HMICFRS

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services

Cyber: Keep the light on

An inspection of the police response to cyber-dependent crime

October 2019

© HMICFRS 2019

ISBN: 978-1-78655-900-5

www.justiceinspectorates.gov.uk/hmicfrs

Contents

Foreword

There are few aspects of everyday life that have not been affected by the development of digital technology. It has transformed how we spend our leisure time, socialise with family and friends, and go about our daily lives. Very few businesses, from large multinational organisations to small cottage industries, would be able to function without it.

In many ways we are reliant on technology to function, both as individuals, and as a wider society. This reliance presents an opportunity for those criminals who, for monetary, ideological or personal reasons, may seek to attack those devices on which we all rely. At one extreme, this could involve holding elements of the national infrastructure to ransom, or, at the other, the unauthorised accessing of a person's private accounts to bully and intimidate.

As a result, it is vital that all law enforcement agencies involved in the response to cyber-dependent crime work together efficiently and effectively. And – particularly at the national and regional level – they do.

We found positive examples of senior leaders working closely across agencies, industry and government departments to build strong partnerships and effective working relationships. This has resulted in the development of a network of staff, which, on a daily basis, keeps people safe.

At a local level, the development of a similar ability to respond to this modern threat has been slower. But, once again, strong national strategic leadership has worked to secure central government funding designed to stimulate activity.

In doing so, national leaders have also been able to establish the importance of having minimum standards of capability and nationally recognised performance indicators. We do not underestimate this achievement.

So, in general, we found a positive picture. But challenges remain.

Firstly, we found that, in some cases, the development of local units has become a potential source of inefficiencies, which include:

- variation in how nationally agreed structures and processes are applied;
- little understanding of demand among forces, leading to duplication of effort or, in some cases, a lack of capability in some roles such as analysts; and
- the potential for regional and local resources to be diverted from the response to a national threat.

All of these bring inconsistency, which assists those that commit this type of crime. Those criminals give little attention to international, national, and regional borders. They pay even less to those that mark where the area of one police force finishes and another starts. It is important that there is a consistent and co-ordinated response.

Secondly, the funding that has been made available will soon come to an end. In too many cases we found that forces had yet to establish clear plans on how – or whether – they were going to maintain their ability to respond to cyber-dependent crime.

This equally applies to some national agencies that are dependent on this additional funding. In one unit we were told that staff could only hope that, after the funding ceased, there would be someone left who could “keep the lights on”.

The threat is too great to be left to chance.

Summary

The Home Secretary commissioned Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) to carry out this inspection of the police response to cyber-dependent crime. The inspection took place between April and June 2019.

There now follows a 14-page summary of our findings followed by our recommendations and identified areas for improvement.

What we assessed

We inspected the effectiveness and efficiency of the police response to cyber-dependent crime (see paragraph 1.5 for a full definition of this term). In doing so, we assessed whether:

- law enforcement has a well designed strategy for tackling cyber-dependent crime;
- organisational structures provide the necessary capacity, capabilities and partnerships;
- victims of cyber-dependent crime receive a high-quality response; and
- staff at local and national levels are provided with appropriate learning opportunities to deal with cyber-dependent crime.

Our full terms of reference can be found in Annex A.

Methodology

We inspected ten police forces in England and Wales, all nine regional organised crime units, the National Crime Agency, Action Fraud, and the National Fraud Intelligence Bureau. We invited the local policing body for each of the ten police forces to give us their views.

We spoke to people from each agency and reviewed policies, case files and documents relating to cyber-dependent crime, and we listened to calls from victims. We asked forces to provide us with cyber-dependent crime-related data. And we used a survey to help us understand the perceptions of victims.

Full details of our methodology can be found in Annex B.

Headline findings

The law enforcement response to cyber-dependent crime is good but can be improved

The national strategy for tackling cyber-dependent crime is well established but, outside national agencies, its relevance is limited. Within police forces, the threat from cyber-dependent crime is often not fully understood and is rarely seen as a priority. Knowledge about good practice isn't shared in a structured way, and as a result there is too much variation in the local responses to a national threat.

Having 43 forces operating independently does not provide an effective response to cyber-dependent crime

Recent funding has encouraged police forces to develop their ability to respond to cyber-dependent crime. But we found that the levels of capability and capacity are often based on the available budget rather than an understanding of the demand. Not enough forces have a clear plan to maintain these resources beyond the short term.

The recent initiative to encourage the regional management of specialist resources in police forces is welcome. However, we found that the principles of this initiative haven't been universally adopted by all forces.

'Protect' campaigns need to be better co-ordinated

National organisations do good work in identifying emerging threats. Regionally, there is a well established network that ensures that initiatives promoting protection against cyber-dependent threats are delivered. And forces are increasingly proactive in communicating protection messages. But these messages are not being consistently co-ordinated. More needs to be done to avoid duplication and omission, and to evaluate how effective these campaigns are.

The response to cyber-dependent crime is improving, but more needs to be done

The introduction of a national tasking process and regional co-ordinators has provided some consistency in when, how, and to what level, cyber-dependent crime is investigated by regional and local teams. Establishing national performance indicators has provided some way of measuring performance.

However, each of these developments has limitations, and there is still too much variation in how cases are approached.

Victims who report cyber-dependent crime are generally satisfied with the service they receive, but there is still confusion about the central reporting process

Whether victims are given good advice on protecting themselves from further cyber-dependent attacks varies depending on who they contact.

They are often given confusing and misleading advice about how (or whether) their case will be investigated and, if it is, how it is progressing.

The approach to learning for staff varies

A national training plan has been established, which includes recommended training providers. However, there is wide variation in how much this is followed by forces. There is little evidence that forces are carrying out any analysis of the training their staff need. And for some roles the training provided is insufficient.

The level of training or resources provided to enable non-investigative staff to recognise cyber-dependent crime is inconsistent across forces.

Summary of findings

Strategy

The national strategy for tackling cyber-dependent crime is well established but, outside national agencies, its relevance is limited. Within police forces, the threat from cyber-dependent crime is often not fully understood and is rarely seen as a priority. Knowledge about good practice isn't shared in a structured way, and as a result there is too much variation in the local responses to a national threat.

National and local strategies and priorities

The National Cyber Security Strategy is based on the 3Ds – defend, deter, and develop. This is similar to the government's 4Ps strategy for combatting serious and organised crime – prevent, pursue, protect and prepare – which was used by every force we inspected as the basis for their response to cyber-dependent crime.

Although 27 forces use the term 'cyber crime' in their strategic priorities, this is a broad and vaguely defined term that often includes other cyber-enabled crime. Over a quarter of forces told us that cyber-dependent crime, and cyber crime more generally, were not a specific strategic priority.

The inconsistent approach to cyber-dependent crime can be seen in how forces structure their staff, in whether they have a specific strategy, and in how clear their understanding is of the level of demand.

Only one force in England and Wales has cyber-dependent crime as an explicit priority. In some forces it is dealt with by teams with broader responsibilities like economic crime or intelligence. Cyber-dependent crime was often said to not be a priority compared with other crimes like those relating to firearms, controlled drug supply and child sexual exploitation.

How well understood is the cyber-dependent threat?

The National Strategic Assessment of Serious and Organised Crime 2018, produced by the National Crime Agency, sets out the scale of threats presented by organised crime, including cyber-dependent crime. The National Fraud Intelligence Bureau provides forces with weekly lists of new victims in their area, six-monthly force profiles, which analyse broader trends, and threat updates. Despite this, the understanding of the threat from cyber-dependent crime is inconsistent across police forces.

This is primarily because of the differing approaches forces and regional units take in analysing information they gather and sharing it.

A national intelligence requirement?

Under-reporting of cyber-dependent crime, particularly by businesses, is a significant challenge for all law enforcement agencies.

Outside national bodies like the National Cyber Security Centre and the National Cyber Crime Unit, we found little evidence of intelligence gathering or any clear process for sharing intelligence.

In most of the forces and regional units we inspected, senior officers and staff were often unaware of the intelligence requirement for cyber-dependent crime.

Police forces and regional organised crime units were not clear about their role in the intelligence-gathering process.

Organised crime group mapping

Only one of the forces we inspected, and a small number of regional units, routinely identified and mapped organised crime groups that are primarily involved in cyber-dependent crime. National consistency in the standards and mechanisms used for mapping cyber-dependent crime groups would be beneficial.

How are good practice and 'what works' highlighted?

We found some examples of good practice being identified and circulated at national and regional levels, generally through inter-agency meetings. But this is not a structured approach. We found little evidence that forces review how effective their initiatives to combat cyber-dependent crime are.

Structure

Recent funding has encouraged police forces to develop their ability to respond to cyber-dependent crime. But we found that the levels of capability and capacity are often based on the available budget rather than an understanding of the demand. Not enough forces have a clear plan to maintain these resources beyond the short term.

The recent initiative to encourage the regional management of specialist resources in police forces is welcome. However, we found that the principles of this initiative haven't been universally adopted by all forces.

The need for reform of national, regional and local arrangements

Our 2018 *Annual Assessment of Policing* identifies some modern types of crime that make police force boundaries less relevant. Cyber-dependent crime is an obvious example: much of it operates across local, regional and national policing boundaries. As a result, having 43 forces operating independently does not provide an effective response to cyber-dependent crime.

Regional and local structures

In July 2016, chief constables agreed that the cyber crime units within regional organised crime units should be viewed as “a nationally networked resource”. In 2017, this was taken a step further by a new structure known as ‘regionally managed, locally delivered’, which was created to help co-ordinate local cyber-dependent resources.

This coincided with central government funds being made available to develop local and regional cyber-dependent capability. Forces and regional units that adopted the agreed model and standards were eligible to bid for grants.

All of these are positive steps. Together they have been instrumental in galvanising activity, particularly at force level.

Both the regional tasking model and the principle of regionally managed, locally delivered have merit. But ultimately, both are voluntary arrangements. Staff to whom the agreement relates remain under the control of local command structures and can be diverted or removed from this broader work depending on local priorities.

We do not believe that this is an acceptable position and believe that consideration should be given to establishing a national policing response to cyber-dependent crime.

Limitations to funding streams

As government funding comes to an end, the availability of local resources cannot be guaranteed. Funding from the National Cyber Security Programme was for forces to use to purchase equipment and training. This funding will stop after 2021. Funding from the Police Transformation Fund can only be used for the creation of cyber-dependent posts and had to be matched from local resources. This funding will stop after 2020.

After these ‘cliff edge’ dates, mainstream policing budgets will be expected to absorb the cost of cyber-dependent capability. However, only one of the forces that we inspected had plans that guaranteed the sustaining of current resources.

How well do police forces understand the demand from cyber-dependent crime?

The demand from cyber-dependent crime is not widely understood by police forces. We asked forces for the number of current cyber-dependent investigations. Most forces were not easily able to provide the data with any confidence.

Of those that could provide the data, eight had low confidence that the number was accurate. This resulted in a total of 17 forces being unable to tell us how many investigations they had conducted (because the data was too difficult to extract or the quality was deemed low).

Five forces couldn't distinguish between cases that were directly reported to the force and those which came via the National Fraud Intelligence Bureau.

None of the forces or regional organised crime units that we inspected had analysts dedicated to cyber-dependent crime. Requests by investigators for support on cyber-dependent investigations were rarely prioritised.

How well do capability and capacity match identified and anticipated demand?

The recent funding has meant that all forces and regional units have been able to increase both capability and capacity to deal with cyber-dependent crime. However, the long-term funding of specialist cyber-dependent posts across all agencies is uncertain.

The total number of dedicated cyber-dependent staff in forces varies. The number of staff in a cyber-dependent protect role averaged one member of staff – and some forces had no dedicated staff, thereby not meeting the minimum standards.

Most forces and regions that we inspected had carried out little or no analysis to establish the levels of demand that units would need to meet. Instead, we were told that staffing levels were set using 'professional judgment'. Often, the prevailing consideration was what budget was available.

We found limited evidence of forces considering the potential benefits of collaborating with other forces in the region. This resulted in duplication of resources and work between neighbouring forces. Conversely, in most of the forces and regions we inspected, worthwhile activity such as analysis wasn't available to investigators.

Action Fraud and the National Fraud Intelligence Bureau capacity and capability

Staff at Action Fraud are generally trained appropriately for their role, but high staff turnover had an adverse effect. Once again, we were told that resources were matched to budget and not the level of demand.

As with local and regional agencies, the short-term funding of the National Fraud Intelligence Bureau makes long-term planning difficult.

Recruitment and retention of staff

The National Crime Agency, regional units, and several forces told us that they find it challenging to recruit and retain staff. At the time of our inspection, about 30 percent of the National Cyber Crime Unit's roles were vacant. In response, the National Crime Agency has launched initiatives to boost recruitment.

The problem is exacerbated by the high level of staff turnover. One large force told us that the staff turnover rate of cyber-dependent specialist staff was significantly higher than for other police roles.

The loss of specialist staff to the private sector is an ongoing problem for law enforcement. There is no simple answer to this issue, and law enforcement agencies need to continue to explore innovative methods of attracting the best individuals into specialist roles. One senior officer told us that “agencies had to take a more permeable approach to recruiting” and accept that specialist staff are likely to move in and out of law enforcement during their careers.

Use of cyber specials and cyber volunteers

Some forces use cyber specials and cyber volunteers who can help law enforcement with knowledge and expertise from the private and charitable sectors, but again the use of this valuable resource was inconsistent. At the time of our inspection, 16 forces and three regional units didn’t use volunteers to tackle cyber-dependent crime.

National and international partnerships

The National Cyber Crime Unit works closely with the National Cyber Security Centre to represent the UK’s interests with international partners.

Police at local and regional levels work with partners but, once again, with wide variation. Some forces were working with industry, academia, and financial institutions. In others, partnerships were limited to other forces or law enforcement agencies.

Protect

National organisations do good work in identifying emerging threats. Regionally, there is a well established network that ensures that initiatives promoting protection against cyber-dependent threats are delivered. And forces are increasingly proactive in communicating protection messages. But these messages are not being consistently co-ordinated. More needs to be done to avoid duplication, and omission, and to evaluate how effective these campaigns are.

Roles and responsibility

The National Cyber Security Centre is the lead organisation at a national level for the development of cyber-dependent protect advice. The responsibility for the national distribution of protect advice sits with City of London Police.

Government funding has helped to develop protect capability in forces, though it is more developed in some than others. This a further example of a lack of national consistency in the approach to cyber-dependent crime.

National campaigns

National campaigns supported by the government and the financial sector, like the ‘Get Safe Online’ campaign, are a major part of the police’s cyber-dependent protect advice.

The National Fraud Intelligence Bureau brings together national agencies to develop consistent advice, campaigns and alerts to be distributed nationally through the cyber protect network. However, the timing of advice and the targeting of specific groups was often left to the judgment of individual officers rather than being co-ordinated.

Protect advice at first point of contact and during investigation

The requirement to provide protect advice is included in the initial training of Action Fraud call takers and is monitored in the quality assurance of calls. This structured approach was less evident in forces, which were less likely to provide specific training in cyber-dependent crime to call takers. In our review of telephone calls to police forces, we found that protect advice was only given in a third of cases.

Protect activity – individuals and businesses

We found numerous examples of agencies engaging with business, government, schools and the public to give protect advice. However, we found little evidence (at any level) of the evaluation of whether protect advice or campaigns were effective, or whether they changed the behaviour of the targeted audience.

Investigation

The introduction of a national tasking process and regional co-ordinators has provided some consistency in when, how, and to what level, cyber-dependent crime is investigated by regional and local teams. Establishing national performance indicators has provided some way of measuring performance.

However, each of these developments has limitations, and there is still too much variation in how cases are approached.

In our report, *Fraud: Time to Choose,* we considered whether City of London Police was the most suitable organisation to oversee the central reporting process. We concluded the following:

- Both Action Fraud and the National Fraud Intelligence Bureau fulfilled their respective functions but “there are unacceptable problems with the current arrangements”.
- In the absence of any obvious alternatives, City of London Police should remain as the lead force for fraud and keep responsibility for Action Fraud and the National Fraud Intelligence Bureau.

- All parts of the central reporting process should be held to account for their effectiveness and efficiency.

This remains our view.

Recording of information and delays within the central reporting process

Telephone calls to Action Fraud are generally recorded well and are reviewed by supervisors to check for accuracy and to identify best practice. However, online reports are not subject to the same immediate review of their quality, and victims entering their own information can lead to inaccurate and misleading reports.

As of July 2019, up to 6,500 fraud and cyber crime cases were being held in quarantine within the National Fraud Intelligence Bureau's database, Know Fraud.

How well do police respond to and prioritise allegations of cyber-dependent crime?

The national response to cyber-dependent crime works well, with a clear understanding across agencies of their roles and responsibilities. However, the response from forces is less consistent. As with fraud, the definition used by forces of 'calls for service' varies.

However, the national prioritisation and tasking process are well understood across all agencies.

The initial response to allegations of cyber-dependent crime

Despite the existence of Action Fraud, some victims still report cyber-dependent crime to their local police force. Forces use the definition of a call for service to identify whether they should act themselves or advise the victim to report to Action Fraud. We found that forces often extend this definition to include additional aspects, including the vulnerability of the victim and the opportunity to recover evidence.

In some cases, forces are treating businesses (generally small and medium-sized enterprises) differently from other victims. This can cause delays in support being provided and adds to levels of dissatisfaction with the response by law enforcement.

Tasking and co-ordination

While most cyber-dependent investigations are allocated directly to forces by the National Fraud Intelligence Bureau, there is a separate tasking process for more complex or serious investigations and live cyber attacks. The Triage, Incident Coordination and Tasking (TICAT) unit is part of the National Cyber Crime Unit. The process, like TICAT itself, is highly regarded by practitioners and we found that it generally works well.

The agreements to enable the national tasking of regional cyber units and the implementation of the 'regionally managed, locally delivered' model have been important steps in the development of a national approach to cyber-dependent crime. We understand that there is an aspiration to extend this agreement to local units so that they too can be part of a national tasking process.

But, as funding from the Police Transformation Fund and the National Cyber Security Programme comes to an end, the availability of local resources cannot be guaranteed.

Investigation – quality and outcomes

Most forces have some form of cyber-dependent crime capability. This means that, in theory, offences are investigated at the appropriate level, by appropriately trained staff. But there is still a gap in the availability of analytical capability.

We examined 103 cases that were investigated by local forces and 26 cases that were investigated by regional teams or the National Crime Agency. Two-thirds of the local force investigations had been undertaken by a dedicated team. The remainder were investigated by non-specialist units, including patrol and neighbourhood staff.

The majority had been finalised with no further action being taken. In most cases there had been no supervisory reviews. None had aims and objectives set by investigators.

This contrasted with the investigations undertaken by regional and national units. These were better structured, with investigation aims and objectives identified and recorded at the outset. Most benefited from supervisory oversight.

The most common outcome for cyber-dependent crime cases disseminated to forces and regional units is investigation completed – no suspect identified. Between 2015 and 2019, this has consistently accounted for between 51 percent and 62 percent of all outcomes. One of the least likely outcomes nationally is for offenders to be charged or summonsed.

Because of the nature of cyber-dependent crime, not every investigation can or should result in a criminal justice outcome. Outcomes based solely on the offender are not, therefore, a reliable yardstick by which police forces should be judged.

Instead, their ability to provide an effective response across all elements of the 4Ps is the method by which their performance should be considered. This includes how effective the investigation is.

Performance indicators

The recent introduction of performance indicators is an important first step in bringing consistency to the police's response to cyber-dependent crime. These include a requirement that "100 percent of Action Fraud referrals will be investigated".

However, it is forces that decide whether their cases have been investigated. To a large degree they are ‘marking their own homework’. Better use should be made of regional co-ordinators to provide independent reviews of investigations.

In addition, forces are using the weekly list provided by the National Fraud Intelligence Bureau to initiate investigations. This is done with the intention of providing victims with a better service. However, it risks duplication of effort between bureau reviewers, the investigating unit and other forces who may have started similar enquiries. A situation that the centralised reporting process was designed to prevent.

How well do police forces recognise and interact with those involved with cyber-dependent crime?

We were disappointed not to find evidence of individual cyber criminals being profiled by forces, and very limited examples of preventative or ancillary orders being used to prevent cyber-dependent crime.

Organised crime groups

We found that organised crime groups whose primary offending was cyber-dependent crime were generally not being mapped. Investigators told us that crime groups involved in this type of crime would rarely be prioritised over those involved in firearms and drugs offences. We were repeatedly told that the process does not provide an easy fit with cyber crime offenders. One investigator told us that trying to map organised crime groups involved in cyber-dependent crime was “like trying to plait smoke”. A nationally consistent approach is needed.

Management of offenders

In general, the prevent element of the national strategy is less developed compared with the resources dedicated to protect activity, although there is a better picture at the national level. We did not find any evidence that people involved in cyber-dependent crime were being identified for integrated offender management and only limited use of ancillary orders.

Some forces don’t have any dedicated staff focusing on prevent activity. In April 2019, we were told that only three to four Serious Crime Prevention Orders had been issued to cyber crime offenders across all 43 forces in England and Wales.

Victims

Whether victims are given good advice on protecting themselves from further cyber-dependent attacks varies depending on who they contact.

They are often given confusing and misleading advice about how (or whether) their case will be investigated and, if it is, how it is progressing.

Sources of evidence

We used an independent survey of 252 victims of computer misuse, and a further 52 qualitative interviews, which asked about perceptions of the support and advice provided by Action Fraud and the police. We also reviewed 232 calls to Action Fraud and different police forces to report cyber-dependent crime.

Action Fraud

There is still an issue of a lack of public awareness of Action Fraud. Just under half of the victims surveyed by us reported their matter directly to Action Fraud, and many had not previously heard of Action Fraud.

The victim survey showed that the clear majority of callers to Action Fraud had a positive experience. However, callers can experience long delays in getting through. At the time of our inspection, 40 percent of calls were being hung up before they were answered. This equates to 20,000 calls (relating to both cyber crime and fraud) being abandoned each month.

Many victims still report cyber-dependent crime to police forces. While forces generally advised victims well about reporting their cyber-dependent crime, there were still examples of officers and staff having a lack of knowledge about Action Fraud or providing an incorrect response.

Advice to victims

Generally, victims who reported directly to Action Fraud were given appropriate advice. The victim survey showed that, in most cases, victims felt more aware and better equipped to protect themselves following the advice given.

Accurate advice about the role of Action Fraud was only given by police forces in a very small number of cases.

How well are vulnerable victims identified?

The identification of vulnerability is a complex issue for forces to resolve. In general, the identification of vulnerability at first point of contact, both at Action Fraud and within forces, was effective, and appropriate support was provided by forces and partners.

The central reporting process for cyber-dependent crime, and the variations in the definition of a call for service, make the complexities even more pronounced. Furthermore, in general, businesses are unlikely to be considered as vulnerable, which can affect how police forces respond to their cases.

How well are vulnerable victims supported?

Once a victim has been identified as vulnerable, most forces will provide additional support. We found that this generally consists of advice on how the victim can further protect themselves, or a referral to a victim support agency.

A small number of forces are currently piloting the use of the National Economic Crime Victim Care Unit. Vulnerable victims of cyber-dependent crime and fraud are identified and provided with support. However, the role of the care units may duplicate activity carried out by staff in forces.

Satisfaction of victims

The victim survey identified that there were moderate levels of victim satisfaction in relation to the reporting process and advice given. Around two-thirds of victims reported that they were fairly or very satisfied.

Learning

Training pathways

A national training plan has been established that includes recommended training providers. However, there is wide variation in how much this is followed by forces. There is little evidence that forces are carrying out any analysis of the training their staff need. And for some roles the training provided is insufficient.

The level of training or resources provided to enable non-investigative staff to recognise cyber-dependent crime is inconsistent across forces.

What learning is provided to enable recognition of cyber-dependent crime?

We found considerable variation in the level and standard of training and guidance provided to staff in roles that require them to identify cyber-dependent crime, like call handlers. Training was more structured at the national level, with call handlers from Action Fraud receiving a two-week training course and continual assessment.

Cyber crime represents only a very small proportion of the calls to police forces that call centre staff deal with. But call handlers from local forces received comparatively little in the way of specific cyber-dependent training. Most received general call handler training, which may include a small amount about cyber crime. It was a similar picture for most non-specialist police officers and staff, with many receiving, at best, just basic awareness.

More positively, we found a number of forces that had developed web-based information sheets providing guidance and advice for staff.

Recommendation

By 1 November 2020, the Home Office, the Cabinet Office, the National Police Chiefs' Council's lead for cyber crime and Coordinator for Economic Crime, the Director General of the National Crime Agency, and interested parties should revise the current police structure for the response to cyber-dependent crime. In doing so they should consider:

- the creation of a national police cyber-dependent crime network;
- the remit of any such network;
- how the network engages with other law enforcement agencies; and
- the tasking and co-ordinating responsibilities that will be required for the network to be effective.

Areas for improvement

There are some areas in which we think those responsible for the police response to cyber-dependent crime and chief constables need to make improvements, but we have not made specific recommendations about how they should do this.

1. Chief constables should evaluate the use that their force makes of cyber specials and volunteers to ensure that they are used effectively.

2. With immediate effect, City of London Police should provide the Home Office with details of how the force intends to address the issue of reports being held in 'quarantine' within the Know Fraud system. Furthermore, the force should also identify its proposals to prevent a re-occurrence.

3. The National Police Chiefs' Council's lead for cyber crime and Coordinator for Economic Crime should revise the key performance indicators contained within the council's minimum capability standards for force cyber crime units. The revised standards should make clear:

    - the minimum standards for investigation;

    - the role of regional cyber crime co-ordinators in the recording, management, and review of cyber crime investigations; and

    - the use of the weekly list provided by the National Fraud Intelligence Bureau to comply with the performance indicators.

4. The National Police Chiefs' Council Coordinator for Economic Crime should review the role the National Economic Crime Victim Care Units in providing advice and support to victims of cyber-dependent crime.

1. Introduction

About our inspection

1.1. This report details the findings of an inspection commissioned by the Home Secretary. The inspection focused on how effectively and efficiently the police and the National Crime Agency respond to the threat presented by cyber-dependent crime.

1.2. In April 2019, we published our report *Fraud: Time to Choose*, which outlined the findings of our thematic inspection of how the police respond to fraud. That report contained 16 recommendations and five areas for improvement. Several of those recommendations equally apply to cyber-dependent crime. We have reproduced those that appeared in the fraud report to highlight their relevance.

About cyber-dependent crime

1.3. Cyber crime takes two forms, cyber-enabled crime and cyber-dependent crime.

1.4. Cyber-enabled crimes are defined as "existing crimes that have been transformed in scale or form by the use of the Internet". The obvious example is fraud, which can be conducted on or offline, but online may take place at unprecedented scale and speed.

1.5. Cyber-dependent crimes are "offences that can only be committed using information communications technology, where the devices are both the tool for committing the crime and the target of the crime".[1] Cyber-dependent crime can result in the theft of personal data, money, intellectual property or other sensitive information. It can also be committed to alter, prevent access to, or otherwise disrupt a system, service or data.

1.6. Methods of committing these offences include the use of ransomware, where malicious software blocks a user's files, computer or device until a ransom is paid, and distributed denial of service attacks, which flood a system with more requests than it can handle, stopping users from accessing it. Perhaps the best known use of ransomware in the UK was in 2017 when the National Health Service was affected by a global ransomware attack known as WannaCry.

[1] *National Cyber Security Strategy 2016–2021*, Cabinet Office, 2016, page 74.

1.7. On a lower level, cyber-dependent crime can involve getting unauthorised access to someone's email or social media accounts. While there is more cyber-enabled crime, cyber-dependent crime often takes greater technical skill and can have a more damaging effect. There is a wide span of offenders, which include: hostile state actors, organised crime groups, and those involved in online harassment and abuse.

1.8. This inspection report examines the response to cyber-dependent crime only.

The scale of cyber-dependent crime

1.9. Cyber-dependent crime is massively under-reported and, as a result, the true scale of it is unknown. This is a significant problem for law enforcement agencies.

1.10. In its 2018/19 assessment,[2] the National Fraud Intelligence Bureau said that there "continues to be a significant gap between reports of cyber-dependent crime and known cyber attacks which impacts on the ability to properly assess the risk and harm caused by this type of offending".

1.11. It goes on to say that in 2017/18 there were "23,525 reports of cyber-dependent crime, but over 656,000 IP addresses were known to have been infected by some form of malware".

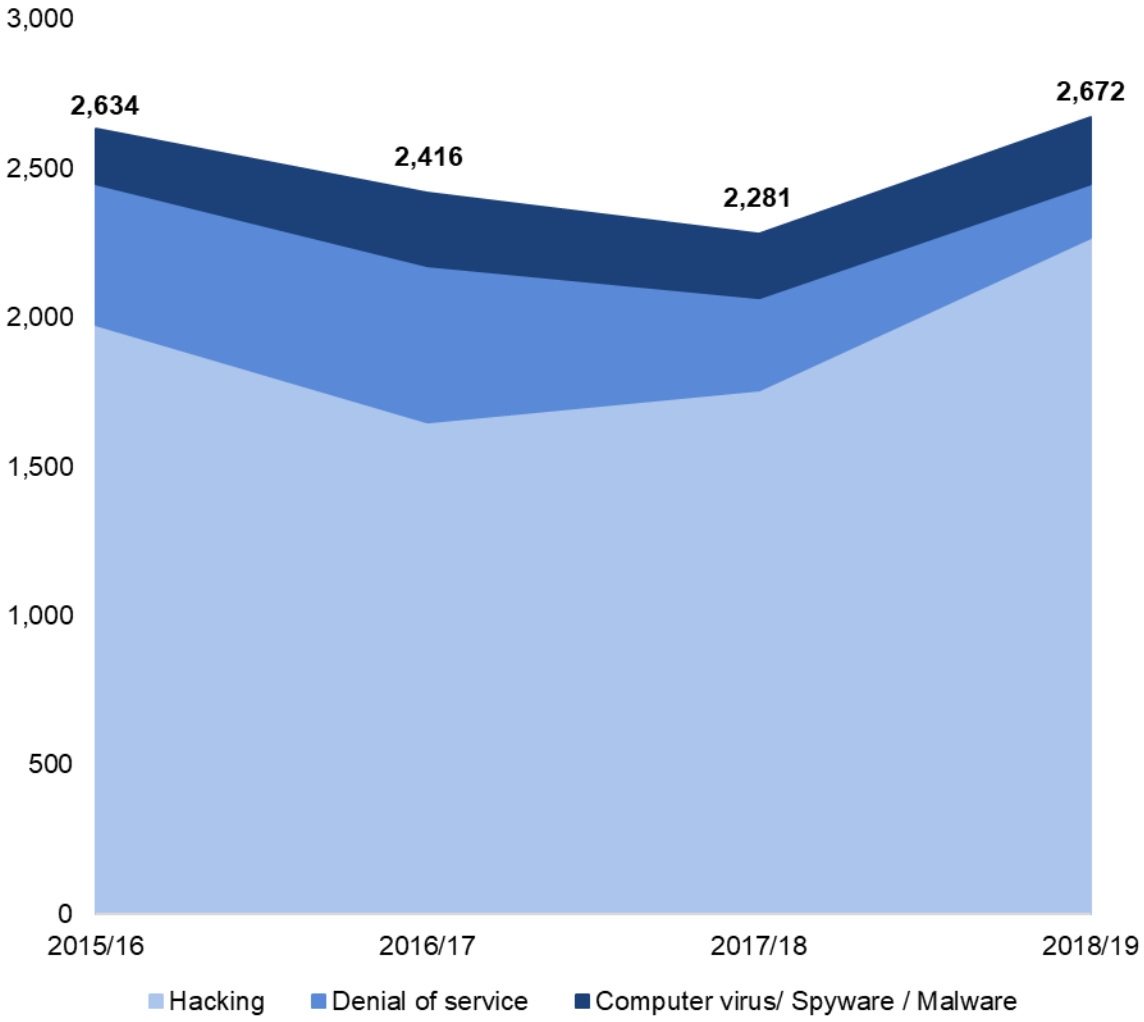
1.12. Similarly, in 2018, the Crime Survey for England and Wales estimated that there were 976,000 computer misuse offences.

1.13. The National Fraud Intelligence Bureau assessment said that the three most common forms of cyber-dependent attack in 2017/18 were the "hacking of social media and email accounts, the introduction of computer virus/malware/spyware and hacking related extortion".

1.14. This is reflected in the number of disseminations for investigation from the National Fraud Intelligence Bureau to law enforcement agencies.

[2] Unpublished.

Figure 1: Number of disseminations for investigation by year and crime type



The harm from cyber-dependent crime

1.15. Cyber-dependent crimes range from attacks on the national infrastructure to individuals and business, affecting reputation and financial wellbeing. The harm caused by cyber-dependent crime can't be overestimated, as the outcome can be devastating for those involved.

1.16. In its 2018 report on the economic and social cost of crime, the Home Office estimated an overall cost of £1.1 billion in 2015/16 from computer misuse incidents against individuals in England and Wales. The estimated average unit cost was £550 per incident.[3]

[3] The report estimates the cost of cyber crime as a combination of defensive costs, cost of stolen property, physical and emotional harm, lost output and health costs, and is based on crime and price data from 2015/16. This estimate is based on experimental statistics and should only be considered as a partial estimate, as it doesn't include some costs associated with the crime. Crucially, this estimate doesn't include the cost to businesses, which are thought to bear the majority of cyber crime costs, and so is likely to be an underestimate.

1.17. The 2017 WannaCry attack affected 80 of 236 National Health Service hospital trusts. Health Service staff were locked out of their devices, appointments were cancelled, there were delays in discharging patients, and there was significant disruption across the service.

1.18. There should be no doubt of the importance of combatting cyber-dependent crime, and those who commit it.

The response to cyber-dependent crime

1.19. In England and Wales, cyber-dependent crime is reported through a central reporting process run by Action Fraud (see paragraph 1.21). The Fraud Intelligence Bureau identifies cases with viable lines of enquiry and allocates them to the most appropriate police force or other law enforcement agency to pursue.This includes an immediate response to live cyber attacks on businesses or organisations.[4]

1.20. Fraud and cyber-dependent crime are the only types of crime that are dealt with like this. The National Fraud Intelligence Bureau also produces intelligence about cyber-dependent crime. Action Fraud and the bureau are both run by City of London Police.

Context: The cyber-dependent crime landscape

Action Fraud and the National Fraud Intelligence Bureau

1.21. Action Fraud is the single reporting centre for all fraud and cyber crime reports from members of the public. It receives crime reports and information reports in four ways:

- directly from members of the public over the telephone;
- directly from members of the public via its website;
- directly from police forces or other law enforcement agencies on behalf of victims through its website; and
- directly from businesses via its website.

1.22. Other than in cases that require an immediate response, the National Fraud Intelligence Bureau processes the information received by Action Fraud along with information provided by other agencies on the Know Fraud system (see paragraph 1.24). When the bureau thinks that an investigation is viable, it

[4] A cyber attack is the deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm. *National Cyber Crime Strategy 2016-2021*, Cabinet Office, 2016, page 74.

is given to a police force or other law enforcement agency to investigate. Neither the bureau nor Action Fraud is responsible for investigating offences.

1.23. The bureau also provides forces and agencies with intelligence products. These include:

- Victim care packages – these relate to particularly vulnerable individuals, who have reported a crime or information, and are sent to the victim's local force to provide additional support.
- Weekly victim lists – these contain the details of all the victims reporting to Action Fraud residing in each specific police force. A schedule of this information is forwarded to every police force and includes crime type, the victim's details and the impact of the offence on the victim.
- Six-monthly force profiles – these are produced biannually and provide statistical analysis of crime trends, crime types and emerging crime techniques used by offenders both within that force's area and nationally.
- Threat updates – these give information about current and emerging cyber-dependent crimes, and provide advice that can be given to the public about preventing them.

Know Fraud database

1.24. Know Fraud is the bureau's intelligence system. It assesses all reports for 'solvability factors' – information that can be used to build a case, such as bank account details, names, addresses and email accounts – and identifies links and patterns in offending.

1.25. Unlike other crimes, for which police forces hold intelligence and information on their own systems, all cyber-dependent crime reports are kept on the Know Fraud system. At the time of our inspection, neither individual law enforcement agencies nor Action Fraud staff had direct access to this system.

1.26. Cases with appropriate solvability factors are reviewed, analysed and developed by bureau staff.

1.27. When there are viable lines of enquiry to pursue, the case is referred to a relevant police force or other law enforcement agency. Which force it goes to depends on who is best placed to conduct the investigation. Depending on the nature of the case, this could be a local force, a regional organised crime unit, or the National Crime Agency. It won't necessarily be the force covering the area where the offence was committed, although that force will be made aware of the crime.

1.28. Those that report cyber-dependent crime will receive a follow-up letter with one of two conclusions, depending on the result of the analysis: that no further action is being taken and that their details will remain on the database; or that lines of enquiry have been identified and the case has been forwarded to a specific police force or law enforcement agency for further action. Victims who make an information report will not receive a further update.

1.29. The bureau's weekly list gives forces details of all cyber-dependent crime victims in their area from the previous week. This allows each force to assess which victims are particularly vulnerable and give additional support if required.

Changes to the reporting process and Know Fraud

1.30. Since 2014 when it took responsibility for both Action Fraud and the National Fraud Intelligence Bureau, City of London Police has recognised that the technology supporting both organisations is not fit for purpose. As a result, it launched a project to design and implement a new system for reporting and for analysing reports. It was initially planned for April 2016, but the implementation was delayed by over two years. The first improvements to the reporting process were introduced in October 2018, and further improvements are planned.

1.31. Changes to the reporting process were outlined in more detail in our report *Fraud: Time to Choose*. The report included the following recommendation.

Fraud report 2019 – recommendation 1

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should publish a timetable for implementing the revised Know Fraud system, making clear which services are to become available at each stage of implementation and thereby enabling forces to make use of each service as early as practicable. The use made of the system by police forces should be monitored and evaluated to identify best practice.

National Cyber Security Centre

1.32. The National Cyber Security Centre was created in 2016 to respond to cyber security incidents and to reduce the harm they cause in the UK. It provides a single point of contact for the public, businesses, government agencies and other organisations. It also works with law enforcement agencies, the intelligence and security agencies, and international partners.

1.33. Although the National Cyber Security Centre is not one of the organisations we are responsible for inspecting, senior managers allowed us to interview their staff to understand the role of the centre and how it interacts with law enforcement agencies.

The National Cyber Crime Unit

1.34. The National Cyber Crime Unit is the part of the National Crime Agency that focuses on major cyber incidents. It works closely with the National Cyber Security Centre, police forces, regional organised crime units, and international law enforcement such as Europol, Interpol and the FBI to share intelligence and co-ordinate action. The National Cyber Crime Unit "seeks to develop close and effective partnerships with private industry to share information and technical expertise".

Regional organised crime units

1.35. Regional organised crime units provide police forces with access to a standard range of capabilities to help them tackle serious and organised crime. There are nine regional units across England and Wales, which have a range of specialist policing capabilities, including a dedicated cyber-dependent capability.

The role of the National Police Chiefs' Council

1.36. The National Police Chiefs' Council co-ordinates the operational response across the entire service to the threats faced in the UK.

1.37. Cyber crime is recognised by the council and the Association of Police and Crime Commissioners as a 'specialist capability'. In 2017, the Specialist Capabilities Programme, which is led by the council, found that just 32 percent of forces had a dedicated cyber crime unit or cyber crime capability.

1.38. In October 2017, the council agreed that every force should have its own dedicated cyber-dependent crime capability. It also agreed that this local capability should be regionally managed and locally delivered. This means that regional teams, through a regional co-ordinator should oversee and manage the cyber-dependent crime investigations being conducted by local forces.

1.39. The development of this capability was overseen by the National Force Specialist Cyber Capability Project Board. The board set the minimum standards for force capability, managed the process by which forces could bid for money, and decided how much was allocated. The board also managed regional governance and tasking arrangements and the identification of appropriate training and equipment.

Funding

1.40. To support the development of capability at local and regional level, funding was secured from the Home Office's Police Reform and Transformation Fund and the Cabinet Office's National Cyber Security Programme.

1.41. Forces and regions that adopted the national model of regionally managed, locally delivered were able to apply for grants to help them to develop their capabilities.

1.42. However, funding from the Transformation Fund will end in 2020 and from the Cyber Security Programme in 2021. At the time of our inspection, funding arrangements for after this were unclear.

Minimum standards

1.43. To be eligible for funding, force units needed to meet, or commit to meet, the minimum capability standards set by the Project Board. These standards were circulated in April 2018. They are intended to improve capabilities at a local level, where they state "local victims of volume cybercrime often get little or no service".[5]

1.44. Based upon the 4Ps (prevent, pursue, protect and prepare) the expectations set out in the standards were clear. These included:

- a dedicated capability that is sufficient to investigate all offences of cyber-dependent crime received by the force – both as a direct call for service[6] or via Action Fraud;
- a dedicated protect and prepare resource; and
- the capability and capacity to carry out prevent activities, including supporting proposed intervention panels, on which the police work with public, private and voluntary sector partners to help to divert young people from getting involved in cyber crime.

[5] Unpublished.

[6] In general terms, a call for service is a report that requires a response from the police. The Home Office Counting Rules define the circumstances that should be treated as a call for service: "offenders are arrested by police; there is a call for service to the police and the offender is committing or has recently committed at the time of the call for service; or there is a local suspect".

1.45. The standards also set out clear performance indicators against which local units would be judged. These indicators are:

- 100 percent of Action Fraud referrals will be investigated.
- 100 percent of victims who report to Action Fraud will get advice in person or over the telephone to prevent them becoming repeat victims (protect).
- 75 percent of organisations and the public who receive protect advice will change their behaviours as a result.
- 75 percent of organisations who receive prepare advice will develop or review incident response plans and test them.
- 100 percent of young people identified as vulnerable to cyber crime will get prevent contact and intervention from a prevent officer where appropriate.

2. Strategy: How well designed is the strategic approach for tackling cyber-dependent crime?

2.1. For this aspect of the inspection, we examined whether national and local strategies were based on a comprehensive understanding of the threat from cyber-dependent crime. We also examined whether those strategies enabled the identification and spread of good practice.

2.2. The national strategy for tackling cyber-dependent crime is well established but, outside national agencies, its relevance is limited. Within police forces, the threat from cyber-dependent crime is often not fully understood and is rarely seen as a priority. Knowledge about good practice isn't shared in a structured way, and as a result there is too much variation in the local responses to a national threat.

The national strategic approach to tackling cyber-dependent crime

2.3. The *National Cyber Security Strategy 2016–2021* sets out the UK Government's vision to ensure that "the UK is secure and resilient to cyber threats, prosperous and confident in the digital world". The strategy organises its objectives under three headings, often referred to within law enforcement as the 3Ds:

> "Defend. We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.
>
> Deter. The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.
>
> Develop. We have an innovative, growing cyber security industry, underpinned by world leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges."

2.4. The government strategy for combatting serious and organised crime[7] (which includes cyber-dependent crime) uses a similar framework known as the 4Ps:

- **Prevent** people from becoming involved in or supporting criminal activity
- **Pursue** prosecute and disrupt those engaged in criminality
- **Protect** individuals and businesses from criminality
- **Prepare** the public and businesses to reduce the impact of criminality.

3Ds versus 4Ps

2.5. Without exception, every force that we inspected used the 4Ps as the basis for their response to cyber-dependent crime. They told us that this was a language and structure that police and partner organisations understood.

2.6. Some people we spoke to saw this as a possible source of confusion because people in government have "different reference points" to policing. We didn't find evidence that this had caused any practical problems.

2.7. In our 2019 report *Fraud: Time to Choose* we adopted the 4Ps terminology. We have done the same in this report for ease of understanding and consistency.

Local priorities and activity

2.8. As part of our inspection we asked all 43 police forces in England and Wales about their approach to cyber-dependent crime.[8]

2.9. Although the more general term 'cyber crime' appears in the priorities of 27 forces, it is often conflated with other types of crime like cyber-enabled fraud.

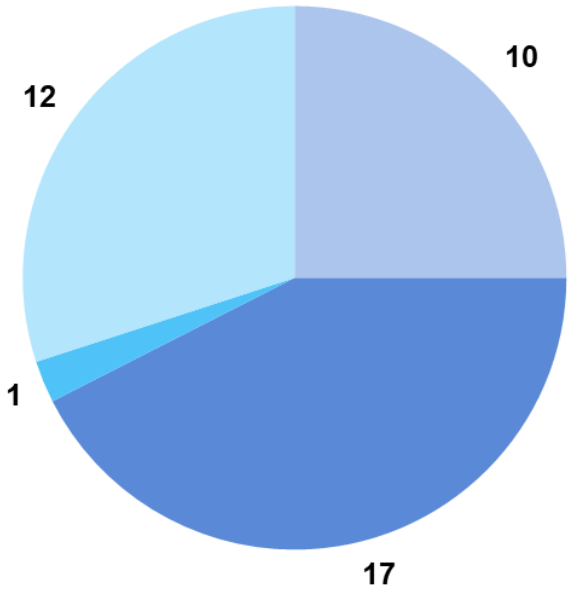
2.10. Over a quarter of forces told us that neither cyber-dependent crime in particular, nor cyber crime in general, were a priority at all. Only one force (not one that we inspected) had identified cyber-dependent crime as a specific strategic priority – they told us that they previously set 'cyber crime' as a

[7] The *Serious and Organised Crime Strategy* (paragraph 16) defines serious and organised crime as: "individuals planning, coordinating and committing serious offences, whether individually, in groups and/or as part of transnational networks. The main categories of serious offences covered by the term are: child sexual exploitation and abuse; illegal drugs; illegal firearms; fraud; money laundering and other economic crime; bribery and corruption; organised immigration crime; modern slavery and human trafficking; and cyber crime."

[8] Some forces provided joint submissions to reflect their collaborative approach to cyber-dependent crime. These submissions were counted as a single submission. As a result, the total number of forces is shown as 40.

priority but because the term was too broad they felt it prevented them from effectively focusing on the problem.

Figure 2: Number of forces that specifically feature cyber-dependent (or cyber crime more generally) in their strategic priorities

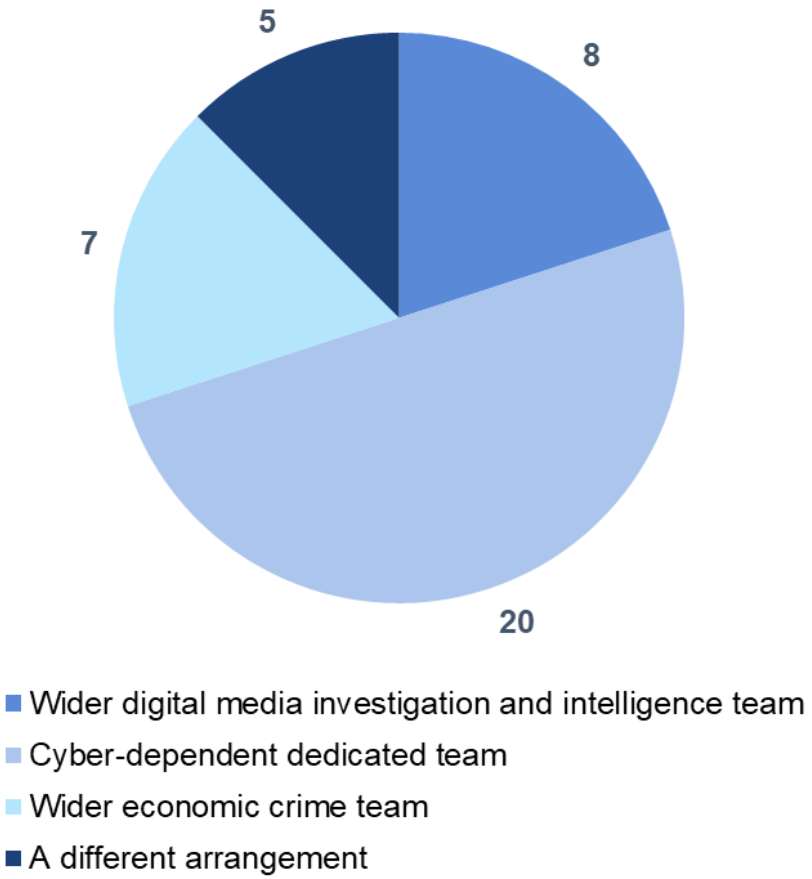


- Cyber crime is a specific strategic priority, which includes mention of cyber-dependent crime
- Cyber crime is a specific strategic priority
- Cyber-dependent crime is a specific strategic priority
- Neither cyber-dependent or cyber crime are specific strategic priorities

2.11. Several of the forces we inspected didn't have clear strategies or plans for tackling cyber-dependent crime. Where they did exist, they often amounted to little more than departmental plans. There was little awareness of them outside the departments that created them.

2.12. Unsurprisingly, this means that the local approach to cyber-dependent crime is inconsistent. Only 20 forces have a team dedicated to dealing only with cyber-dependent crime. In 15 forces, it is dealt with by teams with broader responsibilities, like economic crime or intelligence.

Figure 3: Force cyber-dependent crime team structures



How well understood is the threat from cyber-dependent crime?

2.13. Understanding the scale and nature of the threat from cyber-dependent crime enables resources to be deployed appropriately. It also helps in identifying appropriate strategies and tactics to respond effectively.

2.14. At a national level, a good working relationship between the National Cyber Security Centre and the National Cyber Crime Unit helps to increase awareness of emerging threats. Various assessments and intelligence reports also assist in this process.

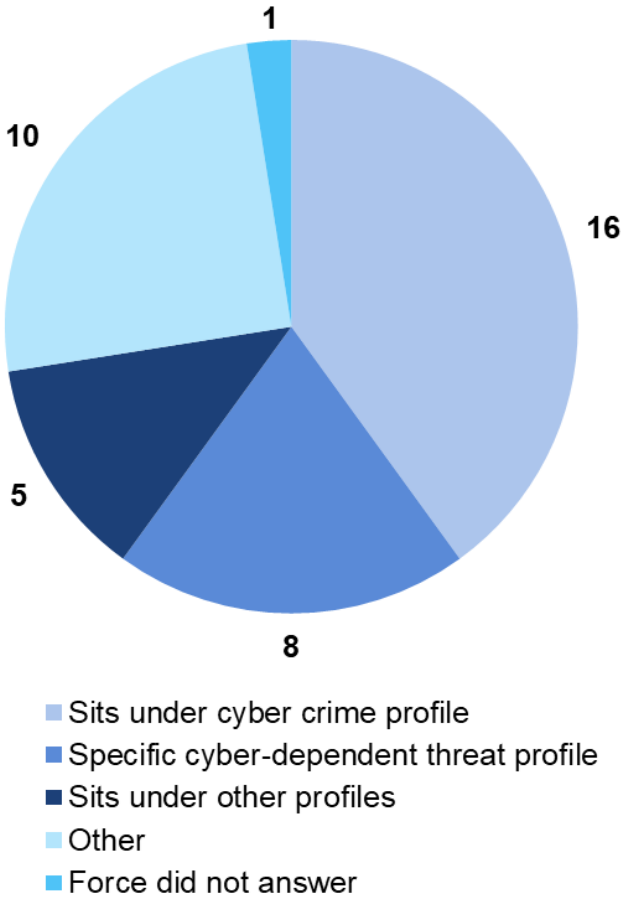
2.15. The *National Strategic Assessment of Serious and Organised Crime 2018*, produced by the National Crime Agency, sets out the scale of threats from organised crime, including cyber-dependent crime.

2.16. The National Fraud Intelligence Bureau provides police forces with intelligence products relating to victim care: weekly victim lists, six-monthly force profiles and monthly alerts (see paragraph 1.23).

2.17. Despite having access to this intelligence, we found that forces and regional organised crime units had an inconsistent understanding of the threat from cyber-dependent crime. This is primarily due to the differing approaches forces and regional units take in analysing and sharing information they have gathered. This problem is made worse by forces not having staff with the expertise to analyse the information, and not having processes for sharing it.

2.18. Only eight forces have created a specific 'problem profile'[9] for cyber-dependent crime. And, even in those cases, what constituted a problem profile varied significantly.

Figure 4: How do forces monitor the threat from cyber-dependent crime?



[9] A problem profile is intended to provide the force with greater understanding of established and emerging crime or incident series, priority locations or other identified high-risk issues. It should be based on the research and analysis of a wide range of information sources, including information from partner organisations. It should contain recommendations for making decisions and options for action.

2.19. Where they do exist, most forces' problem profiles rely heavily on data from the six-monthly profiles supplied by the National Fraud Intelligence Bureau. These are useful documents but realistically, given the high levels of under-reporting for cyber-dependent crime, they can only provide a partial picture.

Under-reporting of cyber-dependent crime

2.20. Under-reporting, particularly by businesses, is a significant challenge for all law enforcement agencies in understanding both threats and future levels of demand.

2.21. Often the primary concerns of businesses who fall victim to a cyber attack are: to avoid reputational damage; to deal with the prevailing issue; and to get their computer systems back online. These businesses fear that investigative processes may interfere with that, costing them money in the long run, which makes them reluctant to engage with the police or other agencies.

2.22. We were pleased to find examples of forces seeking ways to encourage the sharing of cyber security information through initiatives such as cyber resilience security centres[10] and local partnerships.

The General Data Protection Regulation (GDPR)

2.23. The protection and appropriate use of someone's data is important. Often unlawful access to information is used to enable other crimes such as online fraud, including identity theft.

2.24. This is recognised in legislation such as the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). The Act places a responsibility on those who hold personal data for "any business or other non-household purpose". Under GDPR all such organisations are obliged to report certain types of personal data breach to the relevant supervisory authority within 72 hours of it being identified. In certain circumstances people whose data has been breached must also be notified.

2.25. In the UK, the relevant supervisory authority is the Information Commisioner's Office (ICO), the independent authority responsible for upholding information rights in the public interest. As well as providing advice and guidance on data protection, it monitors compliance and takes enforcement action where appropriate.

[10] These are partnerships between public and private sector organisations that enable small and medium-sized enterprises to be more cyber secure through advice, guidance, or subsidised consultancy services.

2.26. In some circumstances, organisations that have been the subject of cyber attacks involving a data breach could also be subject to investigation by the ICO. Some people – both police and in businesses – told us that they believed that this could discourage businesses from working with law enforcement.

2.27. Staff told us that it was becoming increasingly less common for them to deal with the person responsible for managing an organisation's computer systems. Instead, they would be directed to a legal representative, who was focused on reducing the risk of punishment to the company. In their view the process was "breeding perverse behaviours".

2.28. This is reflected in the approach by law enforcement agencies. We were told that forces and other agencies would often remind organisations of their duty to report data breaches to the ICO. But at the same time felt they needed to make it clear that they wouldn't pass details on or engage with the ICO without the victim's consent. Forces justified this as a means of developing trust and encouraging the free flow of information.

2.29. Ultimately, neither the ICO nor law enforcement agencies are required to routinely share information with each other.

2.30. While both are seeking to protect individuals from harm and from the unlawful processing of their data, this can create a challenge. The ICO has a responsibility to investigate organisations for not taking appropriate steps to protect personal data, while law enforcement agencies seek to identify those criminals who exploit it. Both are important, but the consequence is that the ability to share information can be complex and both sides may be missing out on useful intelligence.

2.31. We are aware that all parties are making efforts to mitigate this and encourage them to continue to do so.

A national intelligence requirement?

2.32. Outside the National Cyber Security Centre and the National Cyber Crime Unit we found little evidence of intelligence gathering or any clear process for sharing intelligence.

2.33. Police forces and regional organised crime units were not clear about their role in the intelligence-gathering process. For example, most investigators we spoke with didn't routinely feed information gathered during their investigations back into the system. This is a missed opportunity.

2.34. The National Crime Agency is responsible for the National Intelligence Requirement for Serious and Organised Crime.[11] This sets out threats from serious and organised crime, including cyber-dependent crime. It also notes where there may be gaps in the knowledge and understanding of those threats, so that law enforcement agencies can follow up.

2.35. In most of the forces and regional units we inspected, senior officers and staff were often unaware of the intelligence requirement for cyber-dependent crime.

2.36. This wasn't universal. We did find some examples of local and regional units who had intelligence requirements that reflected the National Crime Agency's. But these were the exception rather than the rule. We didn't find any examples of forces routinely contributing to the national intelligence picture.

Organised crime group mapping

2.37. When a police force identifies a group of individuals it suspects may be involved in organised crime, it carries out a standardised mapping procedure[12] that is managed on the Police National Database.[13] In our *PEEL: Police effectiveness 2016: A national overview* report we commented on the importance of mapping organised crime groups. In that report we also highlighted the challenges presented by emerging crime types.

2.38. During this inspection, we were told that, for a variety of reasons, the traditional identification of organised crime groups was not "a good fit" for crime groups involved in cyber-dependent crime. For example, people involved in this type of crime are often a network of loosely affiliated offenders rather than an organised group. Often the network is spread across international boundaries, or the details of those involved are unknown or limited to a username, IP address[14], or location. One analyst told us that it was "like trying to plait smoke".

[11] The priorities for intelligence collection are agreed by the National Crime Agency and the main UK law enforcement agencies, and form part of the national strategic assessment.

[12] Organised crime group mapping is used by forces, regional organised crime units, the National Crime Agency and a number of non-police organisations such as Border Force.

[13] The Police National Database is an IT system that allows the police to share and search local force information on a national basis. It is designed to provide forces with immediate access to up-to-date information drawn from local crime, custody, intelligence, child abuse and domestic abuse systems.

[14] Internet protocol address – a unique string of numbers separated by full stops that identifies each computer using the internet protocol to communicate over a network.

2.39. This was reflected in the variety of approaches that forces and regional units take to mapping cyber crime groups. Only one of the forces we inspected routinely identified and mapped crime groups that were primarily involved in cyber-dependent crime. However, a small number of regional units did. At a national and international level there is progress being made in mapping high-level organised crime groups involved in cyber crime.

2.40. Despite the difficulties encountered with the mapping process for cyber dependent crime groups, NCA and regional units have made use of Management of Risk in Law Enforcement (MoRiLE) to assist assessment of threat and risk in operational activity for cyber-dependent crime. National consistency in the approach to identification and mapping of cyber-dependent crime groups would be beneficial.

How is good practice and 'what works' highlighted?

2.41. Alongside the effective sharing of intelligence, we hoped to find a clear process for evaluating and disseminating good practice across law enforcement, partner organisations and academia. In our view, this would encourage a national approach and help in the early adoption of tactics that protect individuals and businesses from cyber-dependent crime.

2.42. We found that training exercises were undertaken nationally, regionally and locally. This helped to enhance preparedness and identify gaps in training. Very often these exercises were undertaken with partner agencies, enhancing the joint learning.

2.43. Nationally, we found some examples of identifying and circulating what was considered best practice. National and regional meetings help with this. For example, the national cyber protect network meetings and regional cyber leads meetings are both used for sharing information and good practice. Both are highly regarded by practitioners.

2.44. However, while information was shared among the people who attend these meetings, there is no clear structure to make sure that this learning informs the national picture. We found little evidence that the learning was circulated through the Cyber Crime Hub for the benefit of all cyber crime practitioners.

2.45. Among regional and local staff, there appeared to be less awareness of how to share best practice.

The Knowledge and Cyber Crime Hubs

2.46. Law enforcement agencies and partners have access to an online learning facility called the Knowledge Hub.[15] In July 2018 a specific area known as the Cybercrime Hub was established. This is intended to be "a one stop shop for all officers and staff with an interest in cybercrime, with useful resources across all 4Ps that will help everybody from experienced cyber investigators to those that have little knowledge or experience in this area".

2.47. At the time of our inspection the Cyber Crime Hub had 662 subscribers from across the UK.

2.48. The *Cybercrime Investigation Manual* has been available via the hub since January 2019.[16] It provides guidance for cyber crime investigations. There are also discussion groups.

2.49. Both the hub and the manual are welcome additions to the resources available to practitioners. However, this is still short of a clear structure for making sure best practice is shared across all law enforcement.

2.50. We found little evidence that the effectiveness of initiatives was being reviewed. When reviews took place, they were very limited in nature.

[15] The Knowledge Hub is provided by the Police ICT Company. It is a single, centrally managed platform that enables police and partners to share ICT-related information, discuss ideas and opportunities and collaborate, in order to reduce duplication, drive efficiency, and support closer working.

[16] The *Cybercrime Investigation Manual* was funded by the National Cyber Security Programme. It is not a public document. It seeks to "offer guidance to UK policing as it goes about its day to day operational response to the cyber threats we face in the UK".

3. Structure: How well do current structures help law enforcement to tackle cyber-dependent crime?

3.1. We have sought to establish whether levels of capability and capacity provided at national, regional and local levels are consistent with law enforcement's strategic approach for tackling cyber-dependent crime. We also examined whether national and local structures and partnerships enabled the effective receipt, assessment and investigation of cyber-dependent crime.

3.2. Recent funding has encouraged police forces to develop their ability to respond to cyber-dependent crime. But we found that the levels of capability and capacity are often based on the available budget rather than an understanding of the demand. Not enough forces have a clear plan to maintain these resources beyond the short term.

3.3. Most cyber-dependent crime cuts across local, regional and national policing boundaries. As a result, the current local policing model, with 43 forces operating independently, doesn't provide an effective response.

3.4. We welcome the current initiative to encourage the regional management of specialist resources in police forces. However, we found that the principles of this initiative haven't been universally adopted by all forces.

The need for reform of national, regional and local arrangements

3.5. Our *2018 Annual Assessment of Policing* contains four principal points. All are relevant to how law enforcement responds to cyber-dependent crime, but the fourth – "that there needs to be reform of national, regional and local arrangements" – is particularly pertinent.

3.6. As the assessment discusses, in the 21st century certain types of crime operate in ways that make police force boundaries less significant. Cyber-dependent crime is an obvious example.

Regional and local structures

3.7. In July 2016, the National Police Chiefs' Council agreed that the cyber crime units within regional organised crime units should be viewed as a nationally networked resource. In effect, this enabled the tasking and co-ordinating of resources that belong to police forces and regional units. This was a significant step, and we have little doubt that this has contributed greatly to the national team ethos that we found in all the units that we visited.

Regionally managed, locally delivered

3.8. In October 2017, this was taken a step further when the council agreed a model for developing cyber-dependent crime capability at the level of local police forces.

3.9. The principle of the proposal was that units should be managed and co-ordinated by regional organised crime units, but should remain located within their force. This was referred to as 'regionally managed, locally delivered'. To support this, regional co-ordinator posts were created in each regional cyber unit.

3.10. This coincided with central government funds being made available from the National Cyber Security Programme and the Police Transformation Fund to develop cyber-dependent capability in local forces and regional units. Grants could be bid for from both funds by forces and regional units that adopted the model agreed by the council.

3.11. To be eligible, units also had to meet – or commit to meeting – a minimum capability standard (see paragraph 1.43). This money was intended as seed funding to encourage police forces to develop their capabilities for fighting cyber-dependent crime.

3.12. In our view, the adoption of the regionally managed, locally delivered model was a positive step. Together with the financial incentive, it has been successful in galvanising activity, particularly at a force level. In principle, there is much to support:

- the development of a national team ethos;
- a consistent approach to referrals from the National Fraud Intelligence Bureau;
- the ring-fencing of cyber-dependent resources; and
- the introduction of performance indicators (see paragraph 1.45).

3.13. Despite this, we still found evidence of forces not fully committing to the regionally managed, locally delivered model. Some resisted the idea of being regionally managed, and the level of contact between force and regional teams varied significantly.

Limitations to funding streams

3.14. At the time the regionally managed, locally delivered model was agreed, several threats to the successful creation of specialist cyber-dependent capability in forces were identified.

3.15. One of these was a lack of dedicated resources to support the model. Funding from the National Cyber Security Programme was for forces to use to purchase equipment and training. This funding will stop after 2021. Money from the Police Transformation Fund can only be used for the creation of cyber-dependent posts, and had to be matched from local resources. This funding will stop after 2020.

3.16. After these 'cliff edge' dates, mainstream policing budgets will be expected to absorb the cost of cyber-dependent capability.

3.17. Given the continuing pressure on police budgets, there is a risk that individual forces and police and crime commissioners may choose not to invest in this area. This could happen even when they recognise that this will leave a gap in service.

3.18. The funding streams available at the time of our inspection give an incentive for forces to adopt the regionally managed model, along with its associated minimum standards and performance indicators. However, only one of the forces that we inspected had plans that guaranteed the sustaining of current resources beyond 2020.

3.19. Regional organised crime units are in a similar situation. Several of the units can't guarantee their structure beyond 2020. Senior managers told us that this uncertainty caused them difficulties. One senior officer told us that their hope was just that beyond 2020 there would be a sufficient structure to "keep the lights on".

3.20. Both the regional tasking model and the principle of regionally managed, locally delivered have merit. But ultimately, both are voluntary arrangements.

3.21. Furthermore, staff to whom the agreement relates remain under the control of local command structures, and can be diverted or removed from this broader work depending on local priorities.

3.22. We do not believe that this is an acceptable position, and believe that consideration should be given to establishing a national policing response to cyber-dependent crime. There is a precedent for this in the counter-terrorism network.

The counter-terrorism network

3.23. This is a collaboration of regional counter-terrorism units that work together, supported by a headquarters function.

3.24. In 2018, we assessed its effectiveness in providing a bridge between national and local policing in England, Wales and Scotland to reduce the risk from terrorism.[17]

3.25. Although we don't advocate the wholesale replication of the counter-terrorism network, in principle it provides a framework on which a national response to cyber-dependent crime could be based.

3.26. In our annual assessment we set out the need for "greater co-ordination at regional and national levels to make sure local factors do not inhibit improvement in policing" generally.[18]

3.27. In recent years, the ability of law enforcement agencies to respond to cyber-dependent crime, particularly at local and regional levels, has significantly improved. But, we believe that, without the creation of a formal national structure that includes local, regional and national elements, the national response to cyber-dependent crime will continue to be inconsistent.

3.28. We have deliberately avoided setting out how this structure or network should be configured. This is beyond our terms of reference and, in our view, should be left to interested parties in law enforcement, government and beyond. However, we propose some important principles:

- local, regional and national organisations all have a role to play in the response to cyber-dependent crime;[19]
- any future network should clearly reflect the division of labour between different tiers of law enforcement; and
- those responsible for the network should have clear authority to task, co-ordinate and, importantly, hold to account dedicated resources. Where appropriate this should build on the tasking powers already available to the National Crime Agency.

---

[17] *State of Policing: The Annual Assessment of Policing in England and Wales 2018*, HMICFRS, 2019, page 92.

[18] *Op cit*, page 40.

[19] In our 2015 report *Real lives, real crimes: A study of digital crime and policing* we described how, on the creation of Action Fraud, some chief constables believed that they had given up responsibility for fraud in its entirety.

Recommendation

By 1 November 2020, the Home Office, the Cabinet Office, the National Police Chiefs' Council's lead for cyber crime and Coordinator for Economic Crime, the Director General of the National Crime Agency, and interested parties should revise the current police structure for the response to cyber-dependent crime. In doing so they should consider:

- the creation of a national police cyber-dependent crime network;
- the remit of any such network;
- how the network engages with other law enforcement agencies; and
- the tasking and co-ordinating responsibilities that will be required for the network to be effective.

How well do police forces understand the demand from cyber-dependent crime?

3.29. We asked all 43 forces in England and Wales to provide some basic data.[20] This included the number of cyber-dependent investigations undertaken by the force, and how these crime reports had come to the force.

3.30. Most forces were not easily able to provide the data with any confidence:

- of those that could provide the data, eight had low confidence that the number was accurate;
- in total 17 forces were unable to tell us how many investigations they had conducted (because the data was too difficult to extract or the quality was deemed low); and
- five forces couldn't distinguish between cases that were directly reported to the force and those that came from the National Fraud Intelligence Bureau for investigation.

3.31. Our findings here are very similar to those in our inspection of fraud. And a lack of analytical capability in local forces limits their understanding of cyber-dependent crime, just as it does for fraud.

[20] Some forces provided joint submissions to reflect their collaborative approach to cyber-dependent crime. These submissions were counted as a single submission. As a result, the total number of forces is shown as 40.

3.32. None of the forces or regional organised crime units that we inspected had analysts dedicated to developing the understanding of cyber-dependent crime or to support specific cyber-dependent investigations. Even when that support was requested, cyber-dependent investigations were rarely prioritised.

National Fraud Intelligence Bureau products

3.33. A vital part of understanding demand on policing resources is making sure that crimes are correctly classified.

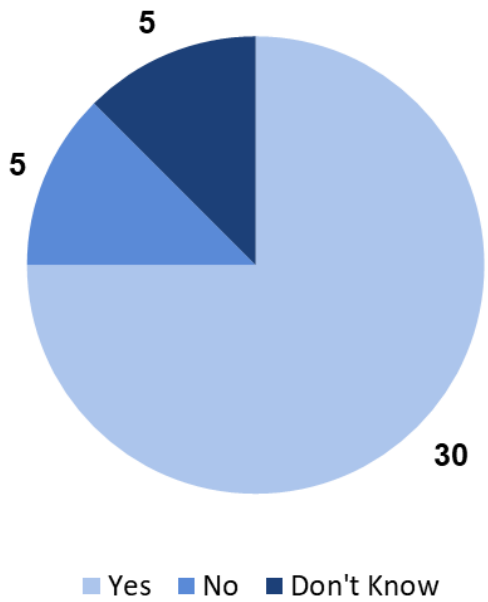
3.34. Like fraud, cyber-dependent crime isn't recorded by police forces in the way that other crimes are. It is recorded by the National Fraud Intelligence Bureau. Cases are then allocated to local forces for investigation. It is these investigations that police forces are required to keep a record of.

3.35. Forces are also required to make a record of cyber-dependent crimes reported to them that they treat as a call for service (see paragraph 6.19). They are required to report these to Action Fraud so that they can also be recorded by the National Fraud Intelligence Bureau.

3.36. The bureau has also increased how frequently it sends victim lists to forces, from monthly to weekly. This was in response to concerns that the delay in telling forces about victims prevented them from providing timely support. During our inspection, we were told that crimes contained in the weekly list were often classified incorrectly as cyber-dependent.

3.37. As part of our survey, 30 forces (75 percent) told us that they believed they had received cases that were incorrectly classified. This creates unnecessary work and duplication within the system. It also undermines confidence in the information produced by the bureau.

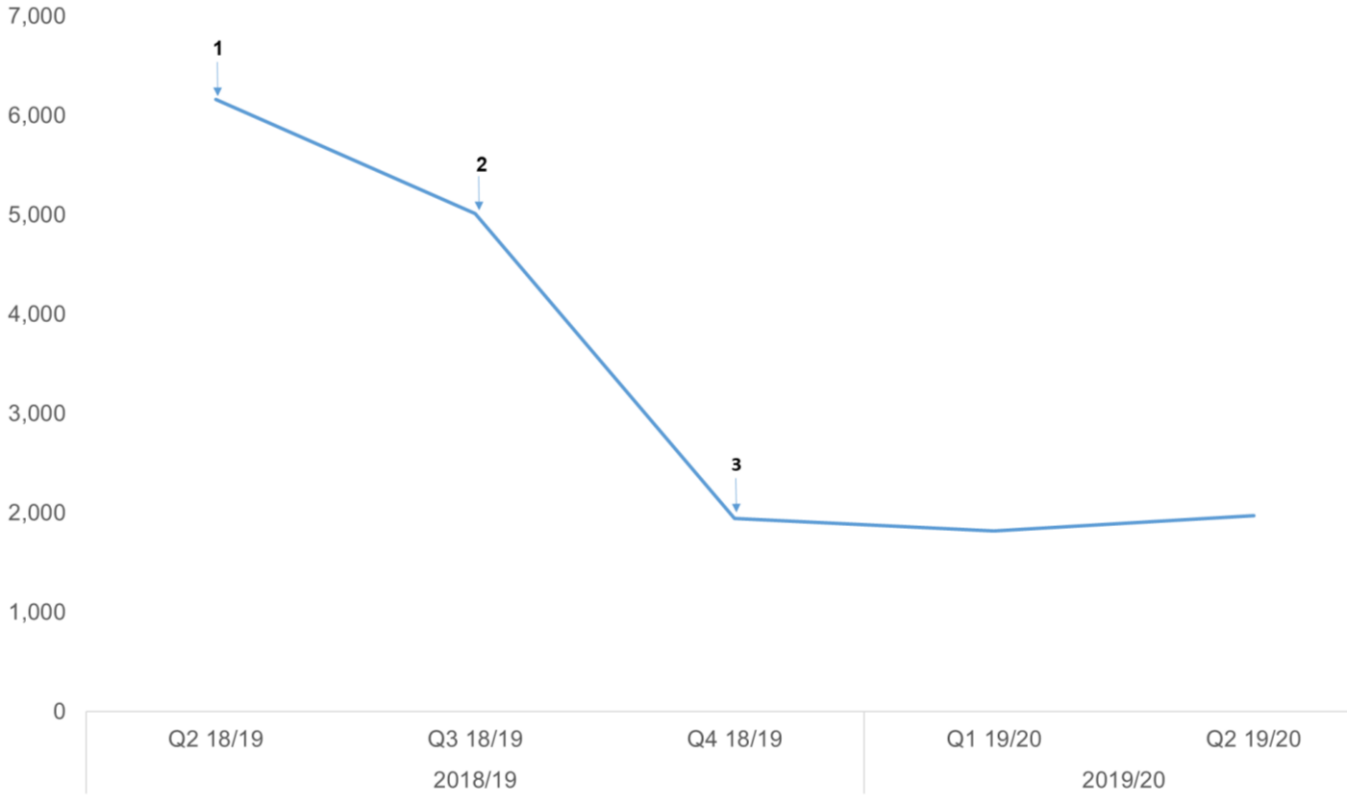
Figure 5: Number of forces receiving incorrectly classified cases



3.38. The bureau recognised this problem and introduced an additional quality assurance process in January 2019. Managers in the bureau told us that they are confident the new process means that crimes sent to forces are now correctly classified.

3.39. This change in the process is reflected in the data provided by the bureau, which shows a drop in the number of cyber-dependent crimes on the weekly list that is sent to forces.

Figure 6: Total number of cyber-dependent cases included in the weekly list (introduced in June 2018; no data prior to that)



1 June 2018 (end of Q1) **–** weekly list introduced by NFIB cyber team – all cyber-dependent crimes are sent on a weekly basis to force
2 November/December 2018 **–** certain reports within each weekly list are flagged to forces – these include those with **vulnerability concerns, mandate frauds and computer software service frauds.** All reports left in weekly lists
3 January 2019 **–** all reports are screened by NFIB cyber team – leaving only cyber-dependent crimes and those deemed to have heightened vulnerabilities. Cyber-enabled crimes are removed from the weekly lists and reclassified on the system

3.40. Bureau staff told us that the production of weekly lists enables forces to respond promptly to the needs of victims. However, some bureau staff were concerned that the list is being used to initiate investigations. They said that this could result in a duplication of effort, with local, regional and bureau staff completing similar investigative enquiries. We agree (see paragraph 5.62).

3.41. Some larger forces also reported struggling with the amount of work that the weekly reports created.

3.42. In our report *Fraud: Time to Choose* we recommended that an evaluation of National Fraud Intelligence Bureau products should be undertaken. The weekly list should be included in that evaluation.

Fraud report 2019 – recommendation 7

By 31 March 2020, the National Police Chiefs' Council Coordinator for Economic Crime should carry out an evaluation of two National Fraud Intelligence Bureau products: monthly victim lists and six-monthly force profiles. The evaluation should include:

- consulting with police forces to establish the uses to which these intelligence products are put; and
- identifying any opportunities to improve the products' utility or reduce the burden on the National Fraud Intelligence Bureau in compiling them.

How well do capability and capacity match identified and anticipated demand?

Capability and capacity within police forces and regional units

3.43. Capability is the ability of a police force or regional unit to carry out a function. Capacity is having the resources available to carry out that function. Capability may be developed through appropriate staff training, acquiring a technical ability or other specialist resource. Capacity is created by making sure that those resources, whether in the form of people or technical equipment, are available.

3.44. The availability of funding (see paragraph 1.40) meant that, at the time of our inspection, all forces and regional units had been able to increase both. This is a welcome development. However, many staff we spoke with were clear that a lot of these recent increases in capability and capacity only took place because of these funding streams, which will have ended by 2021.

3.45. We have set out (see paragraph 1.43) the minimum standards and performance indicators that forces needed to meet to be eligible for that funding.

3.46. The standards didn't set minimum staffing levels or lay down standard working practices for units. Instead, they established the minimum level of capability that forces are expected to meet. Whether the capability was shared was left to forces to decide. The standards also avoided setting levels of capacity. This has been deliberately left for individual forces to establish.

3.47. The total number of dedicated cyber-dependent staff that forces have varies between zero and ten. The average number of investigative staff across all forces is two. The number of staff carrying out a protect role related to cyber-dependent crime averages one member of staff per force. Some forces reported that they didn't have any dedicated protect staff, despite the clear requirement of the minimum standards.[21]

3.48. Furthermore, five forces were unable to distinguish between staff who worked on investigations and those engaged in protect duties.

3.49. Most forces and regional units that we inspected had carried out little or no analysis to establish the levels of demand that specialised units would need to meet. Instead, we were told that staffing levels were set using 'professional judgment'. More often than not, the prevailing consideration was what budget was available.

3.50. The level of demand from cyber-dependent crime varies from force to force. We asked the forces we inspected to provide details of 20 phone calls to the force reporting cyber-dependent crime (from the six months prior to our investigation), and ten cyber-dependent investigations (from the previous year). Some forces couldn't provide this many examples.

3.51. We found that few forces had considered the capability and capacity available in other forces within their region, or the potential benefits of a shared regional resource. This resulted in duplication of resources and effort, with identical activities taking place in neighbouring forces. Conversely, in most of the forces and regions we inspected, worthwhile activity such as analysis wasn't available to investigators.

3.52. The introduction of a more formal national police network could go some way to removing these inefficiencies.

Action Fraud and the National Fraud Intelligence Bureau

3.53. We found a similar situation in Action Fraud and the National Fraud Intelligence Bureau. Once again, we were told that resources were matched to budget and not the level of demand. For example, the current budget allows the employment of 79 staff within the Action Fraud call centre. Senior managers are aware that these staffing levels will result in 40 percent of callers hanging up before their call is answered. This means that approximately 20,000 calls per month are going unanswered.

[21] This data excludes eight forces, either because their numbers skewed the data or because they couldn't provide the data in the format required. Numbers reported have been rounded to the nearest whole number.

3.54. Staff at Action Fraud were generally trained appropriately for their role but (as reported in *Fraud: Time to Choose*) high staff turnover has an adverse effect. It was clear that staff wanted to do a good job, but they told us that they felt unaware of how the other parts of the process worked.

3.55. Short-term funding is also a problem within the National Fraud Intelligence Bureau. Of the five functions within the bureau's research and analysis department, three are funded by the National Cyber Security Programme. The nature of the funding prevents any long-term planning.

National Crime Agency – National Cyber Crime Unit

3.56. The National Crime Agency has a good understanding of the capability and capacity it needs to meet current and future demand. Capacity-building takes place within a governance framework. Progress against the plan is monitored and authorised at a senior level.

3.57. We also found that the strategic approach to developing capability is informed by good practice – what works. Overall, we found that the way the agency is developing its cyber-dependent capability is coherent and structured.

3.58. However, similar to those units in forces and regions, the National Cyber Crime Unit relies on funding from the National Cyber Security Programme. Over 60 percent of the unit's capability is funded in this way.

Recruitment and retention of staff

3.59. Several forces and regional units told us that they find it challenging to recruit and retain staff. This was also the case for the National Cyber Crime Unit. At the time of our inspection, about 30 percent of the unit's roles were vacant.

3.60. In response, the National Crime Agency has launched a number of initiatives to boost recruitment. These include cyber apprenticeships, and sandwich courses for university students with the offer of employment at the end of their degree.

3.61. This problem is made worse by the high level of staff turnover. One large force told us that the turnover rate of cyber-dependent specialist staff was significantly higher than for other police roles.

3.62. There are several possible reasons for this, which include the funding structure, which means that specialist staff cannot be sure their roles will continue, and a lack of a clear career progression path.

3.63. However, there is little doubt that the most significant issue is pay. Those working in cyber crime work closely with the private sector where salaries are far higher. Private companies and organisations regularly recruit staff from law enforcement agencies. This is costly for law enforcement agencies. Over the period of their employment, specialist investigators represent a substantial investment.

3.64. It also has practical implications for those agencies – increased workloads for staff, and disruption to efficient teamwork and effective partnerships – all of which have a negative effect on their ability to combat cyber-dependent crime.

3.65. However, it isn't simply a matter of pay disparity between the private and public sectors. We saw examples of the widely differing rates of pay for identical roles across government and even law enforcement agencies. In some cases, the difference could be as much as £10,000 per year.

3.66. There is no simple answer to this problem, and law enforcement agencies need to keep exploring innovative ways of attracting the best people into specialist roles.

3.67. One senior officer told us: "agencies have to take a more permeable approach to recruiting". In practice, this means accepting that specialist staff are likely to move in and out of law enforcement during their careers. In recognising this, the police and national units should ensure that routes from the private sector and other organisations back into specialist police roles are not encumbered by unnecessary regulations and protocols.

Use of cyber specials and cyber volunteers

3.68. One way to develop the capability and capacity of units is to use cyber specials and cyber volunteers (special constables and other volunteers with cyber expertise). These can help law enforcement with knowledge and expertise gained in the private and charitable sectors as well as academia. However, yet again, we found that the use of this valuable resource by forces and regional units was inconsistent.

3.69. For example, one force we inspected had a very effective volunteer programme. It used cyber specials and volunteers to spread knowledge and awareness. The force held joint training days with volunteers and permanent staff, which included using software developed for the force by a cyber special.

3.70. Conversely, investigators in one force were less positive, with staff raising doubts about the cost-effectiveness of mentoring volunteers who they deemed unsuitable. In this force we found little evidence of a culture that promoted the use of cyber volunteers.

3.71. The National Police Chiefs' Council's lead for cyber crime has encouraged the use of both special constables and volunteers in this area. For example, within the online facility known as the Knowledge Hub (see paragraph 2.46) there is a specific area aimed at the recruitment and use of cyber specials and volunteers.

3.72. The recruitment and deployment of force cyber specials and cyber volunteers was included in the minimum capability standards set by the Capability Project Board. At the time of our inspection, 16 forces and three regional units told us that they didn't use either special constables or volunteers to tackle cyber-dependent crime. We are clear that this is a missed opportunity.

Area for improvement 1

Chief constables should evaluate the use that their force makes of cyber specials and volunteers to ensure that they are used effectively.

Are the necessary partnerships in place to tackle cyber-dependent crime?

3.73. Given how prevalent and widespread cyber-dependent crime is, partnerships between the law enforcement agencies and other organisations are extremely important.

3.74. Encouragingly, we found that agencies worked well with international partners, industry, local government and third sector organisations, either to protect the public or to give additional support to victims. At the national level, there are various well established partnerships.

3.75. However, at the local level, although partnerships with other police forces and law enforcement agencies are well established, there was less evidence of arrangements with industry and other organisations outside law enforcement.

National and international partnerships

3.76. The National Cyber Crime Unit works closely with the National Cyber Security Centre to represent the UK's interests with international partners. This includes both government and private organisations who can provide an operational response to incidents, including the development of appropriate advice and messages to victims.

3.77. As part of this process, the National Cyber Crime Unit plans to develop its working relationships with international partners to help meet its priority of tackling the threat of cyber crime to the UK. This includes engagement with international bodies such as the FBI and Europol. For example, the unit is a member of the Global Forum on Cyber Expertise.

3.78. The unit is able to undertake this role largely thanks to funding from the National Cyber Security Programme.

Europol

3.79. The European Union Agency for Law Enforcement Cooperation, better known as Europol, is the European Union's law enforcement agency. Based in The Hague, Netherlands, Europol uses analysis to support the law enforcement agencies of European Union member states in combatting serious and organised crime, including cyber-dependent crime.

3.80. The National Cyber Crime Unit is a member of the Joint Cybercrime Action Taskforce at Europol. Among other things, the taskforce enables effective information sharing between jurisdictions. The taskforce has 18 members, including countries from both inside and outside the European Union. We were told that the UK is considered a main contributor to the taskforce.

3.81. Europol uses the information-sharing platform known as the secure information exchange network application (SIENA) to share information between member states. At the time of our inspection, SIENA was available to all UK law enforcement agencies through regional organised crime units. Europol also facilitates joint investigations and collaboration between agencies.

3.82. We were told that over 80 percent of investigations by regional organised crime units make use of SIENA and gain useful information as a result.

Regional and force arrangements

3.83. We found evidence of partnership working at the local and regional levels but, once again, this varied in nature. In the more advanced forces, we were provided with examples of working closely with industry, academia, and financial institutions. At a more local level, some forces were developing digital security centres.

3.84. However, in other forces, partnerships were limited to working relationships and information sharing with other forces or law enforcement agencies. The relationships that did exist were general in nature and were not focused on the threat from cyber-dependent crime.

4. Protect: How well do police forces help to protect individuals and businesses from cyber-dependent crime?

4.1. For this part of the inspection, we looked at the advice that forces give to people and businesses about how to protect themselves from cyber-dependent crime.

4.2. We also considered whether, and how, forces identify people and businesses who may be at increased risk from cyber-dependent crime, and what they do to protect them from it.

4.3. National organisations do good work in identifying emerging threats. Regionally, there is a well established network that ensures that initiatives promoting protection against cyber-dependent threats are delivered. And forces are increasingly proactive in communicating protection messages. But these messages are not being consistently co-ordinated. More needs to be done to avoid duplication and omission, and to evaluate how effective these campaigns are.

Roles and responsibility

4.4. The National Cyber Security Centre is the lead organisation at a national level for the development of cyber-dependent protect advice. The centre has several teams that provide guidance to: government departments; organisations that support the national infrastructure; financial institutions; and businesses including small-to-medium enterprises.

4.5. The National Cyber Security Centre website has up-to-date information about new threats, and links to sources of information for those needing advice. The centre works closely with the National Cyber Crime Unit to mitigate the effect of cyber attacks and make sure that organisations can respond effectively. This includes the use of Cyber Security Information Sharing Partnerships known as CiSP.

4.6. The responsibility for distributing protect advice nationally sits with City of London Police, working with the National Police Chiefs' Council lead for cyber crime. It is responsible for making sure that the advice prepared by the National Cyber Security Centre is provided in a timely way to regional units, forces and the public. It does this through the National Fraud Intelligence Bureau and the public-facing elements of Action Fraud.

4.7. The availability of funding streams has enabled the creation of a network of cyber protect staff across regional units and forces. These officers and staff are trained to give protect advice about cyber crime as part of the National Cyber Crime Strategy.

4.8. The development of the protect function is more established in some forces than others. In one force we inspected, a protect officer had been in place for over three years. But in other forces, despite available funding, protect posts still have to be filled and those forces rely on regional resources. This is a further example of a lack of national consistency.

National campaigns

4.9. Police forces, the National Crime Agency and the government have promoted Get Safe Online. This is a national campaign run in partnership betweeen government and private sector organisations from banking, retail, internet security and other areas. It gives practical advice about how people can protect themselves and their businesses against fraud, identity theft, viruses and many other problems encountered online.

4.10. The National Fraud Intelligence Bureau brings together other agencies to develop consistent advice, campaigns and alerts that are distributed nationally through the cyber protect network.

4.11. In theory, the use of the protect network should bring consistency to the advice that local officers give to their communities. However, the timing of advice and the targeting of specific groups was often left to the judgment of individual officers rather than being co-ordinated.

4.12. And, while we found some good examples of national campaigns and alerts being adapted with local perspectives, some forces just share the messages on social media. Staff in one force told us that the level of effort in publicising national campaigns varied. If the subject was important to the force then the campaign would be supported, but if not the force would simply “go through the motions”.

4.13. In another, the protect officer told us that force processes prevented the running of any national campaigns that didn’t reflect local issues. This prevented the force from publicising awareness-raising campaigns from the National Fraud Intelligence Bureau.

4.14. We found little evidence at any level of any evaluation of whether protect advice or campaigns were effective, or whether they changed the behaviour of the targeted audience.

Protect advice at first point of contact

4.15. Action Fraud's call handlers have processes for giving advice to the public and organisations to help them avoid becoming repeat victims of cyber-dependent crime.

4.16. While this is often basic advice, such as changing passwords or dealing with particular viruses, it can be reassuring to victims. Call handlers also give details of approved organisations that might be able to provide further help. The requirement to provide protect advice is included in the initial training of Action Fraud call takers and is monitored in the quality assurance of calls.

4.17. This structured approach was less evident in forces, which were less likely to provide specific training in cyber-dependent crime to call takers. In our review of telephone calls to police forces, we found that protect advice was only given in a third of cases.

Protect activity: Individuals and businesses

4.18. Despite the problems we have outlined, we did find numerous examples of agencies engaging with business, government, schools and the general public to give protect advice. Protect staff in some forces worked with local banks to hold cyber awareness days. Others used cyber volunteers to publicise protect messages to local schools, community groups and businesses. Some regions also carry out stress-testing exercises with organisations to test their vulnerability to cyber attacks.

4.19. City of London Police have developed the Cyber Griffin initiative, which is available to businesses within the force area. It has four levels: baseline briefings; business continuity training; table-top exercises; and incident response training. The Metropolitan Police Service has also produced *The Little Book of Cyber Scams*, which gives individuals and businesses easy-to-follow guidance on protecting themselves from cyber crime.

People and businesses at increased risk of cyber-dependent crime

4.20. While giving general advice is an essential part of preventing cyber-dependent crime, it can be more effective to focus that advice towards people who are at increased risk.

4.21. In general, we found that local protect activity focused on types of crime rather than being aimed at vulnerable categories of people. In most cases local campaigns were based on the judgment of staff rather than any analysis. Even when groups of people or businesses associated with trends in offence types could be identified, they were rarely targeted with advice about protecting themselves.

5. Investigation: How well does law enforcement investigate cyber-dependent crime and deter potential offenders?

5.1. During our inspection we have considered the following questions. Does the central reporting process help in the investigation of cyber-dependent crime? How well do the police prioritise, task and respond to cyber-dependent crime? And is there enough emphasis on engaging with those involved in cyber-dependent crime?

5.2. Because of the international nature of cyber-dependent crime, a centralised process is the only practical response. However, we found problems with the effectiveness of the process regarding timeliness, quality and duplication of effort with delays in the system inhibiting investigations.

5.3. Our conclusion is that the way forces are responding to cyber-dependent crime is improving, but more needs to be done.

5.4. The introduction of a national tasking process and regional co-ordinators has provided some consistency in when, how, and to what level, cyber-dependent crime is investigated by regional and local teams. Also, establishing national performance indicators has provided some way of measuring performance.

5.5. However, each of these developments has limitations, and there remains too much variation in how cases are approached, particularly at a local level. At the regional and force level we found little evidence of effective targeting of people involved in this type of crime.

Does the central reporting process help in investigating cyber-dependent crime?

Are there alternatives to a central reporting system?

5.6. As well as assessing the existing system for reporting cyber-dependent crime, we have considered whether there are any viable alternatives to a central reporting system.

5.7. In our report *Fraud: Time to Choose*, we considered whether City of London Police was the most suitable organisation to oversee the central reporting process. We concluded the following:

- Both Action Fraud and the National Fraud Intelligence Bureau fulfilled their respective functions but “there are unacceptable problems with the current arrangements”.

- In the absence of any obvious alternatives, City of London Police should remain as the lead force for fraud and should keep responsibility for Action Fraud and the National Fraud Intelligence Bureau.

- All parts of the central reporting process should be held to account for their effectiveness and efficiency.

5.8. This remains our view.

Project Fortis

5.9. Later in this report (see paragraph 6.6), we outline some of the issues that victims face when trying to report cyber-dependent crime. These include a lack of awareness of Action Fraud's role in the reporting of cyber-dependent crime. In some cases, this could account for the high levels of under-reporting of this type of crime.

5.10. Reporting cyber-dependent crime can be even more complicated for businesses and large organisations. This is due to the number of law enforcement agencies and other statutory bodies that they may need to inform. This can be time consuming and expensive, especially with complex cases.

5.11. At the time of our inspection, the National Cyber Security Centre, the National Crime Agency, City of London Police and other national agencies were using funding from the Cabinet Office to address this. They are developing an online platform called Project Fortis, which would allow victims to report cyber incidents to all law enforcement agencies at the same time. This would streamline the reporting process and provide what was referred to as a "single front door" to law enforcement agencies.

5.12. However, this project was still in the early stages of development, and several questions remained. For example, whether Project Fortis would be used solely for businesses, and if any new systems would interact with current Action Fraud and National Fraud Intelligence Bureau processes.

Recording information

5.13. During the inspection, we reviewed calls to Action Fraud and the records created as a result. We found that staff at the Action Fraud contact centre had accurately recorded the details of most incidents.

5.14. Inaccurate or incomplete information makes it hard to draw connections between crimes or to identify lines of enquiry. Recognising this, calls to Action Fraud are reviewed by supervisors to check for errors and to encourage the spread of best practice.

5.15. However, online reports are not subject to the same immediate review of their quality, and victims entering their own information can lead to inaccurate and misleading reports.

Delays within the National Fraud Intelligence Bureau process

5.16. All reports of cyber-dependent crime received by Action Fraud are assessed by the bureau's team of crime reviewers. Initially, the reviewers consider whether the reports are correctly classified as a cyber-dependent crime. Cases that have been incorrectly classified are redirected to the appropriate unit within the bureau.[22]

5.17. Those that meet the definition of cyber-dependent crime are included in weekly lists that are sent to each force (see paragraph 3.38). The lists give each force limited details of every victim of cyber-dependent crime within its area. They were initially intended to enable forces to respond quickly to the needs of victims including giving protect advice.

5.18. Following this initial triage process, reviewers then consider reports for lines of enquiry that are viable. Cases are prioritised for review according to the vulnerability of the victim. When viable lines of enquiry are identified, reviewers carry out intelligence and other checks before disseminating the case to the relevant force (see paragraph 1.14).

5.19. Following the updating of the Know Fraud system in October 2018, a significant number of reports of potential fraud and cyber-dependent crimes have been held in quarantine. In some cases the automated system mistakenly identified reports as containing malicious coding. In April 2019, we were informed that approximately 9,000 reports were being treated in this way – although by July 2019 this had been reduced to approximately 6,500.

5.20. In these quarantined cases, victims haven't received confirmation that their report has been received. Nor have they been reviewed for viable lines of enquiry or forwarded to forces for either victim care or investigation.

5.21. At the time of our inspection City of London Police told us that they were actively working to solve this problem.

[22] Occasionally, some cyber-enabled cases, such as fraud, may still be disseminated if reviewers consider that the victim has heightened levels of vulnerability.

Area for improvement 2

With immediate effect, City of London Police should provide the Home Office with details of how the force intends to address the issue of reports being held in quarantine within the Know Fraud system. Furthermore, the force should also identify its proposals to prevent a re-occurrence.

How well do police respond to and prioritise allegations of cyber-dependent crime?

5.22. The national response to cyber-dependent crime works well. National agencies have a clear understanding of their roles and responsibilities.

5.23. However, the response from police forces is less consistent. The definitions used by forces to identify calls for service (see paragraph 6.19) about cyber-dependent crime vary. They often include the vulnerability of the victim, although this is normally only applied to individuals. As a result, businesses are sometimes treated differently, which can affect both when and how their crime is investigated.

National prioritisation

5.24. Cyber attacks are categorised by how severe they are. Each incident is given one of six categories of severity. This is then used to decide how best to respond. The levels are:

- Category 1 – national cyber emergency
- Category 2 – highly significant incident
- Category 3 – significant incident
- Category 4 – substantial incident
- Category 5 – moderate incident
- Category 6 – localised incident

5.25. Category 1 to 3 attacks receive the highest level of response. This involves cross-government co-ordination and close co-operation between the National Cyber Security Centre and the National Crime Agency.

5.26. The response to category 4 attacks is also led by the security centre, but it can involve the use of regional cyber crime unit resources. Responding to category 5 and category 6 attacks is generally the responsibility of regional and local units.

5.27. We found this process, and the subsequent tasking process, to be well understood across all agencies.

The initial local response to allegations of cyber-dependent crime

5.28. Despite the centralised fraud-reporting process, not all victims of cyber-dependent crime report their case to Action Fraud. Instead, as mentioned previously, some report to a local police force, either by telephone or online.

5.29. When receiving calls from members of the public, forces should use the Home Office Counting Rules for cyber-dependent crime to decide whether they need to record the incident and respond to it as a call for service (see paragraph 6.19), or if they should refer the victim to Action Fraud.

5.30. We found that forces were generally good at identifying calls for service. Often, they extended the Home Office Counting Rules definition to include the vulnerability of the victim and the opportunity to recover evidence.

Vulnerable victims and recovery of evidence

5.31. Securing and preserving evidence at an early stage is an essential part of a successful investigation. And when a crime is reported to the police and resources are allocated to that crime, the police are generally good at this.[23]

5.32. For cyber-dependent crime reported to Action Fraud, the process is different. As Action Fraud is a contact centre, its call handlers cannot secure or preserve evidence. In general, call handlers give advice to victims about securing and preserving evidence themselves, such as documents or computer records.

5.33. Some forces treated a report of cyber-dependent crime as a call for service if they identified that the victim was vulnerable. Having dealt with the victim's needs, the cases were recorded on local systems and investigations started. In many of these cases, it would have been more appropriate to refer the case to Action Fraud. Clarity for officers and staff is needed.

[23] *PEEL: Police effectiveness 2017: A national overview*, HMICFRS, 2018, page 45.

5.34. A further inconsistency arises from the use of the THRIVE model for assessing the vulnerability of victims. We found that businesses were less likely to be considered vulnerable, despite the National Fraud Intelligence Bureau Annual Assessment 2018–2019[24] identifying businesses as being at a high risk of becoming victims.

5.35. This means that, in some force areas, businesses (normally small and medium-sized enterprises) are treated differently from other victims. This can cause delays in support being given and adds to levels of dissatisfaction with the response by law enforcement.

5.36. Equally, when forces start investigating reports that don't amount to a call for service, the assessment, review and allocation process managed by the National Fraud Intelligence Bureau is undermined.

5.37. This was highlighted in our report *Fraud: Time to Choose*. In that report, we made it clear that we don't want forces to stop supporting vulnerable victims or giving a good level of service to victims generally. However, clarity for officers and staff is needed. As a result, we made the following recommendation, which is equally applicable to cyber-dependent crime.

Fraud report 2019 – recommendation 11

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should issue guidance to police forces in relation to fraud-related calls for service as described in the Home Office Counting Rules. The advice should make clear to forces the circumstances in which they are expected to intervene, and the circumstances in which they may refer the case direct to Action Fraud. The advice should also make clear how:

- responses to reports of fraud may adequately meet the needs of the victims;
- vulnerable victims should be identified and dealt with appropriately; and
- reports of fraud should be efficiently referred to Action Fraud.

[24] Unpublished.

How well do police forces deal with allegations of cyber-dependent crime?

Tasking and co-ordination

5.38. Most cyber-dependent investigations are allocated directly to forces by the National Fraud Intelligence Bureau. However, there is a further tasking process for investigations that are more complex or categorised as having a higher level of severity.

5.39. These cases are dealt with by the Triage, Incident Coordination and Tasking (TICAT) unit, which is part of the National Cyber Crime Unit. TICAT, working with the National Cyber Security Centre, receives reports of cyber-dependent crime from the National Fraud Intelligence Bureau and allocates the investigation to the most appropriate law enforcement agency.

5.40. The process, like TICAT itself, is highly regarded by practitioners and we found that it generally works well.

5.41. As we have set out previously (see paragraph 3.7), in July 2016, chief constables agreed that the cyber crime units within regional organised crime units should be viewed as a nationally networked resource. They also agreed to adopt the regionally managed, locally delivered model.

5.42. We understand that there is an aspiration to extend this agreement to cyber-dependent crime units in local forces so that they too can be part of a national tasking process.

5.43. While this makes some sense, there are obvious limitations to what is, ultimately, a voluntary arrangement (see paragraph 3.20). For example, we found that one regional unit had declined to accept any tasks from the national process for over a year, on the basis that its staff were committed to other duties.

5.44. We also found several examples of forces not committing to the regionally managed, locally delivered model agreed by chief constables. The level of influence of the regional co-ordinator varied across the regions, and as a result the tasking and co-ordination between local and regional units wasn't as effective as it should have been.

Investigation – quality and outcomes

5.45. As discussed in chapter three, most forces have some form of cyber-dependent crime capability. This means that, in theory, offences are investigated at the appropriate level by appropriately trained staff.

5.46. Help is also available from regional units – although we found that this was very often limited to advice and guidance rather than hands-on support with specialist skills, equipment and expertise.

5.47. As highlighted throughout this report, most regional and local cyber crime units have no dedicated analytical capability to produce threat assessments and problem profiles or to help with day-to-day investigations.

5.48. Our inspection examined 103 cases that were investigated by local forces and 26 cases that were investigated by regional teams or the National Crime Agency.[25] We found considerable variation in the quality of the investigations and their subsequent outcomes. The investigations by the regional and national teams were, in our view, of considerably better quality overall than those done by local forces.

5.49. Two-thirds of the local force investigations had been undertaken by a dedicated team. The remainder were investigated by non-specialist units, including patrol and neighbourhood staff.

5.50. We found that 80 had been finalised with no further action being taken, and only three had resulted in a charge or a caution. Thirty-four cases gave possible opportunities to disrupt future criminal activity, but these had only been considered on seven occasions. In most cases there had been no supervisory review. None of the 103 cases had aims and objectives set by force investigators at the start. In most cases, the possibility of collaborating with partners had not been considered.

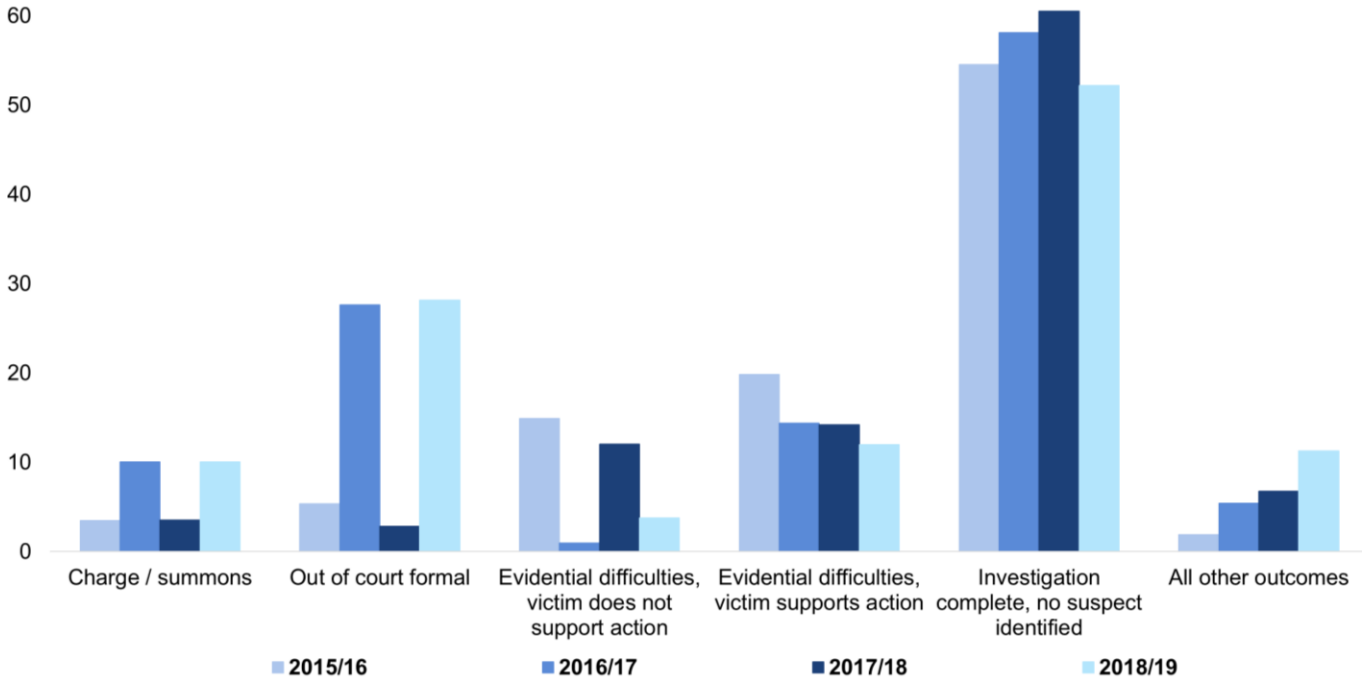
5.51. In contrast, the cases investigated by the regional or national team were better structured. Their investigation aims and objectives were identified and recorded at the outset. Most of the cases had been appropriately reviewed by supervisors and opportunities to disrupt future criminal activity had been considered. We found that in most cases the needs of the victim had been assessed effectively, and partners had been used to support the investigation.

Outcomes

5.52. The most common outcome for cyber-dependent crime cases disseminated to forces and regional units is investigation completed – no suspect identified. Between 2015 and 2019, this has consistently accounted for between 52 percent and 61 percent of outcomes. Offender charged or summonsed is consistently one of the least likely outcomes nationally.

[25] We recognise that our sample size of investigations is not large enough to draw statistically valid conclusions.

Figure 7: Percentage of assigned outcomes by crime type



5.53. However, because of the nature of cyber-dependent crime, not every investigation can or should result in offenders being charged or similar. For example, large numbers of offences are committed by criminals operating outside the UK's jurisdiction, specifically in countries with which the UK has no arrangements to allow investigations to take place.

5.54. For this reason, police forces should not be judged based only on what happens to the offender. Instead, their ability to provide an effective response across all elements of the 4Ps (see paragraph 2.4) is the method by which their performance should be considered. This includes how effective the investigation is.

Performance indicators

5.55. As we have set out earlier (see paragraph 1.45) performance indicators for forces and regions have been set by the National Force Specialist Cyber Capability Project Board.

5.56. We welcome these as an important first step in bringing consistency to the police's response to cyber-dependent crime. All the forces that we inspected were aware of them and told us that they complied with them. All but one force told us that they investigated 100 percent of cases referred to them by Action Fraud. However, we do have some concerns.

5.57. The performance indicators were established as a way of ensuring a quality response to victims of cyber-dependent crime. They also make sure that value for money is obtained from the Police Transformation Fund and National Cyber Security Programme. In theory, units that don't achieve the indicators (along with the minimum standards) risk having to return money to the fund. However, we are not aware of any process for returning money that has already been received. And once those funding streams cease to exist, that incentive to comply with national standards will no longer apply.

5.58. And the term 'investigation' isn't clearly defined. During our inspection we found different approaches, some of which fell short of what we would consider to be an investigation.

5.59. During our case review we found examples of crimes with relatively simple lines of enquiry that could have been followed. Instead, the investigation had been ended and no further action taken. Ultimately, it is down to forces to decide whether a case has been properly investigated. To a large degree they are marking their own homework.

5.60. In our view, an investigation should involve a thorough and effective review of the evidence followed by an assessment of lines of enquiry that could reasonably be followed up. Any assessment should be able to withstand scrutiny.

5.61. The role and influence of the regional cyber co-ordinator (see paragraph 3.9) varies across forces. All co-ordinators should have an overview of the cyber-dependent cases sent to forces in their region by the National Fraud Intelligence Bureau. And, in general, they do. However, some simply keep a record of investigations, while others are more engaged.

5.62. In some cases, regional co-ordinators are central to the creation of investigation plans. This has clear value: it gives an independent element to the reviews of investigations, and supports the regionally managed, locally delivered approach. We also found that the nationally agreed approach to investigating "100 percent of Action Fraud referrals" (see paragraph 1.45) had changed. Initially forces focused on those case that had been referred to them for investigation. However, more recently forces had adopted the National Fraud Intelligence Bureau's weekly list.

5.63. Forces are using the list to start investigations without any other reference to the bureau, or the information that may be held within Know Fraud (to which they have no direct access, see paragraph 1.25). We were told that this is done on the basis of improving the timeliness and quality of the service given to victims.

5.64. The result of this is that units are starting investigations on cases that have not been through the bureau's review process including some cases that would not have been sent out for investigation.

5.65. This can lead to staff conducting investigations into suspects who live many miles away in a different force area. This, in turn, can result in a duplication of effort between bureau reviewers, the investigating unit and other forces who may have started similar enquiries. A situation that the centralised reporting process was designed to prevent.

Area for improvement 3

The National Police Chiefs' Council's lead for cyber crime and Coordinator for Economic Crime should revise the key performance indicators contained within the council's minimum capability standards for force cyber crime units. The revised standards should make clear:

- the minimum standards for investigation;
- the role of regional cyber crime co-ordinators in the recording, management, and review of cyber crime investigations; and
- the use of the weekly list provided by the National Fraud Intelligence Bureau to comply with the performance indicators.

How well do police forces recognise and interact with those involved with cyber-dependent crime?

5.66. To succeed in disrupting and investigating serious and organised crime, forces must understand the threat clearly, map organised crime groups accurately, and prioritise their activity against them. Preventing individuals from becoming involved (or continuing their involvement) in cyber-dependent crime is also an important role of law enforcement.

Organised crime groups

5.67. Law enforcement agencies use MoRiLE scoring to assess how much risk these groups present. The ones with the highest risk score are given priority of investigation.

5.68. We were repeatedly told that the process is not an easy fit for cyber crime offenders. Practitioners told us that cyber-dependent crime doesn't score highly on the MoRiLE system. As a result, it is rarely prioritised above organised crime groups involved in drugs and firearms offences.

5.69. One investigator told us that trying to map organised crime groups involved in this type of crime was “like trying to plait smoke”. The failure to identify and map organised crime groups involved in cyber crime results in missed opportunities to target offenders. A consistent approach for practitioners to follow is needed.

Management of offenders

5.70. We found limited activity in forces and regional units to prevent people from becoming involved in cyber-dependent crime, or to prevent further offences. Although worthwhile, this was generally limited to work in schools to discourage young people from becoming involved in cyber offending, supported by national media campaigns.

5.71. Several forces didn’t have dedicated staff focusing on either prevent activity or the management of those involved in cyber-dependent crime. Nor did we find any evidence that offenders were routinely referred to the integrated offender management process, a joint initiative by local and partner agencies that identifies and manages the most persistent and problematic offenders.

5.72. In addition, little use was made of prevention orders. In April 2019, we were told that only three to four Serious Crime Prevention Orders had been issued to cyber crime offenders across all 43 forces in England and Wales.

5.73. At national level the picture is better. The National Cyber Crime Unit has a team dedicated to prevent work. It conducts debriefs with offenders and focuses on the offenders that cause the most harm.

5.74. In general, we found that the prevent element of the national strategy is less developed, particularly in regions and forces, than the protect activity, especially in terms of resources.

6. Victims: To what extent does law enforcement consistently provide a high-quality response to victims of cyber-dependent crime?

6.1. Victims who report cyber-dependent crime are generally satisfied with the service that they receive. However, whether victims are given good advice on protecting themselves from further cyber-dependent attacks varies depending on who they contact.

6.2. It can also be confusing for victims to understand where and how to report cyber-dependent crime. We found that many victims were unaware of Action Fraud's existence, role and purpose.

6.3. Furthermore, victims are often given confusing and misleading information about how (or whether) their case will be investigated and, if it is, how it is progressing.

Sources of evidence

6.4. We used information from a survey conducted by the University of Portsmouth[26] to help us understand victims' perceptions of the support and advice they received from Action Fraud and the police. The university carried out an online survey of 252 victims of cyber-dependent crime, and a further 52 qualitative interviews with victims who contacted Action Fraud.

6.5. We also carried out a review of 50 calls to Action Fraud and 182 calls to police forces from victims reporting cyber-dependent crime.

How easy is it to report cyber-dependent crime?

Action Fraud

6.6. The victim survey highlighted that many victims hadn't previously heard of Action Fraud and had to be directed to it. They found it confusing that the name doesn't refer to cyber-dependent crime.

6.7. Just under half of the surveyed victims reported their matter directly to Action Fraud. Many victims didn't understand the Action Fraud process and contacted the police instead.

[26] 'Victims of computer misuse and cybercrime', Button, M, Blackbourn, D, Sugiura, L, Kapend, R, Shepherd, D and Wang, V., 2019. Unpublished at time of inspection.

6.8. However, victims told us that, once they established who they should report their crime to, they found the process easy. The confusion relating to the role of Action Fraud was identified in our report *Fraud: Time to Choose*. It is equally applicable to cyber-dependent crime.

Fraud report 2019 – recommendation 14

With immediate effect, the National Police Chiefs' Council Coordinator for Economic Crime should:

- carry out (and subsequently evaluate) a campaign to raise the public awareness of the existence and role of Action Fraud; and
- provide chief constables with a description of the role of Action Fraud for uploading to force websites.

Direct to Action Fraud by telephone

6.9. Action Fraud's advisers are available between 8.00am and 8.00pm Monday to Friday, with a limited service for general enquiries from 8.00pm to 12.00 midnight. If they call out of hours, people are advised to call during the core service hours or use Action Fraud's online reporting tool. Reports from members of the public of a live cyber attack, during normal working hours, are dealt with by the general call takers.

6.10. There is a 24-hour reporting service for live cyber attacks against businesses, charities and other organisations. These reports are put through to dedicated call takers who use a specific cyber crime template. This helps to establish the nature of the incident and whether it is a live cyber case.

6.11. In our review of calls to Action Fraud we found that the details recorded by staff were accurate in 98 percent of cases. The University of Portsmouth survey also found in their qualitative interviews that those reporting to a call taker generally had a positive experience.

6.12. However, we found significant delays were experienced in victims receiving a response on the telephone, and that 40 percent of calls were abandoned before they were answered. This equates to 20,000 calls from the public (relating to both cyber crime and fraud) being abandoned per month. Lengthy waiting times and high abandonment rates are indicators of a process that is both inefficient and ineffective.

6.13. At the time of our inspection, senior managers within Action Fraud had no way of understanding how satisfied (or otherwise) people who used their service were.

6.14. This was identified in our fraud report *Fraud: Time to Choose*, and it is equally applicable to cyber-dependent crime.

Fraud report 2019 – recommendation 15

With immediate effect, the National Police Chiefs' Council Coordinator for Economic Crime should take steps to remedy the absence of published performance indicators at Action Fraud. As soon as practicable, performance indicators should be set in relation to, for example, call handling waiting times and abandonment rates, online reporting and victim satisfaction levels. Thereafter, information on performance against those indicators should be published.

Direct to Action Fraud online

6.15. As well as by phone, cyber-dependent crime can also be reported via Action Fraud's online reporting process. The website also has a webchat facility, which is available at all times. This can be used to help complete the online form or to seek advice. It cannot be used to report fraud or cyber crime or to get updates about previous reports.

6.16. Online reporting is clearly an efficient and effective way to report this crime and reduce the demand on call takers. In the qualitive interviews victims made positive comments about the online reporting tool. But there were also negative comments, particularly about the time it takes to complete the forms.

6.17. One issue with the online tool is the reliance on victims to correctly identify the type of crime they have been a victim of. Self-reported cases often include incorrectly classified crimes and inaccurate or incomplete information. The online tool also asks victims to assess how vulnerable they perceive themselves to be. This can lead to inconsistent results, which then need to be reassessed.

Reporting cyber-dependent crime to police forces

6.18. Despite the existence of Action Fraud, many people still report cyber-dependent crime to police forces. When this happens, the police will decide whether to deal with the call themselves and treat it as a call for service, or to advise the caller to contact Action Fraud.

Call for service

6.19. In general terms, a call for service is a report that requires a response from the police. In the case of fraud and cyber-dependent crime, the Home Office Counting Rules define the circumstances that should be treated as a call for service. These are:

- "offenders are arrested by police; or
- there is a call for service to the police and the offender is committing or has recently committed at the time of the call for service; or
- there is a local suspect."

6.20. In cases where victims don't want to, or can't, report to Action Fraud, officers and staff can make the report on their behalf.

6.21. During the inspection, we reviewed 182 calls made to police forces to report cyber-dependent crime. Nearly a third of them were not calls for service that needed police attendance. However, in most of these cases callers weren't advised to contact Action Fraud. Instead, officers visited the victim and began enquiries.

6.22. As we have highlighted earlier (see paragraph 5.36), when forces record and attend reports of cyber-dependent crime that don't qualify as a call for service, this leads to duplicated effort, and the assessment, review and allocation process managed by the National Fraud Intelligence Bureau is undermined.

Advice to victims

6.23. It is important that victims have realistic expectations of the service that Action Fraud and police forces can provide. To enable this they must be given information that is clear, concise and accurate.

6.24. We found that, generally, victims who reported directly to Action Fraud were given appropriate advice to protect them from further crime.

6.25. In most cases, this consisted of basic advice such as changing passwords, or useful websites and victim support groups.

6.26. The University of Portsmouth victim survey showed that most victims were satisfied with their interaction with the call handler. In most cases victims felt more aware and better equipped to protect themselves following the advice given.

6.27. Our examination of 50 calls received by Action Fraud showed that a good level of advice was given in 37 of those cases. In 49 cases, appropriate advice was given about securing and preserving evidence for any future investigation.

6.28. By contrast, victims reporting to the police appeared to receive less in the way of advice. Out of the 182 calls to forces examined as part of the inspection, advice was given on only a third of occasions.

6.29. In a small number of cases, we didn't think the advice given by call takers was relevant to the reported crime.

6.30. When victims called the police, they were only given accurate advice as to what to expect from Action Fraud on a very small number of occasions. We highlighted this point in our report *Fraud: Time to Choose*.

Fraud report 2019 – recommendation 16

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should provide guidance to Action Fraud and chief constables. This is to ensure that, promptly on reporting a fraud, victims are provided with explanations of:

- the role of Action Fraud;
- the process by which their fraud report will be considered for assessment or referral to the police (or other law enforcement agency) by the National Fraud Intelligence Bureau;
- how to obtain an update on the progress of their case;
- how, following referral from the National Fraud Intelligence Bureau, the decision on whether and how to investigate rests with the police (or other law enforcement agency); and
- the options open to victims of fraud to seek civil redress as an alternative (in cases where criminal investigations are not carried out or do not lead to convictions).

How well are vulnerable victims identified?

6.31. In general, vulnerability was effectively identified at first point of contact, both by Action Fraud and local forces, and support was given accordingly by forces and partners.

6.32. The National Fraud Intelligence Bureau also carries out a secondary assessment of vulnerability, referring cases to forces more urgently if necessary. This is supported by a daily management meeting where issues of vulnerability are overseen by senior managers.

6.33. The weekly victim list supplied by the bureau was helpful to most forces in identifying new opportunities to support vulnerable people. It is generally the

first indication the force will have of a victim residing in their area and enables it to interact quickly with victims where necessary.

6.34. When they receive the weekly list, we found most forces conducted their own vulnerability assessment, using their own staff or the voluntary sector to provide support.

6.35. Vulnerability assessments (using the THRIVE model) were, however, focused on the individual or business reporting the crime, and not the technology that was targeted. Cyber-dependent crime targets weak technology or poor user practice rather than particular types of victim. While the identification of victim vulnerability was found to be of a good standard, we didn't find any examples of routine assessment of the technology used.

6.36. We found that businesses were rarely identified as being vulnerable, even though the effect on a business is often similar to that on an individual. However, most forces had staff who were able to give appropriate advice and support to businesses who were victims of cyber-dependent attacks.

6.37. We didn't find any evidence of forces evaluating the effectiveness of identifying vulnerability in cyber-dependent cases.

How well are vulnerable victims supported?

6.38. Once a victim has been identified as vulnerable, most forces will provide them with additional support. This usually means giving advice on how they can further protect themselves or referring them to a victim support agency.

6.39. Sometimes victims are directed to national agency websites to obtain more advice or are referred to safeguarding teams. The approach to additional support doesn't seem to be structured, but rather based on the professional judgment of the staff dealing with the victim. This was generally appropriate.

6.40. Several forces use cyber volunteers and special constables (see paragraph 3.68) who have experience of cyber crime issues to give additional support to victims. Other forces use police community support officers (PCSOs). They can all make a valuable contribution to victim care.

Economic Victim Care Units

6.41. The national Economic Crime Victim Care Unit (part of City of London Police) has a remit to "support vulnerable people who have fallen victim to fraud and cyber crime, with the aim being to make them feel safer and reduce the possibility of them becoming a repeat victim".

6.42. The unit operates on behalf of a small number of forces. It assesses the needs of the victims of cyber-dependent crime and gives them basic prevention advice. Those needing additional support are referred for additional bespoke support or a personal visit.

6.43. At the time of our inspection the unit was operating with a backlog. This meant that some victims of cyber-dependent crime were contacted up to six months after initially reporting their crime. This could diminish the benefit of any additional support.

6.44. We are concerned that the National Fraud Intelligence Bureau's weekly list and the performance indicator requiring victim contact means the role of victim care units in cyber-dependent crime may be duplicated by forces.

Area for improvement 4

The National Police Chiefs' Council Coordinator for Economic Crime should review the role of the National Economic Crime Victim Care Units in providing advice and support to victims of cyber-dependent crime.

Satisfaction of victims

6.45. The victim survey explored the perceptions of victims who had reported to Action Fraud and subsequently had contact with other services, such as the police.

6.46. The survey found that there were moderate levels of satisfaction with the reporting process and the advice, support and information received from Action Fraud and the police. Around two-thirds of respondents said that they were fairly or very satisfied with the process.

7. Learning: How effectively does each law enforcement agency develop and disseminate relevant learning and guidance?

7.1. We explored the learning and guidance given to all staff, including those in both specialist and non-specialist roles. In doing so, we sought to establish whether staff at national, regional and local levels have the skills they need to identify and investigate cyber-dependent crime effectively.

7.2. A national training plan has been established that includes recommended training providers. However, there is wide variation in how much this is followed by forces. There is little evidence that forces are carrying out any analysis of what training their staff need. And for some roles the training provided is insufficient.

7.3. The level of training or resources provided to enable non-investigative staff to recognise cyber-dependent crime is inconsistent across forces.

Training

7.4. The National Crime Agency, through the National Cyber Crime Unit, has developed nationally agreed training pathways.[27] These are for staff involved in cyber crime investigation, prevent and protect activities, intelligence gathering, and a range of other cyber specialisms. The pathways lead from basic training through to (for highly skilled staff members) acting as a mentor and coach for others.

7.5. Regional cyber-dependent crime units also have a training pathway that specifies recommended training courses for their staff.

7.6. To support the national and regional pathways, a national training needs analysis has been undertaken and training providers have been identified and commissioned.

7.7. Despite this, there are inconsistencies in both who provides training and whether the training pathway is followed at all. We found that several forces had stepped outside the pathway or identified their own provider. Unsurprisingly, budget was once again cited as the deciding factor.

7.8. We highlighted earlier the Knowledge Hub, the online facility available to law enforcement agencies and partners (see paragraph 2.46).

[27] A training pathway is the route taken by an individual through a range of learning activities, which allows them to build knowledge progressively.

What learning is provided to people responsible for investigating cyber-dependent crime?

7.9. We found that training and learning in the investigation of cyber-dependent crime was generally well supported, structured and co-ordinated within national agencies. This was less evident in regional units, and even less so in local units.

7.10. The training at regional and local level was inconsistent, with considerable variance between both regional organised crime units and forces. Unsurprisingly, we found that the training was influenced by budget and, as such, relied on support at senior levels to make funding available. We found little evidence that any structured analysis of training needs had been undertaken locally or regionally.

7.11. Instead we found examples of forces and regions identifying their own training providers outside the recognised training pathway. For example, one regional unit sent staff to the US for training. We were told that this was the most cost-effective method of obtaining the training needed for the role in question.

7.12. At the other end of the scale, we found that some units used on-the-job training. Staff learnt from colleagues while carrying out investigations rather than receiving formal training.

7.13. The level of available training for some roles is inadequate. For example, we found that little training was available for analysts, adding to the problem of lack of analytical support for investigators.

7.14. As we have identified (see paragraph 3.50), the level of demand across all 43 forces varies. This means that after they have been trained some staff may not use their skills for some time and will lose their expertise.

7.15. We also found little evidence of continuous professional development being available for most staff. Where we did, it wasn't structured but was largely driven by staff.

7.16. This has been recognised by strategic leaders, who have established standard training based on the 4Ps (see paragraph 2.4). This includes a foundation course for all staff. However, these courses were implemented after the conclusion of our inspection and did not form part of it.

7.17. This training of investigators and other cyber-dependent crime specialists is expensive. And, as we set out earlier (see paragraph 3.61), the high turnover of staff adds to that expense. As the funding streams from the Police Transformation Fund and the National Cyber Security Programme come to their respective conclusions, pressure on the training budgets of individual forces will increase.

7.18. This is likely to lead to even more units moving away from the training pathways. This, in turn, will lead to an increasingly fragmented approach to cyber-dependent crime.

7.19. In our view, this adds support to the argument for the creation of a national cyber-dependent crime network. This would lead to a more effective and efficient approach to the training and deployment of specialist staff.

What learning is provided to help staff recognise cyber-dependent crime?

7.20. Considerable elements of the investigation of cyber-dependent crime are, rightly, considered by law enforcement agencies to be specialist skills. However, the increasing prevalence of this type of crime means that the ability to recognise it, initiate investigations, and give sound advice to victims shouldn't just be the responsibility of a small set of investigators.

7.21. We found considerable variation in the level and standard of training and guidance given to staff in roles that involve the identification of cyber-dependent crime – for example, call handlers.

7.22. The training was more structured at the national level – call handlers from Action Fraud attend a two-week training course and are then assessed over the following months. A pass rate of 85 percent is applied to their assessment process.

7.23. We recognise that the role of call handler in local forces is much more generalist in nature. Cyber-dependent crime represents only a very small proportion of the calls that these staff deal with daily.

7.24. Having said that, we found that call handlers from local forces received comparatively little in the way of specific cyber-dependent training. Most received only the general call handler training, which may include a small amount about this type of crime. It was a similar picture for most non-specialist police officers and staff – many receive, at best, only basic information.

7.25. More positively, we found some forces had developed web-based information with guidance and advice for officers and staff. We also found that aide memoires and templates were often used by call handlers in both Action Fraud and local forces. This helped in achieving a minimum standard and consistency in the service being given to callers.

Definitions and interpretations

In this report, the following words, phrases and expressions in the left-hand column have the meanings assigned to them in the right-hand column. Sometimes, the definition will be followed by a fuller explanation of the matter in question, with references to sources and other material that may be of assistance to the reader.

Action Fraud	the UK's national fraud and cyber crime reporting centre, providing a central point of contact for information about fraud and cyber crime
Chief Constables' Council	senior operational decision-making body for the National Police Chiefs' Council; brings together chief constables of police forces in the UK
cyber-dependent crime	offences that can only be committed using information communications technology, where the devices are both the tool for committing the crime and the target of the crime
cyber-enabled crime	existing crimes that have been transformed in scale or form using the internet
denial of service (DDOS)	a malicious attempt to overwhelm an online service and render it unusable
hacking	gaining unauthorised access to data in a system or computer
Home Office Counting Rules (HOCR)	provide a national standard for the recording and counting of 'notifiable' offences recorded by police forces in England and Wales (known as 'recorded crime'); rules in accordance with which crime data – required to be submitted to the Home Secretary under section 44 of the Police Act 1996 – must be collected; set down how the police service in England and Wales must record crime, how crimes must be classified according to crime type and categories, whether and when to record crime, how many crimes to record in respect of a single incident and the regime for the reclassification of crimes as no-crimes; specify all crime categories for each crime type including the main ones of homicide, violence, sexual offences, robbery, burglary, vehicle offences, theft, arson and criminal damage, drug offences, possession of weapons, public order offences, miscellaneous crimes against society and fraud

integrated offender management (IOM)	management of the most persistent and problematic offenders by police and partner agencies working together
IP address	internet protocol address – a unique string of numbers separated by full stops that identifies each computer using the internet protocol to communicate over a network
malware	software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system
management of risk in law enforcement (MoRiLE)	process designed to assist law enforcement agencies to use a standardised assessment to assist decision makers in identifying and prioritising threat, risk and harm; its use complements the National Intelligence Model (NIM) and National Decision Model (NDM) and links threat, risk and harm assessments to organisational capacity and capability
National Crime Agency	non-ministerial government department established under the Crime and Courts Act 2013 as an operational crime-fighting agency with responsibility for leading national efforts to tackle serious and organised crime; its remit includes strengthening national borders, fighting fraud and cyber crime and protecting children and young people from sexual abuse and exploitation; replaced the Serious Organised Crime Agency
National Fraud Intelligence Bureau	part of City of London Police, the National Fraud Intelligence Bureau processes the information received by Action Fraud along with information supplied by other agencies, such as the Credit Industry Fraud Avoidance Service (Cifas) and UK Finance, which is stored centrally on one system known as Know Fraud
National Police Chiefs' Council	organisation that brings together 43 operationally independent and locally accountable chief constables and their chief officer teams to co-ordinate national operational policing; works closely with the College of Policing, which is responsible for developing professional standards, to develop national approaches on issues such as finance, technology and human resources; replaced the Association of Chief Police Officers on 1 April 2015
organised crime group	criminals working together and involved in planning, co-ordinating and committing serious crime on a continuing basis

organised crime group mapping	standardised method of assessing the risks that OCGs present to communities and prioritising activity against them
regional organised crime unit	operational police unit endowed with regional jurisdiction and specialist capabilities to disrupt and dismantle organised crime units; officers and police staff are normally seconded to regional units from forces within the region
serious crime prevention order	court order issued in accordance with the Serious Crime Act 2007 to protect the public by preventing, restricting or disrupting a person's involvement in serious crime
serious and organised crime	serious offences (defined by the Serious and Organised Crime Act 2015) that are planned, co-ordinated and conducted by people working together on a continuing basis and whose motivation is often, but not always, financial gain
spyware	software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive
THRIVE	threat, harm, risk, investigation, vulnerability and engagement assessment used by call handlers to help assess the appropriate initial police response to a call for service

Annex A – Terms of reference

Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services will inspect the police and National Crime Agency response to the threat presented by cyber-dependent crimes.[28]

The inspection will examine:

- whether the police and National Crime Agency have a well co-ordinated and adequately resourced structure to deal with the threat presented by cyber-dependent crime, with sufficient capability and capacity to tackle those crimes, and those that commit them, efficiently and effectively;
- whether the police and National Crime Agency remit, roles and responsibilities are appropriate, understood and discharged effectively, including responsibilities to gather, develop and disseminate intelligence and to investigate and disrupt cyber-dependent crimes, at the local, regional, national and international levels;
- how effectively the police and National Crime Agency engage with the public and businesses to reduce vulnerability to cyber-dependent crimes;
- how effectively the police and National Crime Agency respond to incidents, including an examination of how well they work with other bodies to reduce the adverse effect of cyber-dependent crimes;
- the manner in which learning, development and training material is disseminated to enable effective first response and specialist capabilities, including the quality of the material and its impact on the threat; and
- their level of engagement with other bodies – from government, academia and the private sector – to inform the response to cyber-dependent crime in accordance with current government strategy.

The inspection will be conducted in accordance with Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services powers under the Police Act 1996 to inspect police forces in England and Wales (including force collaborations such as the regional organised crime units), and under the Crime and Courts Act 2013 to inspect the National Crime Agency.

[28] Cyber-dependent crimes can only be committed using information communications technology, where the devices are both the tool for committing the crime and the target of the crime. *National Cyber Security Strategy 2016–2021*, Cabinet Office, 2016, page 74.

Annex B – Methodology

Our inspection took place between April and June 2019. We inspected ten police forces in England and Wales, all nine regional organised crime units, the National Crime Agency, Action Fraud, and the National Fraud Intelligence Bureau. We invited the local policing body for each of the ten police forces to give us their views. A full list of those inspected is in Annex D – Forces and regional organised crime units inspected.

In each organisation, we interviewed the people responsible for the strategic and tactical response to cyber-dependent crime, and we held focus groups with relevant operational staff.

We also spoke to people from other relevant organisations, including the National Cyber Security Centre. We canvassed other police forces (that were not inspected) for opinions and examples of best practice. Finally, we spoke with other non-government organisations that provide advice and support to victims of cyber-dependent crime.

In total, we spoke with around 600 people to whom we are grateful for their contribution.

We reviewed documents such as control strategies, action plans, policies and procedures, some of which were specific to each organisation.

We listened to and reviewed telephone calls from members of the public to each of the forces we inspected and to Action Fraud. We reviewed investigations in each force, regional organised crime units and the National Crime Agency. In total, we reviewed 232 calls and 129 investigations. More information about how we did this can be found in Annex E – About the data.

At our request, police forces, regional organised crime units and the National Crime Agency provided us with examples of cases that they felt demonstrated their approach to investigations and other activity in the fight against cyber-dependent crime.

We asked police forces, Action Fraud and the National Fraud Intelligence Bureau to provide us with a selection of data relating to cyber-dependent crime. We have used this to understand the demand from cyber-dependent crime and how this is recorded and managed.

We also asked forces to tell us how easy or difficult it was to supply the data we requested using the following definitions:

- **Easy**: The exact data requested can be extracted from force systems with minimal effort by the force.
- **Moderate**: The data can be extracted but it requires additional resource or analysis to meet the exact requirements requested.
- **Difficult**: The data cannot easily be extracted and would require significant effort to meet the exact requirements requested.
- **Impossible**: The data is not recorded/held by the force.

We also asked them to give us their views on the quality of the data using these definitions:

- **Low**: There are flaws in the data that the force is aware of – there is no assurance applied to this data.
- **Medium**: Use can be made of the data, but there are some caveats.
- **High**: The data is fully assured and the force is confident in its use.

When forces identified data as “difficult” or “impossible” to identify or deemed it “low” quality, they were not asked to provide that data.

Some forces provided joint submissions to reflect their collaborative approach to cyber-dependent crime. These submissions were counted as a single submission. As a result, the total number of forces is shown as 40.

To support our inspection, a survey of victims of computer misuse was carried out by the University of Portsmouth using the online survey provider Qualtrics. A total of 252 victims who had suffered at least one offence of computer misuse in the previous two years took part in this survey.

The survey greatly assisted our understanding of victims’ experiences with cyber-dependent crime and interaction with law enforcement agencies.

We formed a cyber-dependent crime external reference group, which was invaluable to us in challenging and shaping our terms of reference and methodology.

Annex C – Legislation and types of cyber-dependent crime

Cyber crime generally takes two forms, cyber-enabled crime and cyber-dependent crime.[29]

Cyber-enabled crimes are defined as "existing crimes that have been transformed in scale or form by the use of the Internet". The obvious example is fraud, but it can include the purchasing of illegal drugs or firearms and child sexual exploitation. All of these can be conducted on or offline, but online can take place at unprecedented scale and speed.

Cyber-dependent crimes are "offences that can only be committed using information communications technology, where the devices are both the tool for committing the crime and the target of the crime".

Cyber-dependent crime has been the sole focus of this inspection. Cyber-dependent offences can result in the theft of personal data, money, intellectual property or other sensitive information. It can also be committed to alter, prevent access to, or otherwise disrupt a system, service or data.

Methods of committing these offences include the use of ransomware, where malicious software blocks a user's files, computer or device until a ransom is paid, and distributed denial of service attacks, which flood a system with more requests than it can handle, stopping users from accessing it.

Legislation

The primary legislation relevant to cyber-dependent crime is the Computer Misuse Act 1990.

Introduction of the Act introduced new offences of:

- unauthorised access to computer material;
- unauthorised access with intent to commit or facilitate a crime;
- unauthorised acts with intent to impair the operation of a computer; and
- making, supplying or obtaining articles which can be used in computer misuse offences.

[29] *National Cyber Security Strategy 2016–2021*, Cabinet Office, 2016, page 74

Annex D – Forces and regional organised crime units inspected

National agencies

Action Fraud (City of London Police)

National Crime Agency

National Fraud Intelligence Bureau (City of London Police)

Forces

Greater Manchester Police

Hampshire Constabulary

Hertfordshire Constabulary

Humberside Police

Lincolnshire Police

The Metropolitan Police Service

Northumbria Police

South Wales Police

Warwickshire Police

Wiltshire Police

Regional organised crime units

Eastern Region Special Operations Unit

East Midlands Special Operations Unit

North East Region Special Operations Unit

North West Regional Organised Crime Unit

South East Regional Organised Crime Unit

South Wales Regional Organised Crime Unit

South West Regional Organised Crime Unit

West Midlands Regional Organised Crime Unit

Yorkshire and Humber Regional Organised Crime Unit

Annex E – About the data

The information presented in this report comes from a range of sources. It includes data published by the Home Office and the Office for National Statistics; inspection fieldwork; and data we collected directly from Action Fraud, the National Fraud Intelligence Bureau, National Crime Agency, regional organised crime units and the 43 police forces in England and Wales.

When we collected data directly from police forces, we took reasonable steps to agree the design of the data collection with forces. We gave them the opportunity to check and validate the data they gave us to confirm the accuracy of our evidence. For example, we checked the data that forces submitted and raised queries when the information was inconsistent or notably different from that of other forces.

Review of calls to Action Fraud

We reviewed 50 calls to Action Fraud from victims reporting cyber-dependent crime between October and December 2018.

Review of telephone calls to police forces

We randomly selected and reviewed recordings of 20 telephone calls made between July and December 2018 by victims reporting cyber-dependent crime to each of the police forces we inspected.

Review of cyber-dependent investigation files

We randomly selected and reviewed ten police crime investigation files recorded between January and December 2018 by each force we inspected.

We also received briefings on up to four complex cyber-dependent crime cases that were investigated during 2017 and 2018 by the National Crime Agency, each of the forces we inspected, and the regional organised crime units.