

# Cyber Crime Strategy



## Warwickshire Police and West Mercia Police 2016 Cyber Crime Strategy



Warwickshire  
**POLICE**



West Mercia  
**POLICE**

# Contents

Foreword.....	3
PCC commissioning approaches.....	4
Executive Summary .....	5
Cyber Strategy: Strategic Overview .....	8
Strategic Governance & Insight .....	9
Develop and Execute the Strategy .....	9
Vision, Principles, Objectives and Priorities of the Strategy .....	9
Common Objectives.....	11
Common Objective 1 .....	12
Common Objective 2 .....	12
Common Objective 3 .....	13
Common Objective 4 .....	13
Common Objective 5 .....	14
Common Objective 6 .....	14
Appendix 1: Assistive Legislation .....	17
Appendix 2: Partners for Building Block 3: Local Problem Solving & Partners .....	22
Appendix 3: Structure & Current Terms of Reference .....	24
Appendix 4: Glossary .....	26

# Foreword

It is a pleasure to introduce the very first Cyber Crime Strategy for Warwickshire Police and West Mercia Police. The internet represents a huge social and technological change in our lifetime. It is a wonderful resource and key enabler to communities to enjoy and achieve things. However, our increasing reliance on cyberspace has brought new risks, with organised criminals using the internet to exploit victims and steal large amounts of money, often through the theft of our personal information.

Law enforcement recognises the challenges and the requirement to work in partnerships to protect our communities from such harm. Warwickshire Police and West Mercia Police take these risks seriously. We are determined to tackle the threats, but in a way which balances security with respect for privacy and fundamental rights.

I believe that the publication of this strategy is an important step in building upon the excellent partnerships we have in place. This strategy will support businesses by setting out how we will support you, and will foster opportunities for business to be involved in schemes such as Cyber Essentials and the Cyber Information Sharing Partnership.

This strategy outlines how individuals concerned about their security, be it from fraud or identity theft can identify how to help themselves. By 2018, it is the aspiration of Warwickshire Police and West Mercia Police that the strategy will have enabled communities and individuals to protect themselves, businesses will have the right information to help themselves, and police will be effectively dealing with those criminals causing most harm.



**Stephen Cullen**

Temporary Assistant Chief Constable Protective Services

# PCC commissioning approaches

The Police and Crime Commissioners' commissioning approaches to cyber crime will encompass the whole pathway from prevention, early intervention, providing support to victims and then working with the police to understand the cause of crime and how best to tackle offenders.

It is vital that we empower our communities to be safe and secure in a digital age and partnership working is key to this. Our commissioning intentions include raising awareness amongst young and old people and businesses, those particularly vulnerable to cyber crime, on how they can protect themselves from falling victim of cyber crime and ensuring the vulnerable in society have access to tailored advice on how to stay safe online. For those who have fallen victim to cyber crime it is imperative that they know how to report the crime and are offered support to cope and recover.

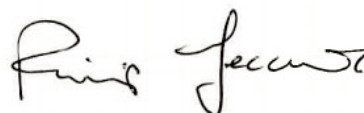
"I pledged to create a West Mercia that puts victims and survivors first, is reassured, reformed and is more secure. Having an effective strategy for tackling cyber crime is clearly an important aspect of delivering those promises. We must have an agile approach to cyber crime to ensure policing and law enforcement keeps pace with emerging threats. By giving officers the resources to be dynamic and innovative, empowering communities to play a more active role in preventing cyber crime and helping victims cope and recover we will help create a safer West Mercia."



**John Campion**

West Mercia PCC

"Cyber crime is identified as a Tier 1 national threat while the latest Crime Survey for England and Wales only serves to emphasise how the nature of crime is changing. The most common type of crime people suffer is now fraud and other internet-related offences, as criminals have increasingly shifted their focus to an online digital world. Our response needs to change accordingly – both in terms of law enforcement and as users of digital services. This is a problem which cannot be solved solely by enforcement action by the police, either locally or nationally. The best defence is for people and businesses to be aware of the simple steps they can take which can prevent the majority of offences taking place and increasing awareness of these will remain a high priority during my term of office."



**Philip Seccombe**

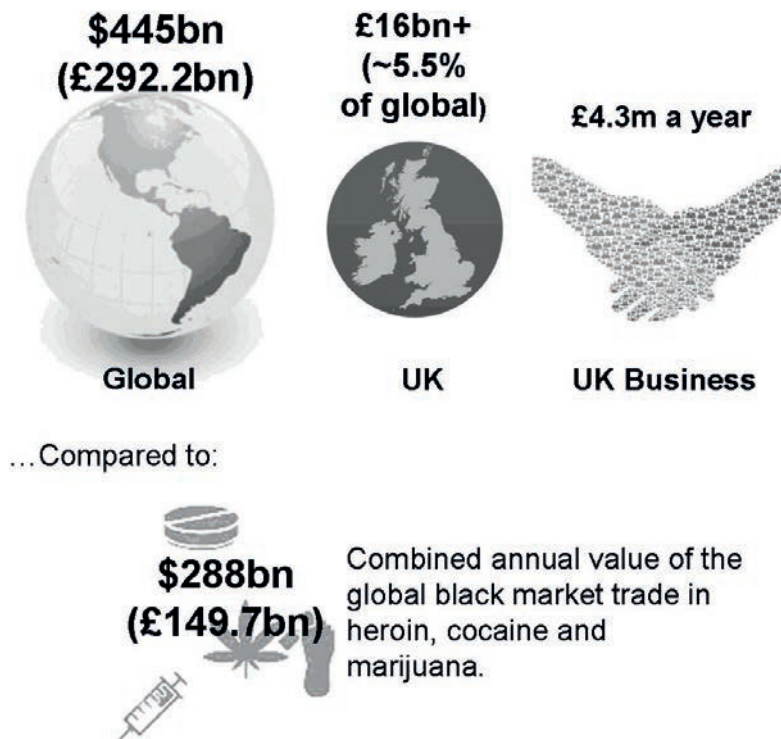
Warwickshire PCC

# Executive Summary

“Cyber crime” or “online and digital crime” is a very real, and very common occurrence in our every day world, and affects every part of our local and global economy, as well as every part of our personal life. Modern devices such as smart phones and tablets have brought the internet not only to our fingertips but to our bedsides, our pockets and to our children. And yet there is strong evidence that access to such technology, with all its opportunities and benefits, can put our businesses and our families at increasing risk of exploitation.


The digital environment, including the Internet and the DarkWeb, has been used to great effect by criminals to trade legitimate and illicit products and services. Sophisticated operators have traded cloned credit card data and bank account details, hire of botnets (infected networks of computers) and the (legal) delivery of hacking tutorials. Online grooming for a variety of purposes has also been demonstrated in a variety of publicly available social media and interactive spaces.

The cost of cyber crime currently is estimated as follows:



The threat is expected to increase. Research indicates that by 2019 the global losses to cyber crime will exceed \$2trillion ([Juniper, 2015](#)). Assuming the above figures stayed in line, the UK alone could expect a loss in excess of £64bn – roughly equivalent to the benefit from the current round of Devolution Deals to the UK Economy ([DCLG, September 2015](#)).





The UK is identified by the G20 as the most cyber-dependent economy of its member nations with 74 percent of the adult population buying goods and services online.

UK total online spending in 2014 was £175bn – 31% of the UK's total spend in that year by debit and credit card (£567bn) ([UK Cards Association, 2014](#))

“Despite long term falls in traditional crime types, there is growing evidence that crime has moved online. Digital and cybercrime is no longer a curiosity or new specialism in policing: it's what we deal with on a daily basis.

“The priorities for law enforcement are to make the UK a hostile place for cyber-criminals to target or operate, improve the response to victims and develop capabilities in local forces.


The NPCC is working closely with the National Crime Agency and College of Policing to develop effective systems and train staff to tackle fraud, cyber and digital crime.

Transforming our response to these crimes is a challenge but it is a priority for investment in policing. Additional funding through the National Cyber Security Programme has supplied specialist investigators and protect officers at regional level and there's increasing evidence of forces supporting this with local cyber-capabilities.”

National Police Chiefs' Council Lead for Cybercrime, Deputy Chief Constable Peter Goodman (2016)

Concerted and coordinated Partnership working, with existing and new partners from the local to the national, will be essential to protect people from the greatest harms. The public and the online and digital industry will also have to play their part to ensure that their experiences and services remain positive, fulfilling and secure.

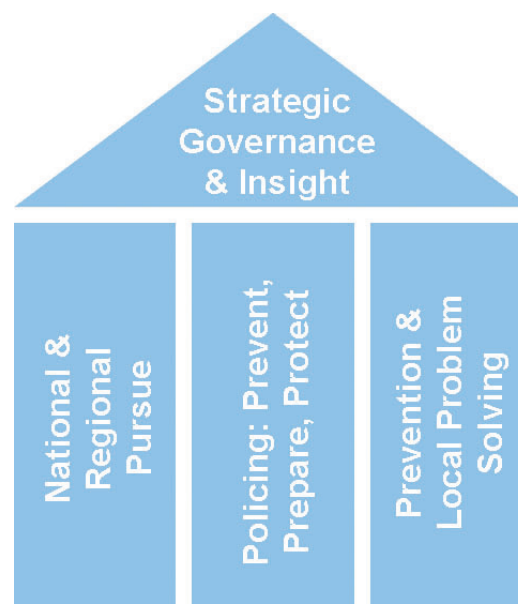
This strategy document sets out the overview for how Warwickshire Police and West Mercia Police and partners will operate its Cyber Strategy. It will set out the three building blocks of the strategy landscape of national to local partnership. The remainder of the document will then specifically focus on the most public facing of the building blocks: Prevention and Local Problem Solving.



This strategy will at all times remain consistent with obligations under the Strategic Policing Requirement and the NCA National Cyber Strategic Assessment.

# Cyber Strategy : Strategic Overview

The structure of the Cyber Strategy will look like this:



Each part of the above strategic approach will have 2 common phases to govern its progress:

1. Developing and executing implementable, valid workstreams.
2. Evaluating outcomes and adjusting working methodologies based on evidence based findings.

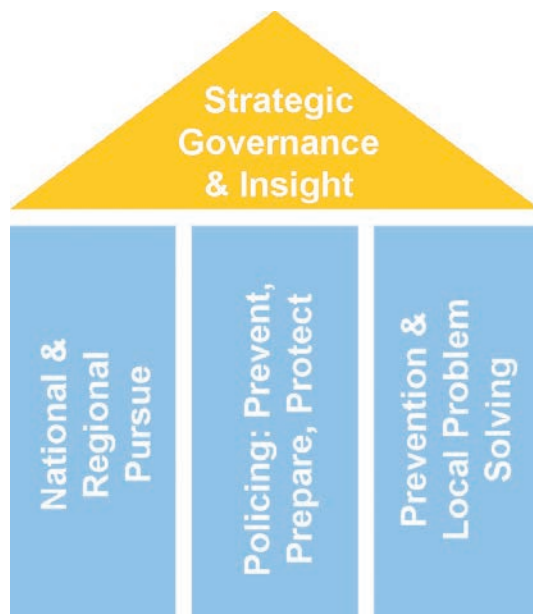
Following the Deming cycle - Plan, Do, Check, Act - three main approaches will be used to assist evaluation and adjustment:

1. Linear approach: the strategy will be developed, implemented, evaluated and eventually terminated (or replaced).
2. A lifecycle approach: the output of the evaluation phase will be used to maintain and adjust the strategy itself.
3. A hybrid approach: several continuous improvement cycles on different levels may exist.



# Strategic Governance & Insight

## Develop and Execute the Strategy



This section will provide guidance to the Strategic Governance Group (SGG) and Partnerships to the strategy on the main components and actions that should be considered during the development and execution phases. Each of the remaining 3 building blocks will focus on core objectives that require attention, and the programme of work required to meet these objectives. These objectives will support the Vision and Principles of the overall strategy in a “local philosophy”, and provide the content to drive delivery against each of the action plans.

## Vision, Principles, Objectives and Priorities of the Strategy

### The Vision

- To promote in partnership a social and economic online environment where individuals and communities understand the risks and are better protected from harm

### Scope of the online and digital environment in the Vision, for Cyber Crime purposes

Warwickshire Police and West Mercia Police definition of a cybercrime that “An offence should be flagged as cyber-enabled where the reporting officer believes that on the balance of probability, the offence was committed, in full or in part, through a computer, computer network or other computer enabled device.”

The National adopted definition of cybercrime as of 7th October 2014 is:

1. Cyber Dependent crimes, where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to commit further crime).
2. Cyber Enabled Crimes. ‘Existing’ crimes that have been transformed in scale or form by their use of the Internet. The growth of the Internet has allowed these crimes to be carried out on an industrial scale.

3. The use of the Internet to facilitate drug dealing, people smuggling and many other 'traditional' crime types.

### **The Principles for Strategic Governance & Insight**

1. A Risk based, Evidence-Based approach
2. Working in partnerships

### **A Risk based, Evidence-Based approach**

The purpose of adopting this approach is to enable the SGG to set priorities for the year ahead in order to meet the Vision, and relevant Objectives for each building block. Deployment of resources will be determined based on where the threat from cyber crime is the most greatest and where we can demonstrate our interventions and obtain greatest impact for the investment.

The key threats in the National Cyber Strategic Assessment 2015 are:

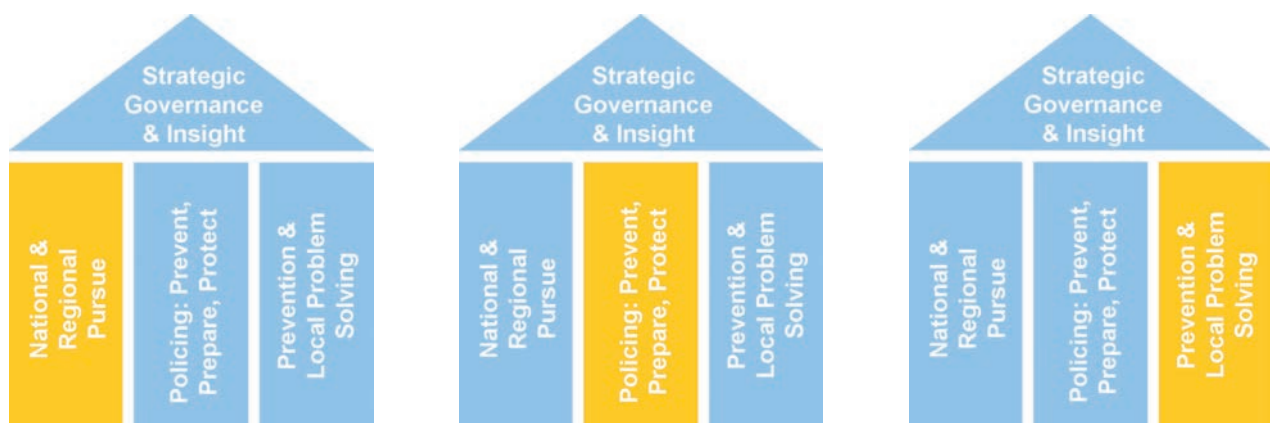
- Child Sexual Exploitation / Abuse.
- The proliferation of indecent images of children (IIOC) and online child sexual exploitation (OCSE) continue to subject children to risk.
- The large-scale harvesting of personal and business data to commit fraud offences against individuals and organisations.
- According to phishing statistics, Social Networking sites are the third target of phishing behind payment and financial systems.
- Victims are continuing to lose large sums of money from investment fraud (e.g. boiler room fraud or ponzi schemes). The call centres from which these frauds are perpetrated are often based in locations in the EU and South Asia. These frauds can have a significant financial, social and emotional effect on victims.
- Insider fraud is increasingly seen as a high risk area for the private sector domestically and globally. The targeting by OCGs of an organisation's staff members to coerce them into providing sensitive information and/or to facilitate criminal activity is of concern.
- With the introduction of major government online payment systems there is likely to be substantial interest from criminals with a shift toward more cyber-enabled fraud and more criminal use of identity.
- Bespoke mobile malware already exists and is well-established outside the UK. International groups already deploying mobile malware elsewhere may start to target the UK, and groups currently targeting western markets by other means may adopt mobile malware deployment. The increasing use of apps designed for legitimate financial transactions will, over the next 12 - 18 months, provide new opportunities for criminals.

- Abuse of identity documents continues to be a key enabler used by criminals. Identity theft occurs when criminals access enough personal information about an individual to commit fraud. They use various techniques to steal these details, from outright theft and social engineering to harvesting data through cybercrime. With this information, criminals can impersonate the victim in order to access bank accounts, fraudulently claim benefits or obtain genuine documents in the victim's name.
- Increasing use of the hidden internet, accessed through anonymising programs, is expected, allowing criminals to hide their real identity online and in the real world. This will give criminals increased confidence in their criminal activities online as it is much harder for law enforcement to establish their identities.

## Common Objectives

**These objectives are common to all 3 operational and partnership building blocks:**

1. Effectively lead and govern the development, execution, evaluation and adjustment of protect activity across all levels to manage the threat that online and digital crime poses, engaging with all those inside the police service, public and private sector who are able to provide expertise.
2. Identify those most vulnerable to cyber harm in order to coordinate operational response.
3. Identify, test and deliver interventions that reduce cyber crime which make the online and digital environment more secure, in order to promote safer social and economic activity.
4. Lead and support media awareness campaigns to promote understanding of the risks and what can be done to effectively protect individuals and communities.
5. Reduce the harm caused by Fraud.
6. Pursue and Prepare - mainstreamed digital capability that delivers an effective and efficient operational response.



## Additional Objectives

By agreement with the SGG, each building block may adopt specific additional objectives that assist the common phases set out in the strategic approach. This will help to maintain consistency of governance while allowing greater flexibility to accommodate emerging needs or challenges.

### Common Objective 1

Effectively lead and govern the development, execution, evaluation and adjustment of activity all levels to manage the threat that online and digital crime poses, engaging with all those inside the police service, public and private sector who are able to provide expertise.

#### Priority Actions

1. Establish clear leadership and governance for each operational and partnership building block, with focused development and execution plans, based on evidence based practices and including evaluation.

### Common Objective 2

Identify those most vulnerable to cyber harm in order to coordinate operational response.

#### Priority Actions

1. Identify all current interventions and use the [Evidence Based Policing Matrix](#) to show what we know works, what doesn't and what is promising but needs further evaluation. Identifying the 'evidence gap' through consultation with police and specialist cyber units, businesses and individuals affected by it – With the **Better Policing Collaborative** (Police Knowledge Fund project). Working with the emerging new arrangements in forces where specialist units are being developed and/or regional cyber units to:
  - Provide support via evidence review, evaluation and technical support to shape evidence-based tactical and strategic decisions;
  - Pool information to develop towards a standardised approach based upon identified good practice within and across forces.
2. Identify, enhance and support existing online and digital crime programmes across the schools, FE and HE in Warwickshire, Worcestershire, Herefordshire, Shropshire and Telford and Wrekin, with the specific needs of each building block.
3. Work with schools to offer victim care and confidence to report; as well as educating those responsible for the impacts.
4. Work to protect the elderly from harm through the existing cyber seniors programme.

5. Gather and develop knowledge products for our staff and partners based on existing and available evidence based policing<sup>1</sup> research which we are working with the Birmingham University to update, and also obtain outcomes from the Police Knowledge Fund.
6. Identify the victim demographic and the level of social media enabled crime in a number of forces to identify best practices and lessons learned.
7. Using the victim demographic, assess the impact of similar programmes with partner groups, and prioritise based on risk threat and harm.

### Common Objective 3

Identify, test and deliver interventions that reduce cyber crime which make the online and digital environment more secure, in order to promote safer social and economic activity.

#### Priority Actions

1. Adopt Cyber Essentials, and encourage its adoption by local government, businesses and organisations.
2. Join CiSP – the Cyber security Information Sharing Partnership – part of CERT-UK. Enables members to share cyber threat vulnerability information and reduce vulnerabilities.
3. Promoting the Department for Business Innovation and Skills 10 steps to cyber security.
4. Promoting the CPNI / CESG Alpha guidance to Public and Private sector on BYOD.
5. Promoting greater awareness of fraud risks.
6. Instigating the behaviours that individuals, businesses and public services can change to enable self-protection.

### Common Objective 4

Lead and support media awareness campaigns to promote understanding of the risks and what can be done to effectively protect yourself and others from harm.

#### Priority Actions

1. Adopt the #becybersmart brand for campaigns, and promote available awareness and education opportunities internally and externally including the Home Office supported and Open University-developed Massive Open Online Course '[Introduction to Cyber Security](#)' and the GCHQ supported app to teach people about cyber security and encryption. [A link to the free app – named Cryptoy - is available here](#)

---

<sup>1</sup> e.g. [Cyber crime: A review of the evidence Research Report 75 Dr. Mike McGuire \(University of Surrey\) and Samantha Dowling \(Home Office Science\) October 2013](#) and other studies being carried out across the UK, which are available through the SSI Environmental Scanning team.

2. Select additional awareness topics.
3. Build a business case.
4. Build a communication framework to deliver the plan.
5. Implement an awareness programme, using a variety of channels.

## Common Objective 5

### Reduce the harm caused by Cyber enabled Fraud

#### Priority Actions

1. Identifying good practice and sharing it with National and Regional stakeholders to promote effective response.
2. Work with existing local fraud victims to improve the level of service that we can give.
3. Improve public and business awareness of fraud and self-protection from it.
4. Improve information and knowledge, providing a centre of expertise to raise the priority of fraud, secure and use counter fraud resource appropriately and achieve better prevention and enforcement of fraud.
5. Working with public and private organisations to identify and reduce the risk from the key fraud enablers and high threat areas.
6. Champion and coordinate the counter-fraud community, helping it become more joined up, more efficient and effective - we will do this by building relationships, sharing good practice, dealing with the gaps and overlaps and helping to streamline the counter-fraud community landscape.

## Common Objective 6

### Pursue and Prepare - mainstreamed digital capability that delivers an effective and efficient operational response

#### Goal:

Embedding a distributed DII capability within Warwickshire Police and West Mercia Police

The National DII programme identifies the five key areas for success:

1. Ways of working
2. Digital Exploitation
3. People
4. Digital Sources
5. Collaboration & Partnerships



## How will we deliver the objective?

The DII governance board should commission a more systematic review of Force level capabilities to facilitate effective prioritisation.

The DII Leads in Force should focus on developing priority capability development areas once these have been validated.

Development of a new performance framework that looks at cybercrime and operational DII capabilities rather than just numbers of officers and more traditional crime statistics.

Provision of appropriate support for cybercrime victims.

Using partnerships to enhance capability:

- Academic, Commercial, Police Staff Volunteers (PSV) / Special Constabulary (SC)

Mainstreaming cyber enabled digital awareness for all officers and frontline staff.

Digital crime prevention at a local level able to provide victims of crime with the right support:

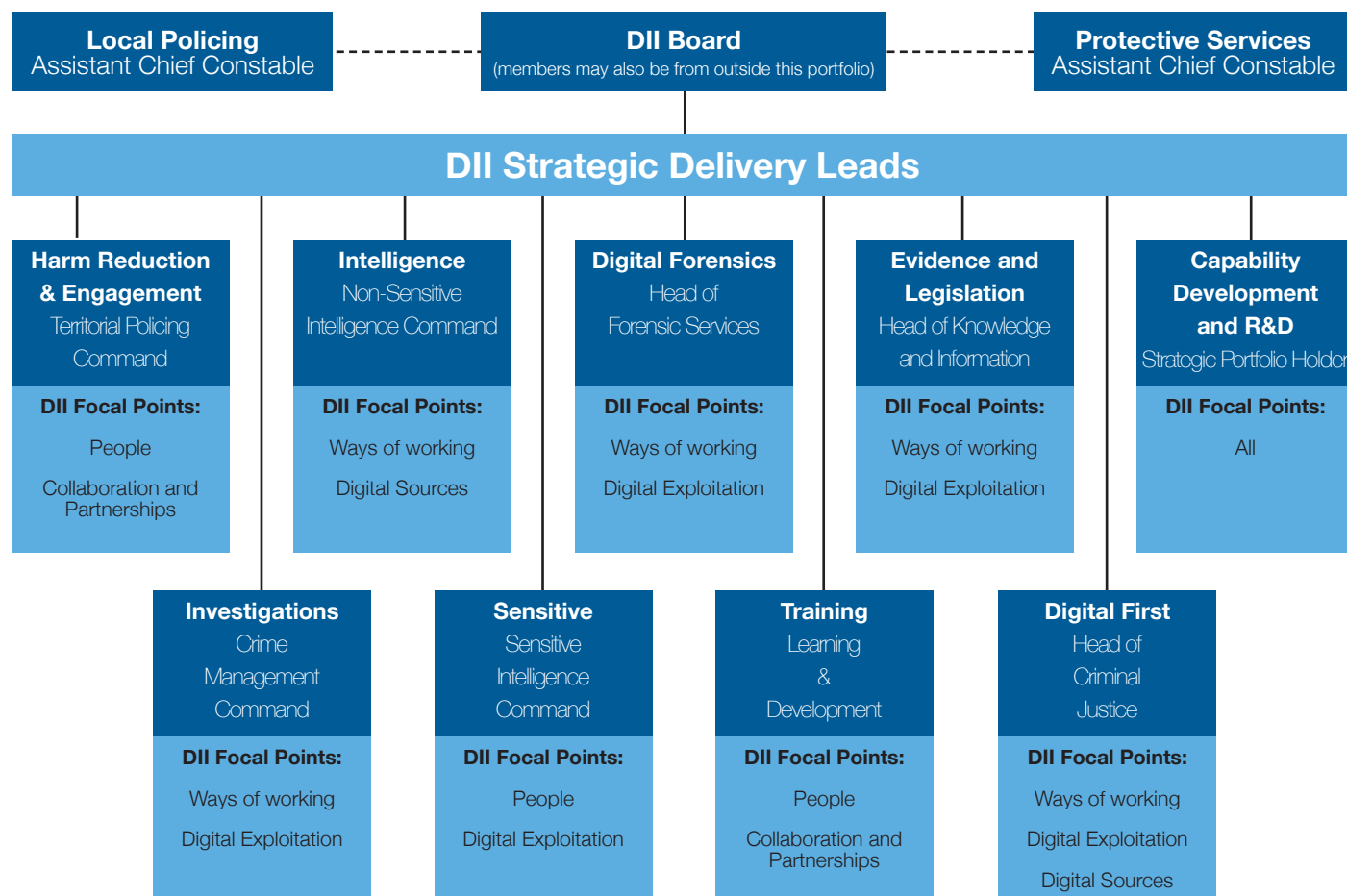
- Collaborative approach to data exploitation / big data
- Development of career paths for digital specialists
- Communicating with members of local public and raising awareness
- Provide management oversight
- Provide assurance to senior leadership
- Ensure accountability
- Establish named portfolio leads and ownership of workstreams
- Adopt the Strategy implementation framework

DII Board has 4 strategic roles:

1. Setting the strategic vision for DII
2. Establish an integrated approach to DII development
3. Maintaining oversight of DII capability delivery
4. Setting standards and monitoring operational delivery

Adopt five key areas:

- People, Ways of Working, Digital Exploitation, Digital Sources, Collaboration & Partnerships



**DII will meet quarterly, chaired by the DII lead.** It will:

- operate as the ‘engine room’ driving progress and monitoring performance;
- include new leads for each of the five capability areas, as a single accountable owner each area to ensure coherence and effective integration;
- include leads from the identified cyber / digital portfolios.

**Draft Board terms of reference.** It will:

- Identify areas of cyber related concerns that have or are likely to have an impact on the Constabulary and its ability to effectively deal with crime
- Ensure that all stakeholders are represented, ensuring visibility of both current and proposed workstreams across organisational functions
- Ensure that appropriate governance is maintained over digital activities in order to ensure that associated risks are managed effectively

# Appendix 1 : Assistive Legislation

Term	Explanation
Crime & Disorder Act 1998	Section 17 of the Crime and Disorder Act 1998 Act places a duty on the responsible Authorities, Police, Fire and Rescue, Probation, Health and Local Authority to work together to prevent crime and disorder.
<a href="#">Computer Misuse Act 1990</a>	<p>An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes’.</p> <p>Sets out three computer misuse offences:</p> <ol style="list-style-type: none"> <li>1. Unauthorised access to computer material</li> <li>2. Unauthorised access with intent to commit or facilitate commission of further offences</li> <li>3. Unauthorised modification of computer material</li> </ol>
<a href="#">Privacy and Electronic Regulations (EC Directive) 2003</a>	<p>These regulations, the UK implementation of EU directive 2002/58/EC (each member state of the EU is left to implement this directive for themselves), are enforced by the Information Commissioner’s Office, the UK’s independent authority set up to promote access to official information and to protect personal information.</p> <p>According to the regulations, companies must get an individual’s permission before sending email or SMS messages (the law applies also to telephone calls and faxes). There are significant limitations. In the first place, the regulations only apply to messages sent to individuals’ email addresses, not business addresses. The penalties are also limited, when compared to penalties for offences covered by the Computer Misuse Act. The legislation only applies to senders within the UK. Most spam originates from beyond the UK.</p>
<a href="#">Police and Justice Act 2006</a>	<p>Includes amendments to the Computer Misuse Act. The maximum prison sentence under section 1 of the original Act was increased from six months to two years. Section 3 of the Act (‘unauthorised modification of computer material’) was amended to read ‘unauthorised acts with intent to impair or with recklessness as to impairing, operation of computer, etc.’ and carries a maximum sentence of ten years.</p> <p>The Act also added another section, ‘Making, supplying or obtaining articles for use in computer misuse offences’, carrying a maximum sentence of two years.</p>

<a href="#">Serious Crime Act 2007</a>	<p>Provided the police with powers ‘to detect, disrupt and prevent serious crime’ (Home Office press release, 30 October 2009). However, some people have raised concerns about the implications for civil liberties, not least because the burden of proof required in a civil court is lower than that required in a criminal court and there is consequently more scope for potential miscarriages of justice.</p> <p>In 2009 reports in the press said that the police had the power to hack into the computers of suspects without a warrant.</p>
<p>Serious Crime Bill (currently passing through Parliament) – to become the Serious Crime Act 2015</p>	<p>To replace the Serious Crime Act 2007, the Bill will also make a number of changes to the Computer Misuse Act 1990, in particular to ensure that sentences for attacks on computer systems fully reflect the damage they cause. It will:</p> <ul style="list-style-type: none"> <li>a) new offence of unauthorised acts relating to a computer that result, either directly or indirectly, in serious damage to the economy, the environment, national security or human welfare, or creates a significant risk of such damage. The offence will carry a maximum sentence of life imprisonment for cyber-attacks which result in loss of life, serious illness or injury or serious damage to national security and 14 years’ imprisonment for cyber-attacks causing, or creating a significant risk of, severe economic or environmental damage or social disruption.</li> <li>b) Extend section 3A (making, supplying, or obtaining articles for use in offences under sections 1 or 3) of the 1990 Act to include an offence of ‘obtain for use’ to cover the event of tools being obtained for personal use to commit offences under section 1</li> <li>c) Extend the existing extra territorial jurisdiction provisions in section 4 of the 1990 Act to provide a legal basis to prosecute a UK national who commits any 1990 Act offence whilst physically outside the UK, where the offence has no link to the UK other than the offender’s nationality.</li> </ul>
<p>Electronic Commerce (EC Directive) Regulations 2002</p>	<p>The Regulations, also known as the “E-Commerce Regulations”, apply to all businesses that sell or advertise goods and services to consumers on the internet or by email. The Regulations govern the information that must appear on a website where a consumer can enter into a contract. Businesses must provide consumers with the following information (this is not an exhaustive list), and some requirements may overlap with ICACS (see below):</p> <ul style="list-style-type: none"> <li>a. Full business name. You must state the full company name (e.g. ABC Ltd), or in the case of a sole trader/partnership, you must state the individual names (e.g. Mr A Bloggs t/a ABC Services).</li> </ul>

	<ul style="list-style-type: none"> <li>b. Full business geographical address (including post code).</li> <li>c. Your (business) contact details, including email address.</li> <li>d. Your VAT registration number (if applicable).</li> <li>e. The price for each item (inclusive of any tax) and delivery costs.</li> <li>f. Clear technical guidance on how to complete the contract online.</li> <li>g. Once the contract has been made online, immediate confirmation of the order to the consumer by electronic means.</li> </ul>
Consumer Contracts Regulations 2013 (ICACS)	<p>The Regulations replace the Distance Selling Regulations 2000 and apply to all online sales after the 13th June 2014. The Regulations require businesses to provide the following information to consumers:</p> <ul style="list-style-type: none"> <li>i. A full description of the goods or services, including how long any commitment will last on the part of the consumer.</li> <li>ii. Total price of the goods or services, or the manner in which the price will be calculated if the total price cannot be determined (including any taxes).</li> <li>iii. Cost of delivery and details of who pays for the cost of returning those items if you have a right to cancel and change your mind.</li> <li>iv. Cancellation rights – including a standard cancellation form. Consumer's cancellation rights start from the time the order is made and have been increased to 14 days (from 7 days) from the day after the goods are received.</li> <li>v. Full business name and geographical address.</li> </ul> <p>Failure to provide the required information, or provide it in the correct format, could result in cancellation rights being extended by up to a year.</p> <p>Unless the return is due to an item being faulty, you must refund the consumer within 14 days of either getting the goods back or on receiving evidence that the goods have been returned e.g. proof of postage receipt (whichever is sooner). The refund must include the item price plus the cost of basic delivery. Exceptions to the consumer's right to cancel, for example, for health and hygiene reasons (Reg28).</p> <p>Other than for a faulty item, or if your terms &amp; conditions state otherwise, the consumer is responsible for paying for all return delivery charges and a business may deduct a 'reasonable' amount if the consumer has handled the goods beyond what is necessary to establish the nature, characteristic and function of the goods.</p>

Consumer Rights Act 2015	<p>The Consumer Rights Act 2015 received royal assent on the 26th March 2015. The Act replaces 8 existing laws including the Sale of Goods Act 1979, Supply of Goods and Services Act 1982 and the Unfair Terms in Consumer Contracts Regulations 1999. The Act came into force on 1st October. It:</p> <ul style="list-style-type: none"> <li>• Addresses digital content as a separate product category and outlines the rights to repair or replace faulty intangible digital content.</li> <li>• Outlines a clearer route for consumers interested in understanding their rights and the remedies they have if they feel goods/services fail to do what was promised.</li> <li>• Clarifies when terms &amp; conditions can be considered unfair.</li> <li>• Clarifies the periods for repair, replacement and refunds related to both good and services</li> <li>• Simplifies the process by which small businesses can take legal action against bigger companies that are breaking competition laws.</li> </ul>
Protection of Children Act 1978	<p>Currently, the Act defines as offences:</p> <ul style="list-style-type: none"> <li>• To take or make any indecent photograph or pseudo-photograph of a child;</li> <li>• To show or distribute such (pseudo-)photographs;</li> <li>• To possess such (pseudo-)photographs with intent to show or distribute them;</li> <li>• To advertise for showing or distributing such (pseudo-)photographs.</li> </ul>
Criminal Justice Act 1988	<p>Section 160 of the CJA 1988 covers the offence of possession of an indecent photograph of a child. There are four defences to this offence: three are listed in section 160(2) of the CJA 1988, and one is listed in section 160A. Three of these defences are very similar to those that apply to some of the offences under section 1 PCA 1978, i.e. marriage, etc of a child aged 16 or 17, legitimate reason, and the defendant's lack of knowledge. The fourth defence, which is not found in the PCA 1978, is that the photograph or pseudo-photograph was sent to the defendant without any prior request made by him and he did not keep it for an unreasonable time.</p>



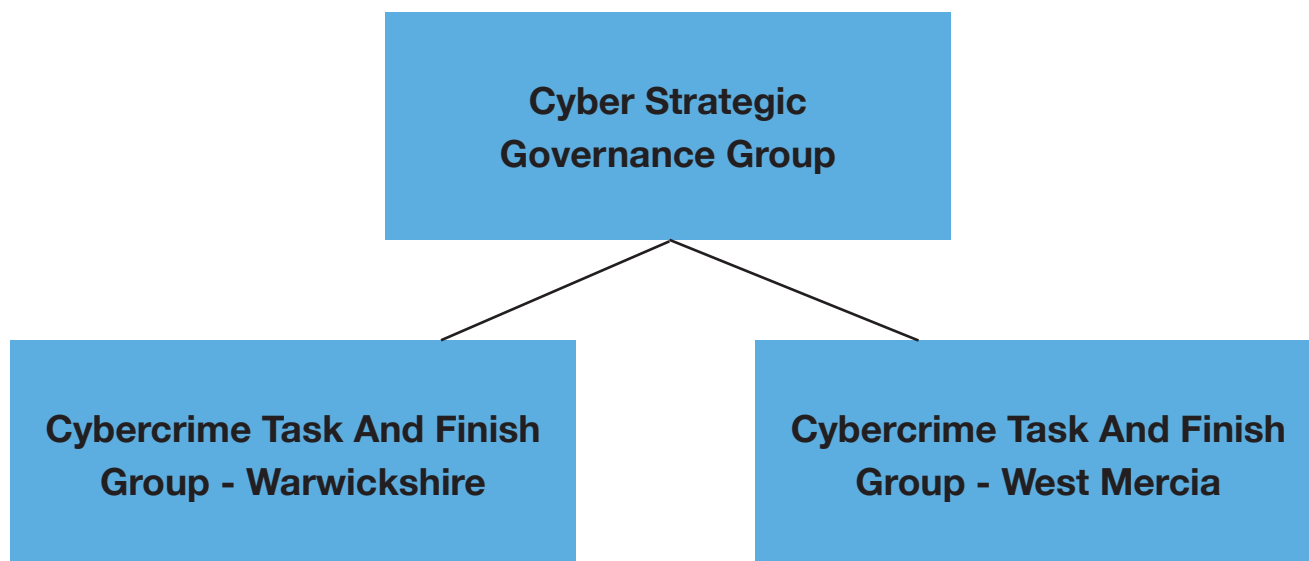
Protection From Harassment Act 1997	<p>Protection from Harassment Act 1997. is the main legislation dealing with harassment. It creates 2 criminal offences (sections 2 &amp; 4) and also authorises civil courts to award damages and make injunctions in harassment cases (section 3). Though it was passed primarily because of concern about 'stalking' the wording of the Act allows it to be used to cover other types of harassment as well as 'stalking'</p> <p>'A person must not pursue a course of conduct</p> <p>(a) which amounts to harassment of another, and</p> <p>(b) which he knows or ought to know amounts to harassment of the other.'</p>
Communication Act 2003	<p>The Communications Act 2003 section 127, covers the sending of improper messages. Section 127(1)(a) relates to a message etc that is grossly offensive or of an indecent, obscene or menacing character and should be used for indecent phone calls and emails. Section 127(2) targets false messages and persistent misuse intended to cause annoyance, inconvenience or needless anxiety; it includes somebody who persistently makes silent phone calls (usually covered with only one information because the gravamen is one of persistently telephoning rendering separate charges for each call unnecessary).</p>
Serious Crime Act 2015	<p>15A Sexual communication with a child</p> <p>(1) A person aged 18 or over (A) commits an offence if for the purpose of obtaining sexual gratification, A intentionally communicates with another person (B), the communication is sexual or is intended to encourage B to make (whether to A or to another) a communication that is sexual, and B is under 16 and A does not reasonably believe that B is 16 or over.</p> <p>For the purposes of this section, a communication is sexual if - any part of it relates to sexual activity, or a reasonable person would, in all the circumstances but regardless of any person's purpose, consider any part of the communication to be sexual.</p>
Criminal Justice and Courts Act 2015	<p>Revenge Porn is the sharing of private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress. The images are sometimes accompanied by personal information about the subject, including their full name, address and links to their social media profiles. The offence applies both online and offline and to images which are shared electronically or in a more traditional way so includes the uploading of images on the internet, sharing by text and email, or showing someone a physical or electronic image.</p>

## Appendix 2 : Partners for Building Block 3 Local Problem Solving & Partners

Name	Role / Duty
Police and Crime Commissioners	The Police and Crime Commissioners for both Warwickshire Police and West Mercia Police have identified cybercrime as a key priority. PCCs have made funds available to contribute to developing the required infrastructure, technical capabilities and skills at all levels during the coming Alliance change programme, all of which, will contribute to building a local response to this emerging threat. In essence the volume of cybercrime is being pushed ever higher by these crimes and by crime groups utilising the cybercrime as a service to enable traditional crime types. The PCCs in Warwickshire and in West Mercia recognise that there needs to be a co-ordinated approach to counter this trend with everyone showing greater awareness and taking action to step up their own on-line security.
Community Safety Partnerships	Community Safety Partnership (CSP) have to develop a Partnership plan which outlines key priorities and a robust action plan and framework which will demonstrate how collectively the partnership works together to reduce crime and disorder.
Health and Well Being Board	Health and Social Care Act 2012 establishes health and wellbeing boards as a forum where key leaders from the health and care system work together to improve the health and wellbeing of their local population and reduce health inequalities.
Local Safeguarding Children Board	<p>An LSCB must be established for every local authority area. The LSCB has a range of roles and statutory functions including developing local safeguarding policy and procedures and scrutinising local arrangements. The statutory objectives and functions of the LSCB are described in the box below.</p> <p>Statutory objectives and functions of LSCBs</p> <p><a href="#">Section 14 of the Children Act 2004</a> sets out the objectives of LSCBs, which are:</p> <p>(a) to coordinate what is done by each person or body represented on the Board for the purposes of safeguarding and promoting the welfare of children in the area; and</p> <p>(b) to ensure the effectiveness of what is done by each such person or body for those purposes.</p>
Neighbourhood Watch	Mid Warwickshire NHW, North Warwickshire NHW, Rugby Borough NHW, Nuneaton and Bedworth NHW, Stratford District NHW, Herefordshire NHW, Telford & Wrekin NHW, Shropshire NHW, North Worcestershire NHW, South Worcestershire NHW.

Name	Role / Duty
Trading Standards	Advice and support for consumers and businesses, and pro active operations in the county of Warwickshire to tackle a range of activity causing harm and loss to our communities.
University of Worcester	The University of Worcester is a British public university, based in Worcester, England. With a history dating back to 1946, the institution was granted university status in September 2005.
Malvern Cyber Cluster	The Malvern Cyber Security Cluster was founded in September 2011 and is run by <a href="#">Key IQ Ltd</a> . The majority of small cyber security companies in Malvern are located at the <a href="#">Wyche Innovation Centre</a> and this is also where the Cluster meetings take place. However, Core companies within the Cluster are spread across Worcestershire, Herefordshire and Gloucestershire with Satellite member companies across the whole of the UK.
Federation of Small Business	The Federation of Small Businesses is the UK's largest campaigning pressure group promoting and protecting the interests of the self-employed and small business owners.
Getsafeonline	Get Safe Online one of the UK's leading source of unbiased, factual and easy-to-understand information on online safety.

## Appendix 3 : Structure & Current Terms of Reference



**Warwickshire Police and West Mercia Police Cyber Crime Strategic Governance Group**

### Terms of Reference

#### **Vision**

Is to create a safe and vibrant cyber environment that delivers social value to the communities of Warwickshire and West Mercia and protects people from harm

#### **Objectives**

- To create effective leadership, and governance arrangements and strategies at all levels to manage the threat that digital crime poses, engaging with all those inside the police service, public and private sector who are able to provide expertise
- Identify those most vulnerable to cyber harm in order to coordinate operational response
- Tackling cyber crime and making cyberspace more secure in order to do business
- Helping to shape an open, stable and vibrant cyberspace that the public can use safely and that supports open societies
- Having the cross-cutting knowledge, skills and the capabilities to underpin all cyber activities
- Lead and support awareness campaigns with public and private sector to protect people from harm
- It will provide a forum to discuss cyber crime issues and identify and share good practice across the alliance area

## **Purpose**

The Cyber Strategic Governance Group is to provide governance for and oversee delivery of the Warwickshire Police and West Mercia Police Cyber Crime Strategy.

## **Scope**

The Cyber Strategic Governance Group will be overseeing the strategic direction of the Cyber Crime Task and Finish Group forums delivery groups to ensure that their work complements the Cyber Crime Strategy and delivery plans. The Cyber Strategic Governance group will be representative of Warwickshire Police and West Mercia Police and partners and will meet on a quarterly basis and report to Strategic Tactical Tasking and Coordination group within a timeline proposed by the Gold Lead for Cyber Crime.

## **Governance**

The Cyber Strategic Governance Group will be accountable to the Assistant Chief Constable nominated as Gold Lead for Cyber Crime and both OPCCs.

An appointed alliance strategic portfolio holder for cyber crime of sufficient seniority and standing will be the Silver lead for Cyber Crime who will report quarterly to the Gold lead.

The Gold lead for cyber crime will be responsible for signing off progress on the deliverables.

## **Inputs to meeting - as required:**

- Strategic threat update
- Update on the cyber crime strategy delivery plan (to include DII)
- Update on delivery group activities

## **Outputs from meeting:**

- Record of actions and decisions
- Delivery and action plan updates

## **Frequency**

Quarterly

## **Review date: June 2017**

## Appendix 4 : Glossary

Term	Explanation
#becybersmart	The Warwickshire Police / West Mercia Police Twitter hashtag referring to an online safety awareness campaign that began in 2014.
Bespoke mobile malware	Malicious software that is specifically built to attack mobile phone or smartphone systems. Often made to order.
Better Policing Collaborative	A collaboration of universities and policing partners to better understand ‘what works’ by way of interventions and the costs and benefits of alternate interventions. Involves universities in the East and West Midlands, as well as others from the North West. Has engaged all forces in the West Midlands together with a number of others from across the UK. Warwickshire Police and West Mercia Police approved involvement with a successful bid in 2014/15, relating to cyber crime and other areas.
Boiler Room Fraud	An illegal practice of calling individuals / potential investors and pressuring them to purchase worthless stock or assets from companies that either do not exist or are virtually bankrupt.
Botnets	A number of Internet-connected computers communicating with other similar machines in an effort to complete repetitive tasks and objectives.
BYOD	Bring Your Own Device – a term used to refer to the current trend in many organisations where an employee or business partner can use their own personal electronic device (phone, tablet, computer, etc.) to interact with that organisation in a business or operational capacity.
CERT, CERT-UK	<p>the UK National Computer Emergency Response Team, formed in March 2014 in response to the National Cyber Security Strategy. The National Cyber Security Strategy, published in 2011, sets out the importance of strengthening the UK’s response to cyber incidents.</p> <p>CERT-UK has four main responsibilities that flow from the UK’s Cyber Security Strategy:</p> <ol style="list-style-type: none"> <li>1. National cyber-security incident management</li> <li>2. Support to critical national infrastructure companies to handle cyber security incidents</li> <li>3. Promoting cyber-security situational awareness across industry, academia, and the public sector</li> <li>4. Providing the single international point of contact for co-ordination and collaboration between national CERTs</li> </ol>



CESG Alpha guidance	<p>The UK government's National Technical Authority for Information Assurance (CESG), advises organisations on how to protect their information and information systems against today's threats. It is the information security arm of GCHQ.</p> <p>ALPHA guidance explains what needs to be considered when designing your organisation's approach to security operations and management.</p>
CiSP	Cyber-security Information Sharing Partnership - A means to allow members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment.
Cloned	The fraudulent copying of bank customer details stored on the magnetic strip or other device used to assist in the making of payment.
Community Safety Partnerships	Community safety partnerships (CSPs) are groups of local agencies who work together to tackle crime and anti-social behaviour, established under the Crime & Disorder Act 1998
Counter-fraud community	Collective term for agencies and professional bodies operating in the field of fraud reduction and counter-operations.
Counter-fraud community landscape	The operating environment for organisations in the counter fraud community. National Fraud Authority is actively looking to reduce and simplify the landscape to improve efficiency and effectiveness, by building relationships, sharing good practice, dealing with the gaps and overlaps. NFA is a good partner to engage for this Cyber Strategy.
CPNI	The Centre for the Protection of National Infrastructure (CPNI) protects national security by providing protective security advice.
CSR2	a governmental process in the UK to set firm expenditure limits and, through public service agreements, define the key improvements that the public can expect from these resources. The Second Comprehensive Spending Review will take effect from 2015/16.
Cyber dependent	Offences that can only be committed by using a computer, computer networks, or other form of ICT.
Cyber enabled	Traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT.
Cyber Essentials	Cyber Essentials is a government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks.

Cyber, Cyber Crime, online and digital crime	Any crime that involves a computer and a network.
DarkWeb, hidden internet	Search terms referring to the content on the World Wide Web that is not indexed by standard search engines. Also known as Deep Web, Deep Net, Invisible Web, or Hidden Web.
Deming cycle	A systematic series of steps for gaining valuable learning and knowledge for the continual improvement of a product or process.
Department for Business, Innovation & Skills	The Government department for economic growth.
Devolution Deal	These are deals agreed between local government and Whitehall, much like previous economic deals (City and Growth Deals). Their purpose is to enable places to take greater control over and responsibility for the key things that make it work.
Evidence based	The integration of best available research evidence with expertise and values
Evidence Based Policing, Evidence Based Policing Matrix	Evidence-Based Policing (EBP) is an approach to policy making and tactical decision-making for police departments. The Evidence-Based Policing Matrix is a research-to-practice translation tool that organises moderate to very rigorous evaluations of police interventions visually, allowing agencies and researchers to view the field of research.
FE	Further Education
G20	Formed in 1999 as a forum for member nations to discuss key issues related to the global economy. The mandate of the G-20 is to promote growth.
HE	Higher Education
Indecent Illicit Images of Children, IIOC	The use of digital technologies to produce, distribute or possess offensive or indecent images of children.
National Strategic Assessment	National Strategic Assessment of Serious and Organised Crime 2015. Published by the NCA. Most recent publication: June 2015.
NCA	The National Crime Agency is a national law enforcement agency in the United Kingdom which replaced the Serious Organised Crime Agency. The NCA's mission is to lead the UK's fight to cut serious and organised crime.

NPCC	The National Police Chiefs' Council (NPCC) is an organisation established on 1 April 2015 representing British police chiefs and acting as a national co-ordinating body for some police activities. It replaces the former Association of Chief Police Officers (ACPO), following the Parker Review of the operations of ACPO which recommended its replacement.
OCG	Organised Crime Group
Online child sexual abuse, OCSE	Term used to describe a genre of internet offending which includes, but is not defined by, traditional notions of online grooming. In this context, OCSE includes the much broader threat from online communication between an adult and a child for the purposes of sexual exploitation.
Phishing	the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.
Police Knowledge Fund	The Police Knowledge Fund aims to develop the understanding and use of research in policing; widen understanding of evidence-based approaches to solve problems and, where there are gaps, develop and build new evidence-based approaches and share learning and knowledge across policing. The fund is a joint initiative between the College of Policing and the Higher Education Funding Council for England (HEFCE). It is resourced by the Home Office and HEFCE, who are also administering the fund.
Ponzi Scheme	A form of fraud in which belief in the success of a non-existent enterprise is fostered by the payment of quick returns to the first investors from money invested by later investors.
PREVENT Duty	From 1 July 2015 all schools, registered early years childcare providers and registered later years childcare providers (referred to in this advice as 'childcare providers') are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". Relevant in this document since the use of online and digital techniques has been prevalent in numerous instance of grooming and radicalisation.
Social networking	The use of dedicated websites and applications to interact with other users, or to find people with similar interests to one's own.
Strategic Governance Group, SGG	The single, senior group for direction and control of the cyber strategy in Warwickshire Police and West Mercia Police.

Strategic Policing Requirement	A document, published by the Home Secretary that sets out the national threats that the police must address. Most recent publication: March 2015.
Victim demographic	A term used to describe (but not identify) unique groups affected by an incident or crime. The primary purpose is to aid comparisons between groups.
Vision	A vision, or vision statement identifies what a company would like to achieve or accomplish.