and definitions of cybercrime (e.g. How do you define cybercrime?; What key activities do you associate with cybercrime?); attitudes towards cybercrime and victimisation (What risks are there online? Who do you think is targeted by cybercrime?); and aspects of training and learning (How have you learned about cybercrime? Who would you listen to about cybercrime?).

Before the focus groups, all participants were provided with a detailed information sheet outlining their right to withdraw, informed consent and information about protection of anonymity and the purpose of the research. Participants were also given a verbal debrief at the

conclusion of the focus groups, as well as being given a written debriefing sheet detailing the purpose of the research and the contact details of the lead researcher.

The focus groups were each held in a private meeting room at a local police station. Before the focus groups began, participants were asked to give a brief overview of themselves and their current role. Each focus group lasted for approximately one hour and they were all audio recorded and fully transcribed by an independent transcription company.

***Analysis***

Data were analysed using inductive thematic analysis, following the steps outlined by (Braun & Clarke, 2006): familiarisation with the data; generation of initial codes; searching for and creating themes; reviewing themes; and, refining and naming the themes. Inductive thematic analysis is data-driven, meaning that theme development was not restricted by the researcher's interest in the area (Braun & Clarke, 2006). Another researcher reviewed all transcripts in order to check for validity of the analysis. No differences were reported in relation to coding, however, several themes were expanded to include subthemes.

**Results**

The analysis of data revealed three initial themes: What is cybercrime?; the challenges associated with investigating cybercrime; and a lack of effective and consistent training for cybercrime. Additional subthemes were also identified, each of which are discussed in the context of the overarching themes.

***Difficulties Defining Cybercrime***

In the context of the first theme it was evident that although participants attempted to provide tangible interpretations for what cybercrime is and what it involves, there is still a great deal of confusion about what is meant or included in the term. There were numerous instances where participants stressed the huge variety of activities that the term cybercrime could cover:

*'…you look at the vastness of those tags that we're now putting on to cyber crime…' (RS3, Focus Group 2)*

*'…cybercrime is so ambiguous and so vague.' (RS2, Focus Group 2)*

*'…quite varied I guess.' (RS2, Focus Group 1)*

*'…because it's just too vast.' (RS4, Focus Group 3)*

Words used to describe cybercrime include 'vast', 'ambiguous', and 'vague'. There has been a great deal of discussion on how cybercrime is defined and the public understanding of cybercrime (Wall, 2007; Wall, 2008b). However, it appears that those working in frontline aspects of law enforcement agencies are also facing a similar struggle, this being clearly highlighted in several extracts from the focus groups:

*'I think sometimes it's good to have a word that we all have a general understanding of and people out there have a general understanding of, to kind of give people confidence that we can work towards helping them or at least give them some reassurance with it.' (RS2, Focus Group 1)*

*'You then referred to cyber crime, you're asking us, you know, what base could we need to deal with cyber crime, and I think police ourselves, tell us what it is first.' (RS1, Focus Group 4)*

It is evident that many of the officers who have to deal with aspects of cybercrime on a daily basis feel unprepared to do so, often feeling that they should have a deeper level of knowledge. This is more prominent in the second quotation, where the participant expresses the feeling that if the general public are asking them about aspects of cybercrime, they should have a good basic knowledge of the area. Holt and Bossler (2012) suggested that it is important for all officers to have a rudimentary working knowledge of the diverse range of crimes they may come into contact with. In many cases, individuals will be assigned to cases on the basis of availability rather than specialism, hence they need sufficient knowledge to deal with enquiries effectively (Holt and Bossler, 2012).

### *The Challenges of Investigating Cybercrime*

A key theme in the focus groups related directly to the investigation of cybercrime. Two sub-themes emerged from this overarching theme: feelings of frustration and powerlessness when dealing with cybercrime; and the paradox between the fast speed of development in cybercrime and the slow and laborious investigation process.

#### *Frustrations Related to a Lack of Knowledge and Power to Deal with Cybercrime*

Many of the participants had experienced some level of frustration or feelings of powerlessness when dealing with aspects of cybercrime. These feelings related to a perception that

investigating cybercrime is pointless, with the perpetrators never being bought to justice. A perceived lack of relevant knowledge surrounding aspects of cybercrime also served to generate feelings of frustration, with many participants not knowing how best to deal with calls from the public:

*'Yeah, you do feel frustrated sometimes. Because we tag it for the cyber team and they often add some very useful things that the officers can ask, but you think, where's it going? How are we going to stop this?' (RS1, Focus Group)*

*'When you take that call or you've got that job in front of you, you often feel, what are we going to do? Because we're never going to find these people. So there's a feeling of powerlessness sometimes.' (RS1, Focus Group 1)*

*'…it feels really frustrating that we can't get any further, we can't trace where these people are.' (RS4, Focus Group 1)*

*'… it's almost feeling powerless in yourself to actually advise properly on how you can help them.' (RS1, Focus Group 1)*

*'…you feel powerless.' (RS1, Focus Group 1)*

*'I just –you come across as incompetent and it just- they're coming to you for advice and help and then you just look like a –I'm always honest with people. I said, 'You'll have to forgive me, it's the first time I've come across it' (RS4, Focus Group 3)*

The frequent use of the word 'powerless' was a prominent feature of the focus group discussions, particularly in relation to bringing the perpetrators of such crimes to justice. There is a potential for such thoughts and feelings to bias officers approach to dealing with and processing these crimes, and if they believe there is little point in pursing such reports, this could have a variety of knock on effects, including aspects of under-reporting.

*The Contrast between the Speed at which Cybercrime Develops Versus the Speed of Investigation*

Within the focus groups, it became apparent that the participants had great difficulty keeping track of the development of cybercrime offences and the speed that cybercrime offences evolve. They noted that there is a constant change and new things come up all the time, from different techniques to new applications and social media platforms:

> *'…Yeah, it's like legal highs. They are constantly changing... ' (RS2, Focus Group 2)*

> *'But it's a constant thing, it's like you say. There's a new app that's come out now, the new social media, it's constant.' (RS1, Focus Group 3)*

> *'…something else is going to be a big thing in a minute and we're already outdated on that.' (RS1, Focus Group 2)*

> *'…because like two years ago Facebook was a bit thing, but now it's snapchat.' (RS1, Focus Group 2)*

*'…they're two or three levels ahead of us already, aren't they, these people? They know what's coming. They know where they're going.' (RS2, Focus Group 2)*

*'…because technology's moved on so quickly...' (RS4, Focus Group 2)*

*'..you think how far behind are we? We've not even thought that this is even possible and somebody's already doing it and they're already a step behind –step ahead and we just chasing and keep chasing till we get there, and there's nothing there.' (RS1, Focus Group 2)*

Many of the respondents focused directly on the speed of development in technology, and the constant drive to keep up with these changes. This is particularly evident in the quotation from RS1, Focus Group 2 who acknowledges this constant state of always being one step behind when in comes to being abreast of current threats from cybercrime:

The constantly evolving cyber threat landscape is sharply contrasted with the perceived speed at which participants seen the progression of investigations related to cybercrime:

*'and not only from handling the call in the first place, we then obviously make a decision on whether it's going to be a response to the job… cyber crime is more slower time at the moment…' (RS1, Focus Group 1)*

*'…there is nothing quick about investigating cybercrime…it's a slow thing.' (RS2, Focus Group 2)*

*'…criminals and crime now move a lighting speed, whereas we are still at snail's pace unfortunately.'*

*'It would take us a year to look at a known drug dealer's phone. It's pointless after a year; you might as well just not bother' (RS1, Focus Group 4)*

There is a consistent view that the investigation process sitting behind most cybercrimes is 'a slow thing' or progresses 'at a snail's pace'. It is unclear how the officers in these focus groups drew their evidence from which to base their opinions on the progress of such investigations, but the view was evident throughout all four of the focus group sessions.

*A Lack of Specialist Resources*

In the context of investigating cybercrime and dealing with contact from the public, a number of participants highlighted a clear lack of specialist resources devoted to such an issue. Many perceived this issues to be of critical importance, and felt that as the impact of cybercrime and the amount of time dealing with issues related to it were increasing, there had been a gradual reduction in officers with specialism in this area:

*'we're struggling.' (RS3, Focus Group 3)*

*'…So I think I ended up point-to-pointing someone because it was out of hours, it was weekend and I'm sure there are DMIs that are on or on call, but does that really warrant?..' (RS3, Focus Group 3)*

*'…We need SPOCs really, don't we? We need SPOCs on shift, on PRT, in MAU, in the control room, so someone who's always one and scattered it around that way really.' (RS3, Focus Group 3)*

*'……they reckon there's too many trained people, but there aren't enough.' (RS4, Focus Group 4)*

*'…of all our business have some kind of digital element and we've got five dedicate people.' (RS4, Focus Group 4)*

One of the participants in focus group 3 mentioned the concept of having a Single Point of Contact (SPOC) for aspects related to cybercrime who were attached to different departments within force headquarters. Individuals saw this as a more effective resource as they had someone they knew they could approach, irrespective of time of day, with their requests for information. The dedicated Digital Media Investigation team present within force headquarters were also mentioned as a noted resource, but even then they were seen as a time-limited resource, not available out of normal office hours. The requirement for having specialist officers who have advanced knowledge of cybercrimes has also been highlighted in previous research by Hinduja (2004). Officers in this study suggested that more advanced skills and knowledge in areas such as hacking, cracking, password protection, and encryption would assist them in cybercrime prevention. Although many forces are moving towards dedicated units to deal with the threat from cybercrime, it may also be worth exploring the potential to have dedicated SPOCs that operate in conjunction with such teams, but are accessible outside of office hours.

### *Lack of Effective and Consistent Training for Dealing with Cybercrime*

Overall, the participants shared little positive feedback about their training on cybercrime. Many referenced an online training system that was supplied by National Centre for Applied Learning Technologies (NCALT) in their discussions, whilst others claimed that they had received no formal training in the area, even though they were expected to deal with these types of enquiries on a day-to-day basis.

*Lack of Formal Training*

In discussion with the participants in the focus groups, it became apparent that very few of them could actually identify when and how they had received formal training related to aspects of cybercrime:

> *'I started in the IMU two years ago and I have had no training whatsoever in cyber crime; I am expected to pick it up as I go along. ' (RS2, Focus Group 2)*

> *'I haven't got a clue. I got it off my office-often from them team that taught me what to do in that role, but there's no formal training.' (RS4, Focus Group 2)*

> *'You do your two years probationary, you come out your training, you can now deal with everything that comes at you. ' (RS4, Focus Group 2)*

In the first extract, the participant noted that they had been in post for two years, but had received no formal training in how to deal with aspects of cybercrime. There is also an associated expectation that the officer was to learn about the area as they gained more

experience. Others expressed a similar experience, with participants claiming that they gained their knowledge through others on the team. This finding has some connection with findings from previous research by Hinduja (2004) who noted that many officers rated training in aspects of investigation and evidence gathering as being of critical importance in the context of cybercrime.

*Ineffectiveness of Online Training*

Nearly all of the participants had experience of using NCALT, and viewed it negatively in terms of its overall effectiveness as a learning platform for issues related to cybercrime. Participants made disparaging comments about the training, using words such as 'crap', 'rubbish' and 'boring'. These perspectives are demonstrated in the extracts presented below:

> *'…you know you're just going to have a bad time. It's not encouraging to do at all.' (RS1, Focus Group 2,r1,22)*

> *Int: 'Where did you get your training from?*
>
> *R4: NCALT*
>
> *R3: NCALT*
>
> *Is it effective?*
>
> *R3: It's rubbish.*
>
> *R2: It's not.*
>
> *(RS2, 3, and 4, Focus Group 3)*

> *'……Yeah, and it's to put a tick in a box.'*

*(RS4, Focus Group 3)*

*'I was going to say, it's usually online, rubbish' (RS2, Focus Group 4)*

*'Oh, is it NCALT? Which is the, yeah, worst thing ever.' (RS1, Focus Group 4)*

*'I think just about 90% of people would say that isn't a work- isn't something that works very well.' (RS4, Focus Group 4)*

*'…I mean NCALT is terrible because you're taught at basically and it's like you sit and you watch and that's it...' (RS2, Focus Group 4)*

*'It's not the way to learn.' (RS3, Focus Group 4)*

As can be seen, the effective of the NCALT system for specialised training related to cybercrime fell below par for many of the officers present in the focus group sessions.

Another aspect related to the perceived ineffectiveness of NCALT links into the fluidity of the area of cybercrime. NCALT is an e-learning platform that is designed and distributed to police officers, but appears not to be frequently updated. As a result, may of the participants saw the NCALT system as being out-dated and less informative:

*'NCALT is never going to be effective and I stand by this purely because – for cybercrime, at least that's for cybercrime, because it's always going to be out-dated. ' (RS1, Focus Group 2)*

*'…it's already dated because it's been developed three years ago, it's been put into production two years ago and it took a year to produce it so it's here now. So actually that product has been developed three years ago and we get training on ….. about how crime affects Facebook and Snapchat, by the time we get it, it's something else.' (RS1, Focus Group 2)*

*New offenses come up 'online has opened up a whole raft of different offences that never existed certainly when I joined'. (RS1, Focus Group 4)*

The effectiveness of e-learning platforms has come into question over recent years, particularly in the context of work-based education and training (Boulay, Coultas, & Luckin, 2008). A variety of mediating factors have been suggested to account for the effectiveness of such systems, including the level of computer literacy the individual learner has, alongside how well it provides a personalised experience (Birzina, Kalnina, Janevica, & Cernova, 2009), and motivational factors (Boulay et al., 2008). It would appear that many of the participants in the current study felt that the current NCALT system was out-dated and did not provide them with sufficient engagement to warrant their full engagement, hence limiting the actual retention of information. Many participants had the attitude that it was something that had to be done as quickly as possible in order to get it out of the way, with many stating that it had to be done in their own time.

***How to Increase the Effectiveness of Training?***

According to police officers, training should be more straightforward and to the point in order for it to be effective. They all noted that more interactive methods are needed for gaining a better understanding for cybercrime. In several instances they mentioned that having a real-life session with someone is far more effective than e-learning, which requires less involvement and connection with the learner. Police officers also mentioned that group discussions are helpful, as they provide opportunities sharing information, exchanging and debating information and issues:

*'Good examples would be nice.' (RS3, Focus Group 4)*

*'I think if you're in a group, you- like we are today, we're all bouncing off each other and that's why the conversation has not really sort of stopped…plus it keeps you awake a bit more, doesn't; it, that if you're like- then it's oh, it's like PowerPoint basically, it's just another screen.' (RS1, Focus Group 4)*

*'…and one of the training days we had cyber crime come in, only for literally an hour, bang, bang, bang, but they focused on smartphones.' (RS2, Focus Group 2)*

*'and that is a good example of teaching (focus group).' (RS1, Focus Group 4)*

*'…If you have something like that where you've got somebody who's engaging, really loves the job and wants to get it across to you...' (RS3, Focus Group 4)*

The effectiveness of security awareness campaigns, which has some analogy to the current area of training, has been explored in previous research (Bada, Sasse, & Nurse, 2014). The authors present a series of recommendations, with one of the key aspects being the education aspect has to be more that just presenting individuals with lots of information. The researchers suggested that education and training has to be 'targeted, actionable, doable, and provide feedback' (Bada, Sasse, & Nurse, 2014). Khan, Alghathbar, Nabi, and Khan (2011) found that academic presentations from guest speakers or group-based discussions had the greatest potential to enhance knowledge and attitudes towards aspects of cybersecurity. In contrast emails, newsletters, and computer-based training all had limited effectiveness (Khan, Alghathbar, Nabi, and Khan, 2011). These elements could be taken on board in terms of developing more effective and robust training for frontline officers who have to deal with aspects of cybercrime on a daily basis.

**Conclusion**

The current work aimed to explore the perceptions, attitudes, and challenges a group of front line police officers faced in dealing with cybercrime. This work is seen as a critical starting point from which to build a wider discussion about the issues raised, and focuses directly on the experiences of frontline officers rather than academic-based interpretations.

The work is of critical importance for a variety of reasons, particularly as forces are expected to present an agile and response position in the context of growing cyber-threat. The key issues highlighted in this study surround the effectiveness of understanding the terminology related to cybercrime. If officers have a clearer understanding of the key facets related to cybercrime,

they could ensure that potential victims of such attacks can be supported effectively, as well as ensuring relevant evidence is collected in line with accepted protocols. It is clear that many officers have experienced a degree of frustration or sense of powerlessness when it comes to dealing with cybercrime, which again needs to be tackled at both an individual and organisational level. Motivation through more effective training techniques, as well as a clear pathway to measure the effectiveness of such, would appear to be the most salient solution for such an issue. Key mechanisms to achieve this could involve the development and use of more immersive education techniques, or more specific training being given by experts in the field of cybercrime. This element has been echoed in previous work exploring the effectiveness of cyber security training, showing that professionally organised and prepared training is the most effective (Bada et al., 2014). Many of the participants in the current study focused on the lack of clear training methods for cybercrime awareness. Where such training did exist, it was viewed as being ineffective, boring and disengaging, limiting the capacity for actionable knowledge to be imparted.



**References**

Bada, M., Sasse, A. M., and Nurse, J. R. C. (2014). Cyber Security Awareness Campaigns Why do they fail to change behaviour ? *ISSN*, (July), 118–131.

Birzina, P. R., Kalnina, D., Janevica, J., and Cernova, E. (2009). Effectiveness of interactive e-learning organization and quality assurance in European interuniversity master studies. *European Conference on Education Research*, 1–16.

Bossler, A. M., and Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management*, *35*(1), 165–181.

Boulay, B., Coultas, J., and Luckin, R. (2008). How compelling is the evidence for the effectiveness of e-Learning in the post-16 sector?, (January), 1–145.

Braun, V., and Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Burns, R. G., Whitworth, K. H., and Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice*, *32*(5), 477–493. https://doi.org/10.1016/j.jcrimjus.2004.06.008

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies & Management*, *27*(3), 341–357. https://doi.org/10.1108/13639510410553103

HM Government. (2016). *National Cyber Security Strategy*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Holt, T., Bossler, A., and Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Oxon: Routledge.

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. https://doi.org/10.1089/cyber.2011.0625

Khan, B., Alghathbar, K. S., Nabi, S. I., and Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862–10868. https://doi.org/10.5897/AJBM11.067

McGuire, M., and Dowling, S. (2013). *Cyber crime : A review of the evidence Research*. *… of key*

*findings and implications. Home …*. Retrieved from https://www.gov.uk/government/uploads/.../246751/horr75-chap1

National Crime Agency. (2016). NCA Strategic Cyber Industry Group Cyber Crime Assessment 2016 Need for a stronger law enforcement and business partnership to fight cyber crime, (July), 1–16.

Wall, D. (2001). *Crime and the Internet*. (D. Wall, Ed.). London, UK: Routledge.

Wall, D. (2007). *Cybercrime: The transformation of crime in the Information Age*. Cambridge: Polity Press.

Wall, D. S. (2007). *Cybercrime: The transformation of Crime in the Information Age*. Polity.

Wall, D. S. (2008a). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime1. *International Review of Law, Computers & Technology*, *22*(1–2), 45–63. https://doi.org/10.1080/13600860801924907

Wall, D. S. (2008b). Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge About Cybercrime. *Information, Communication & Society, 11*(August 2010), 861–884. https://doi.org/10.1080/13691180802007788