Safer & Stronger
Communities Board

22 February 2016

Cyber-crime – LGA work plan

Purpose

For discussion and direction.

Summary

This paper updates the Board on LGA work to support councils in preparing for and dealing with the threat posed by cyber-crime.

Recommendations

Members are asked to:

(a) discuss the proposed approach from the Board set out in paragraphs 11 to 16, and

(b) agree the activities outlined in them as part of the wider programme of work on cyber-crime.

Action

Officers to take forward as directed.

Contact Officer:	Ellie Greenwood
Position:	Senior Adviser (Regulation / Community Safety)
Telephone No:	020 7664 3219 / 07795 413 660
Email:	ellie.greenwood@local.gov.uk

Safer & Stronger Communities Board

22 February 2016

Cyber-crime – LGA work plan

Background

1. Although the latest crime figures for England and Wales published in January show that crime has continued to decline in the year to September 2015, it is argued that partly this is because the nature of crime is changing. One area where crime is felt to be increasing is cyber-crime.

2. While national statistics on the level of cyber-crime will not become available until the summer of 2016, a field trial conducted in 2015 by the Office of National Statistics suggested there were 2.5 million incidents of crime in the year to the trial falling under the Computer Misuse Act, such as where a computer had been infected with a virus or where emails or social media accounts had been hacked.

3. This level of crime should not be surprising when 12.4 per cent of all retail sales were made online in the UK in 2015, with over £700 million being spent online by UK consumers each week.

4. Cyber-crime is therefore identified as a high-level threat in both the National Security Strategy and the 2015 Strategic Policing Requirement. The National Crime Agency has a specific unit to lead the UK's response to cyber-crime, and National Trading Standards (NTS) has established an e-crime team to protect consumers and businesses from internet crime and online fraud. At its meeting in September 2015, the Board also indicated an interest in a workstream to support councils to deal with the threat of - and harm caused by – cyber-crime.

5. Officers have subsequently liaised with other teams in the LGA examining this issue, as well as SOLACE and the NTS e-crime team, to explore how our efforts can be targeted most effectively.

Forms of cyber-crime

6. Supporting councils on this agenda is complicated by the fact that cyber-crime covers a range of offences and activity. For a number of years cyber-crime has been divided into two types; cyber-dependent crime and cyber-enabled crime.

7. Cyber-dependent crime can only be committed using computers and other forms of communication technology, and involves activity such as denial of service attacks on networks or servers, hacking and spreading malware. This crime is primarily directed against computers and networks.

8. Cyber-enabled crime refers to traditional forms of crime which have been transformed by the use of computers in terms of their scale and reach such as fraud (for example mass-marketing frauds, 'phising' emails, e-commerce frauds), theft (including theft of personal information), sexual offending and harassment.

Issues

9. There is a range of work already ongoing to support council awareness of and resilience to the threat of cyber-crime.

   9.1. CLG, in conjunction with the National Cyber Security Programme have been running a series of free Local Leadership Seminars aimed at senior local government and local resilience forum colleagues to highlight the important of cyber resilience across localities to deal with cyber-attacks.

   9.2. These events have been promoted by SOLACE, with the organisation also planning further work to raise the knowledge and skills of its members in this area by:

      9.2.1. Launching a survey of members to see what type of support in the area of emergency planning and cyber resilience would be most effective.

      9.2.2. Producing a short best practice guide for new chief executives and senior managers to provide a checklist of what they need to know about resilience and emergency planning (specifically focusing on cyber resilience).

      9.2.3. Taking part in a CLG cyber resilience event to discuss the leadership framework and future sector leadership options around civic cyber resilience.

   9.3. The LGA productivity team is also working with CLG and will be holding an event on reducing councils' exposure to cyber-attacks, in Spring 2016.

10. In light of this ongoing activity, officers sought a view from NTS's national e-crime team as to how the LGA could usefully support its work to tackle cybercrime. The team, which operates out of North Yorkshire County Council, leads national trading standards activity on cybercrime, and acts a centre of excellence for the rest of the sector.

11. The e-crime team highlighted two areas where it would be helpful to have LGA support:

   11.1. **Continuing to make the case for council access to communications data**. The team emphasised the increasing importance of trading standards teams being able to access communications data given the rising proportion of trading standards cases involving the internet and social media. Facebook and increasingly other apps such as Whatsapp, Instagram and so forth are being used to sell fake and counterfeit goods, such as cigarettes, alcohol, fireworks, unsafe toys/cosmetics/electrical items etc. It is considerably harder for trading standards teams to tackle this than it is to address the sale of counterfeit goods in a local market; without access to types of communications data, it would be virtually impossible.

   11.2. A related point is the need to **support training for council officers in relation to conducting investigations on social media**. This extends beyond trading standards work; social media is regularly used as a source of intelligence and investigation across regulatory services, education and social care, and has implications for wider community safety issues such as counter-extremism, modern slavery, violence against women and girls, child sexual exploitation, harassment and other forms of anti-social behaviour, as crimes are increasingly facilitated by the internet. However, in accessing social media, officers need to be aware of the regulatory requirements (and risks) around conducting what could be classified as surveillance, as well as of wider good practice. The e-crime Team has developed and delivered a basic social media course, which received expressions of interest from staff outside of TS, but believe there would be widespread take up of the course if it could be transferred onto an e-learning platform.

12. The Joint Committee scrutinising the draft Investigatory Powers Bill, which will govern access to communications data, published its report on 11 February. The report recognises the need for councils to be able to access communications data in order to support their law enforcement roles. Given that as recently as 2013 government had proposed to withdraw this access, this is an important acknowledgement that reflects repeated and coordinated lobbying on this point by the LGA, National Anti-Fraud Network, Chartered Trading Standards Institute and others.

13. However, the position is not yet secure. Despite finding that concerns about council use of communications data were unfounded, the Joint Committee nevertheless recommended that Parliament give further consideration to defining the purposes for which local authorities may be allowed to apply for communications data when the Bill is introduced. Large sections of the media and many Parliamentarians are deeply hostile to councils retaining access to communications data (due to isolated misuse of related, but separate, surveillance powers several years ago), despite the additional safeguards and restrictions councils are subject to. The LGA will need to continue lobbying on this issue, setting out how councils use this data appropriately, to ensure that access is preserved as the Bill progresses through Parliament.

14. On the social media training, officers have held further discussions with the e-crime team to find out more about the proposed training. It is intended that the training would copy the model of a similar course developed to provide basic level internet investigations training for officers who have limited knowledge of online investigations. The format of the training is a series of online, filmed modules taking participants through each section.

15. The team believe a similar method could be used to develop and roll-out training on social media, the Regulation of Investigatory Powers Act and Investigatory Powers Bill /Act. The team has already developed much of the content for this training, having delivered a training course on this for a group of trading standards officers.

16. Officers have established that the LGA is in a position to financially support the development of this training, in line with our business objective of using a proportion of RSG funding to '*support opportunities for councils and the police to work together more effectively on reducing crime in key areas*.' Subject to the views of the Board, it is hoped that funding can be released quickly to enable the development of a training package by summer 2016.

Next steps

17. Members are asked to:

    17.1. Discuss the proposed approach from the Board and agree the activities outlined above as part of the wider programme of work on cyber-crime.

Financial Implications

18. Funding for the work proposed has been secured from within existing budgets.