CYBERCRIME TIPPING POINT

Public perceptions

CONTENTS

FOREWORD

Chief Constable Stephen Kavanagh
Chief Constable, Essex Police
Lead for Digital Investigation and Intelligence (DII)

"Crime is moving online. The recently published Office for National Statistics crime survey shows that fraud and cybercrime between them account for as many offences as traditional offline crime combined.[1] The daily media focus on cybercrime, of which TalkTalk is just the latest and most high profile example, shows the way in which demand on policing is changing.

Policing is adapting to ensure it is able to respond to this shift. More officers are being trained in online investigation and there is investment in new capabilities despite the challenging resource environment for policing as a whole.

Through National Police Chiefs Council, the College of Policing and National Crime Agency we are co-ordinating our efforts more closely and have a really compelling programme underway to equip policing with the skills, knowledge and capabilities needed to police the digital age.

This study adds to the picture about changing public expectations and helps us recognise the areas where we need to do more, particularly in helping protect and prevent as well as pursue those responsible for digital and cybercrime."

November 2015

[1] Office for National Statistics (2015) 2014/15 Crime Survey for England & Wales.

EXECUTIVE SUMMARY

Carl Roberts
Security and Policing Expert
at PA Consulting Group

“Our latest survey shows that the demands on, and expectations of, the police in tackling cybercrime are set to grow significantly. This is being driven by the emergence of a new generation, characterised by their lifelong exposure to the internet and digital media (dubbed ‘Generation Z’). Police forces will need to balance this new demand with the need to continue to tackle crimes carried out in the real world. They will also have to continue to provide reassurance to older generations and find new ways of working with industry to tackle the threat.

The Office for National Statistics estimated that there were 2.5 million cybercrimes between mid-2014 and mid-2015. PA's first tipping point survey presented the views of police analysts on how they need new digital capabilities to respond to this threat from cybercrime.[2]

However, any new operating model should also be based on an understanding of the needs and expectations of its customers. It is here that we have found a gap in understanding about what the public really expects from the police in relation to cybercrime.

This survey aims to address this gap. We surveyed over 1,000 British citizens about their views on cybercrime. In particular, we asked what they are most concerned about, how they expect the UK law enforcement community to respond, and where they believe resources should be focused.

The findings provide many valuable insights around how the police should shape and develop new capabilities. Most prominently, these include the diverse expectations from different generations that will place new demands on the police. We also found an expectation that service providers should be working alongside national police forces to lead the response. There was a high level of confidence in policing to counter the threat but much lower levels of satisfaction once someone had been a victim of cybercrime when compared to satisfaction levels relating to crimes in the real world.

Over the following pages we share the findings of our survey and make several recommendations. Taken together, these will help law enforcement agencies and other relevant organisations (for example Internet Service Providers (ISPs)) develop a collaborative and effective approach to tackling cybercrime and exploiting digital opportunities. This will help them better address the concerns and expectations of the British public.”

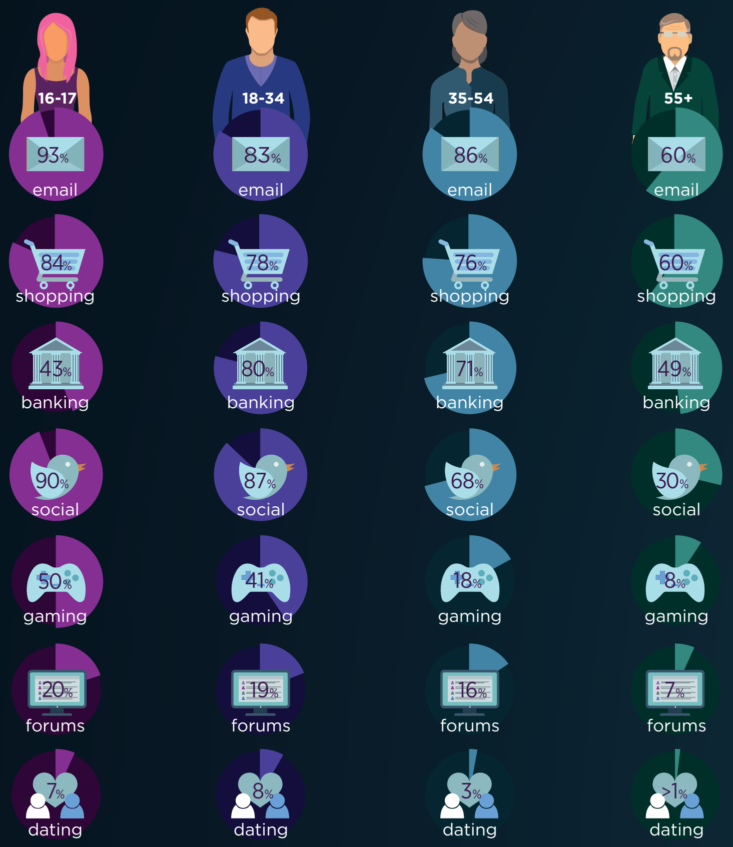
Each age group has different opinions about cybercrime

16-17
Most likely to be affected
18-34
Least concerned but least confident in police response
35-54
Likely to be affected but remain confident in police response
55+
Less vulnerable, but more concerned

[2] PA Consulting (2014) Cybercrime Tipping Point.

EXPERIENCE OF DIFFERENT GENERATIONS

Generations have different levels of exposure to the internet that shape their susceptibility and concerns about cybercrime



EACH GROUP HAS DIFFERENT EXPERIENCES OF THE INTERNET AND CONCERNS ABOUT CYBERCRIME

Internet usage varies

Our survey has reinforced perceptions that the use of the internet, and therefore someone's potential experience of cybercrime, varies significantly by generation.

We have characterised these generations by age bracket:

Over 55s who use the internet less than every other generation, although more than half of these respondents still use it for shopping and email.

Generation X: 35- to 54-year-olds who grew up without the internet but now use it throughout their lives, although still slightly less than younger generations.

Generation Y: 18- to 34-year-olds who have mostly socialised and worked in environments where the internet is a normal feature.

Generation Z: 16- to 17-year-olds dubbed the 'digital natives', and characterised by their lifelong exposure to the internet and digital media.[3] Our survey found that 90% of 16- to 17-year-olds use social media, 84% do their shopping online, and 7% use online dating services.

Younger generations represent the highest risk groups for cybercrime

Our survey results indicate that users who spend the most time online are more likely to become a victim of, or be affected by, online crime. Crime statistics repeatedly confirm that 16- to 24-year-olds constitute the highest proportion of victims and offenders in our society.[4] Generation Z is therefore entering a high-risk phase, as their internet-centred lifestyle creates an additional environment through which they could become victims of the next generation of cyber criminals.

[3] Schmidt, L and Hawkins, P. (July 15, 2008) "Children of the tech revolution". Sydney Morning Herald, 15 Jul. Available from: http://www.smh.com.au/news/parenting/children-of-the-tech-revolution/2008/07/15/1215887601694.html [Accessed 25/09/2015].

[4] Office for National Statistics (2013) 2012/13 Crime Survey for England & Wales.

The older generations are most concerned about cybercrime

While younger generations use the internet more frequently and are exposed to more online crime, our survey revealed that concern about all aspects of cybercrime significantly increases from the 18-34 age group, with the over 55s most concerned about cybercrime.

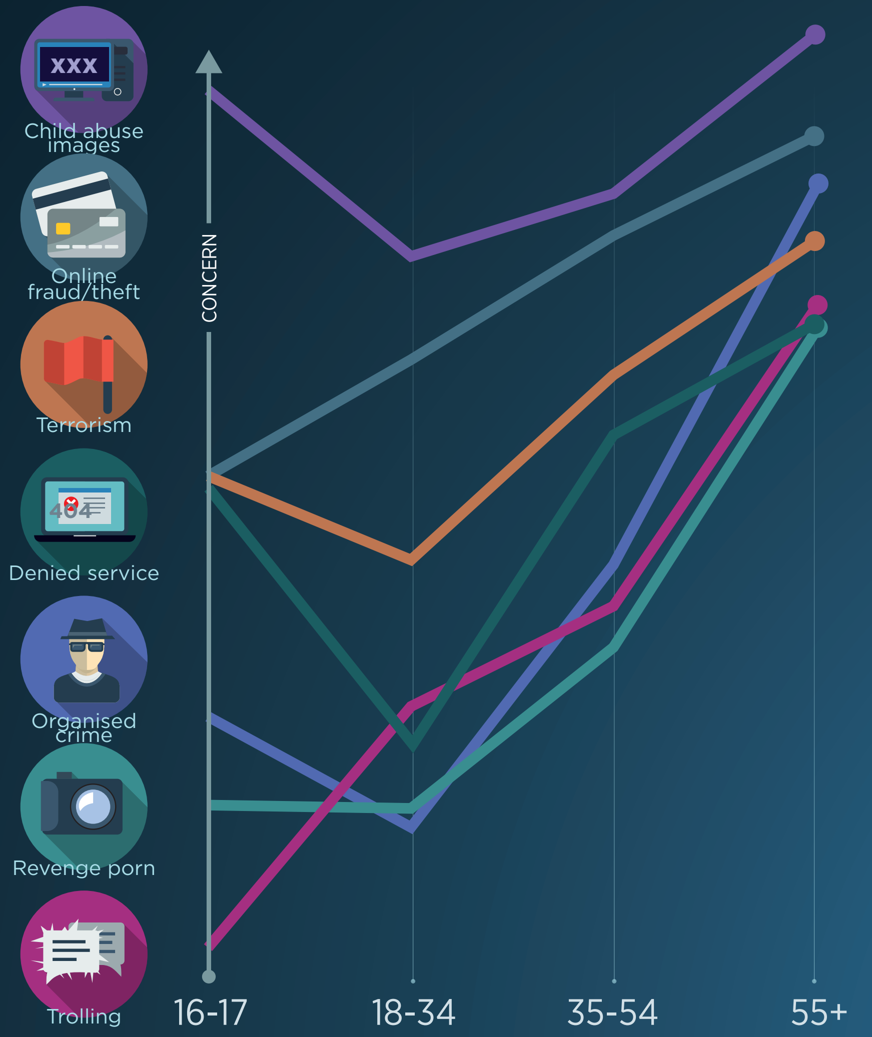
Across generations, child abuse images and online theft or fraud are the areas that prompted the most concern from the public.

Generation Z are more concerned about some types of cybercrime

With the exception of trolling and online fraud, Generation Z were more concerned than the 18-34 age group about denial of service attacks, child abuse images, organised crime and terrorism.

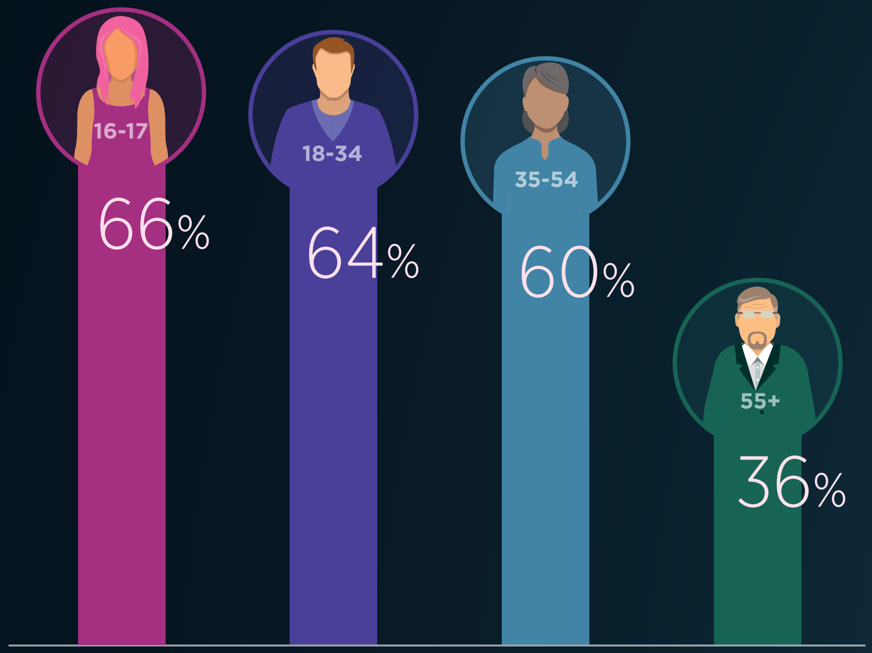
Interestingly, Generation Z participants were the group least concerned about revenge porn and trolling (despite being the group most affected by the latter), which indicates a degree of indifference to these crimes.

Public concerns about cybercrime differ by age group



PUBLIC EXPERIENCE AND EXPECTATIONS

Younger people are most vulnerable



Percentage of respondents who have been affected by cybercrime

EXPECTATIONS OF LAW ENFORCEMENT VARY BASED ON THE TYPE OF CRIME COMMITTED ONLINE

Over 50% of the public have been affected by cybercrime

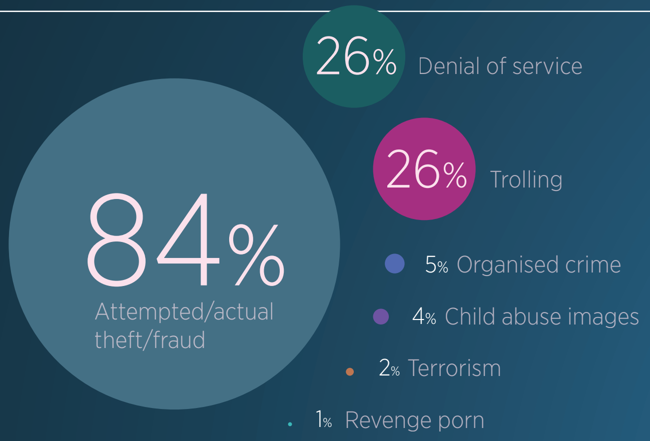
More than half (53%) of those surveyed had been personally affected by cybercrime. Of these, the vast majority have experienced online fraud (84%). Younger people are the most vulnerable to cybercrime, with 66% of 16- to 17-year-olds reporting that they had been affected by cybercrime, compared to just 36% of over 55s.

A quarter of victims had been affected by abuse or threatening behaviour and denial of service attacks, for example the attack on Microsoft Xbox servers during Christmas 2014.

Trolling (the use of threatening or abusive language online) is by far the most common crime affecting Generation Z, with 46% of respondents in this group reporting they had been affected.

This compared with 25% of 18- to 34-year-olds, 10% of 35- to 54-year-olds and just 5% of those over 55.

Fraud/theft is the most common form of cybercrime



Percentage of types of crimes that have affected victims of cybercrime in our survey.

*Each respondent had the option of selecting multiple crimes.

CYBER CRIME

TIPPING POINT

PUBLIC EXPECTATIONS

Half of the population are affected

53% of the public have been affected by cybercrime, **84%** of these incidents were online fraud

Underreporting is an issue

Only **30%** of people have reported cybercrime

Local police aren't expected to play a leading role

instead this expectation is on **internet service providers** for minor crime

and **national policing functions** for more serious crimes

EXPERIENCE OF DIFFERENT GENERATIONS

The internet plays a much greater part in Generation Z's lifestyle.

100% vs **70%** aged **55+**

of **16-17** year-olds use the internet

Generation Z want more emphasis put on tackling cybercrime

43% of Generation Z want more focus put on cybercrime and less on real-world crime

Generation Z are more likely to be victims of online crime

50% have been affected by trolling, but few have expressed concern

Older generations are less affected by cybercrime but feel more vulnerable

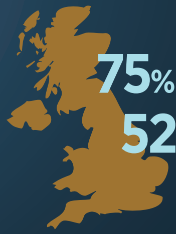
44% of **16-17** year-olds are concerned about cybercrime vs **70%** of **55+** year-olds

CONFIDENCE & SATISFACTION

Public perception of law enforcement capability exceeds reality

59% think the police are more advanced than cyber criminals

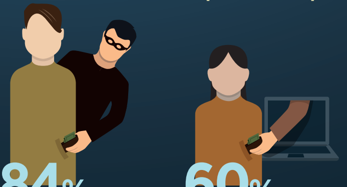
Confidence varies regionally



75% confidence in the North East

52% confidence in West Midlands and East

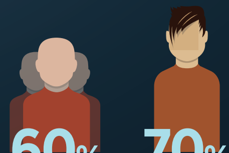
Victims of cybercrime are less satisfied with the police response



84% satisfaction among victims of real-world crime

60% satisfaction among victims of cybercrime

Generation Z have more confidence in law enforcement



60% overall confidence

70% Generation Z confidence

THE PUBLIC EXPECT A NATIONAL RESPONSE TO CYBERCRIME

Under-reporting of cybercrime masks the full scale of the threat

The responses suggest that cybercrime is rarely reported. Only 30% of respondents said they had reported a cybercrime to the police, which indicates a substantial level of under-reporting when compared with the 53% who said that they had been affected by cybercrime.

The public expect Internet Service Providers (ISPs) to deal with less serious crimes, but believe national policing should lead on the more serious crimes

Senior figures in intelligence and law enforcement agencies have made public calls for ISPs to do more to help prevent criminals exploiting the internet.[5] Our survey found public support for this approach for certain types of crimes.

For trolling and denial of service attacks, action by ISPs appears to be preferable to law enforcement involvement. Respondents also felt that ISPs had a leading role to play in responding to online fraud and revenge porn.

However, there is an expectation that national policing (e.g. the National Crime Agency) will lead the response to the most serious crimes such as child sexual exploitation and organised crime.

Limited expectations of local policing

With the exception of trolling, respondents did not think local policing had a major role to play in any cybercrime response. This is likely to reflect a growing awareness that cyber criminals typically operate beyond the boundaries of county forces. There are however preventative outreach activities that local police can deliver to build awareness and resilience to cybercrime. For example, in West London volunteer police cadets ran a series of workshops with older residents of the area to help them identify scams and fraudulent emails or websites.[6]

Type of cybercrime	Who should respond? (top two most popular responses)	
Abusive/threatening language	ISP	LOCAL POLICE
Child abuse images	NATIONAL POLICING	LOCAL POLICE
Attempted/actual online fraud/theft	NATIONAL POLICING	ISP
Denied service attacks	ISP	NATIONAL POLICING
Organised crime	NATIONAL POLICING	SECURITY AGENCY
Revenge porn	NATIONAL POLICING	ISP
Terrorist recruitment, propaganda or knowledge sharing	SECURITY AGENCY	NATIONAL POLICING

'National policing' can include NCA, new national cybercrime units or other national policing functions

[5] BBC (2015) "MI5 boss warns of technology terror risk" BBC Online, 17th Sept. Available from: http://www.bbc.co.uk/news/uk-34276525 [Accessed 20/10/2015].

[6] Metzger, M. (2015) "West London police spearhead cyber-crime initiative" SC Magazine, 14 Sept. Available from: http://www.scmagazineuk.com/west-london-police-spearhead-cyber-crime-initiative/article/438303 [Accessed 20/10/2015].

Most people think the balance between the response to cybercrime and real crimes is about right

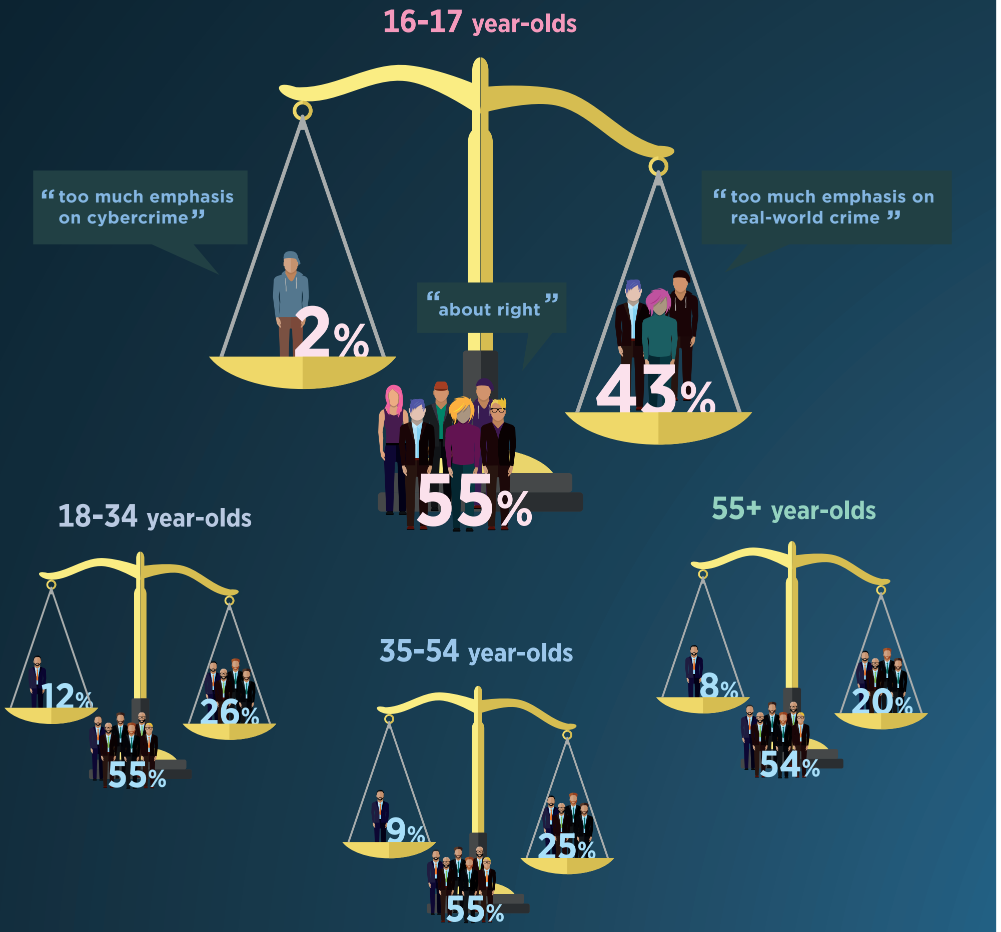
With shrinking budgets and other competing demands, government and the law enforcement community are trying to balance the need to deal with traditional, real-world crimes along with cybercrime. This was highlighted when the head of the National Police Chiefs' Council said, in July 2015, that "We need to move from reacting to some of those traditional crimes to think about focusing on threat and harm and risk and protecting the public", which she felt included cybercrime.[7]

Our survey has found that the majority of respondents think the police have the right balance between the time and money spent on tackling crimes that happen in the real world compared to those that happen online, or cybercrime.

Younger generations are likely to expect more focus on cybercrime

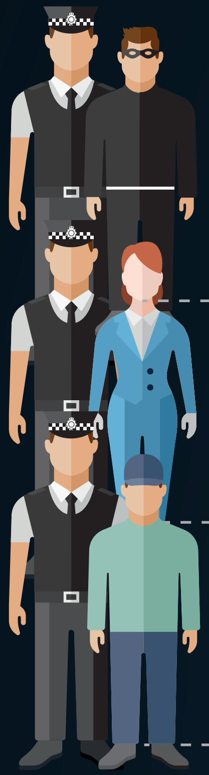
The proportion of respondents who thought that too much emphasis was put on crimes in the real world was greatest in the younger age groups. 43% of 16- and 17-year-olds thought there was too much emphasis put on tackling crimes in the real world, compared with just 2% who felt too much emphasis was put on dealing with online crimes.

More respondents in the younger generations expect a greater focus on cybercrime from the police



[7] BBC (2015) "Sara Thornton: Police may no longer attend burglaries", BBC Online, 28 July. Available from: http://www.bbc.co.uk/news/uk-33676308 [Accessed 20/10/2015].

CONFIDENCE AND SATISFACTION



% of respondents who felt that the police have better cyber capability...

THAN **CYBER CRIMINALS:** 59%

THAN **BUSINESSES:** 68%

THAN **THE PUBLIC:** 72%

THERE IS A POSITIVE PERCEPTION OF LAW ENFORCEMENT'S CAPABILITY TO TACKLE CYBERCRIME

We asked respondents how they thought police cyber and digital capabilities measured up against those of criminals, business and the general public. Most had a favourable view of police capability.

A total of 59% of respondents thought the police were the same as or more technologically capable than cyber criminals, and 68% thought they were more capable than businesses.

Nearly three-quarters (72%) believed the technical capabilities of the police were at least as good as those of the public, with 50% holding the view that the police had more advanced skills.

In reality, the technical capabilities available to the police often lag behind those in the commercial sector due to budget constraints and the need to trial new technology to assess its suitability for police use.

For instance, the police require a more robust telephone handset with longer battery life than commercial consumers. So while consumers have had access to smartphones since 2007, the majority of police forces did not start issuing them until 2010.[8]

However, confidence in the police's ability to tackle cybercrime is lower than for crimes committed in the real world.

While 60% of survey respondents said they are confident in the police's ability to investigate and tackle online crime, this remains lower than public confidence in the police's ability to catch criminals in the real world (68%).[9]

Generation Z, who have grown up watching 24's Jack Bauer exploit technology to catch the perpetrators, had the most confidence in the police's ability to tackle cybercrime (70%). Interestingly, overall public confidence in police ability to tackle real-world crimes follows the opposite pattern. This confidence tends to increase with age (with 16- to 24-year-olds being the least confident).[10]

[8] RUSI (2014) Emergency Services Communications: Resilience for the 21st Century.

[9] ONS (2015) Crime Statistics, Focus on Public Perceptions of Crime and the Police, and the Personal Well-being of Victims, 2013 to 2014.

[10] Ibid.

SATISFACTION AMONGST CYBERCRIME VICTIMS IS LOWER THAN FOR CRIMES IN THE REAL WORLD

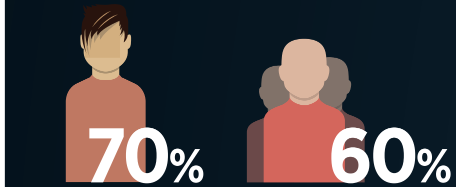
Of those surveyed who had reported a cybercrime, 60% were satisfied with the police response. While this figure is positive overall, it is much lower than the national satisfaction rate for victims of real-world crime (where 74% of victims were "very" or "fairly" satisfied with the police response).[11]

Confidence in law enforcement's ability to prevent and investigate online crime declines in individuals who have been a victim.

Confidence in the police fell slightly from 63% among those not personally affected by cybercrime, to 58% confidence among those affected by cybercrime.

Similarly, the public's perception of the technical capabilities of the police in comparison to cyber criminals and businesses fell among those who had been affected by cybercrime.

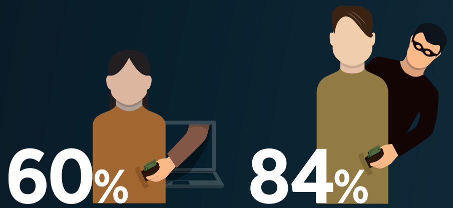
Generation Z have more confidence in law enforcement



70% Generation Z confidence

60% overall confidence

Victims of cybercrimes are less satisfied with the police response

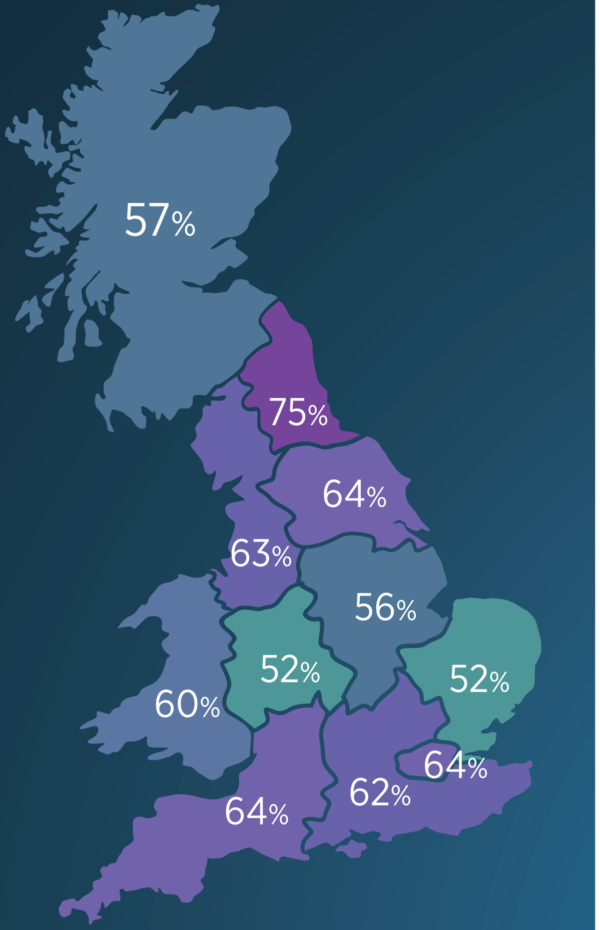


60% satisfaction amongst victims of cybercrime

84% satisfaction amongst victims of real-world crime

CONFIDENCE VARIES REGIONALLY

The pattern of confidence in police capabilities varies regionally across the UK. The North East is by far the most confident, at 75%, compared to much lower ratings in the East of England and West Midlands (52%). This pattern does not correlate with patterns of cybercrime found in this study. For instance, the East of England is an area with one of the lowest rates of cybercrime (46%), but also has one of the lowest levels of public confidence in the police's ability to tackle cybercrime (52%). The reasons for this are unclear and are worthy of further exploration.



[11] ONS (2015) Crime Statistics, Focus on Public Perceptions of Crime and the Police, and the Personal Well-being of Victims, 2013 to 2014.

RECOMMENDATIONS

This survey has explored the public perceptions and expectations of law enforcement in relation to cybercrime. As the law enforcement community and Home Office take forward new initiatives to build digital capabilities to counter the rising trend in digital and online crimes, the response should focus on the needs of the public that they serve. The results from this survey suggest that these initiatives need to address four areas in relation to public perceptions.

Clarifying responsibilities – new operating models for the police response need to make clear who is responsible for preventing and detecting different types of digitally-enabled and cybercrimes at local, regional and national levels.

Supporting victims – the victims of cybercrimes should be offered the same type of local support as they would expect if they had been subject to a burglary, theft or assault. This is also an opportunity to provide preventative advice to reduce the risk of further crimes.

Partnerships with industry – the public don't just see cybercrime as something for the police to respond to. They expect internet service providers to take a leading role in responding to and preventing cybercrimes that are enabled by the ISPs network infrastructure and communications applications. Successful initiatives such as WePROTECT, that stimulated a cross-industry response to tackling online child sexual exploitation, should also be considered for other types of crimes.

Engaging the younger generations – the law enforcement community needs a fresh approach to public engagement, designed to understand and meet the expectations of an emerging generation of 'digital natives'; otherwise they risk alienating entire segments of society.

Two key recommendation of PA's first Cybercrime Tipping Point survey[12], published in December 2014, were that:

- There needs to be a concerted and nationally coordinated effort to improve the measurement and analysis of cybercrime data, in order to improve the understanding of threats and the ability to spot efficiency opportunities where duplication in investigations exist
- To secure legislative change, police and agencies will need to explain the capability gap better; provide assurance that the acquisition and use of communications data is proportionate; and demonstrate they will be held properly to account through independent and transparent scrutiny.

We welcome the new approach to crime recording by the Office for National Statistics[13], which has begun to address this data gap, and the improved clarity on investigatory powers in the report by David Anderson QC, following his independent review of counter-terrorism legislation[14], echoed in the RUSI-chaired Independent Surveillance Review[15]. However, we note that progress has been far slower in relation to our other recommendations.

PA continues to work with national policing leads in the UK to help develop their capability and capacity to address digital investigations and intelligence.

ABOUT THE SURVEY

Populus interviewed a random sample of 1,034 GB adults aged 16+ by in June 2015. Surveys were conducted across the country, with quotas set on age, gender and region. The results have been weighted to the known GB profile of age, gender, region, social grade, whether they had taken a foreign holiday in the last 3 years, tenure, number of cars in the household, working status, and mobile only household.

Due to the nature of the topic, opinions were collected both from people who are connected to the internet and those who are not. A survey conducted over the telephone afforded the opportunity to reach both of these groups. 50% of the sample was contacted via landline and 50% via mobile to ensure that the correct proportion of mobile only households was achieved.

To reach the Generation Z cohort, an additional 30 interviews were conducted with 16 and 17 year olds and the number of interviews is representative of this age group among the population.

Populus is a founder member of the British Polling Council and abides by its rules. Further information at www.populus.co.uk.

For more information please contact:

Carl Roberts, PA Security and Policing Expert, **carl.roberts@paconsulting.com**.

Nick Newman, PA Security and Policing Expert, **nick.newman@paconsulting.com**.

Owen Gillard, PA Security and Policing Expert, **owen.gillard@paconsulting.com**.

[12] PA Consulting (2014) Cybercrime Tipping Point.

[13] ONS (2015) Fraud and Cyber-crime Development: Field Trial.
[14] Anderson, D. (2015) A Question of Trust: Report of the Investigatory Powers Review.
[15] RUSI (2015) A Democratic License to Operate: Report of the Independent Surveillance Review.

CONSULTING
TECHNOLOGY
INNOVATION

We Make the Difference

An employee-owned firm of over 2,500 people, we operate globally from offices across the Americas, Europe, the Nordics, the GCC and Asia Pacific.

We are experts in energy, financial services, life sciences and healthcare, manufacturing, government and public services, defence and security, telecommunications, transport and logistics.

Our deep industry knowledge together with skills in management consulting, technology and innovation allows us to challenge conventional thinking and deliver exceptional results that have a lasting impact on businesses, governments and communities worldwide.

Our clients choose us because we do not just believe in making a difference. We believe in making the difference.

Corporate headquarters

123 Buckingham Palace Road
London SW1W 9SR
United Kingdom
+44 20 7730 9000

paconsulting.com

This document has been prepared by PA. The contents of this document do not constitute any form of commitment or recommendation on the part of PA and speak as at the date of their preparation.