LINCOLNSHIRE POLICE

CYBER CRIME STRATEGY
CONTENTs

Introduction........................................................................................................................................1

What is Cyber Crime?.........................................................................................................................2

What are our aims and objectives?.................................................................................................3

Prevent................................................................................................................................................4

Prepare................................................................................................................................................5

Pursue..................................................................................................................................................7

Protect...............................................................................................................................................8

Timeline...........................................................................................................................................9

Summary.........................................................................................................................................9
Introduction

Lincolnshire Police is committed to reducing crime and protecting victims of crime. This strategy will set out what Lincolnshire Police will do to effectively manage cybercrime in order to minimise the impact of this rapidly evolving crime type on the residents and communities within the county. The strategy will look at both the prevention and detection of offences, but will also focus on how we will support those who report offences within Lincolnshire to reduce the chances of repeat offending against them by increasing their awareness of and vigilance towards this, and other similar, crime types.

The Police and Crime Commissioner, in his plan for 2017 – 2021 has set, amongst others, the following objectives which are relevant to how Lincolnshire Police will deal with cybercrime:

- Work with partners like trading standards and social care to identify and disrupt threats to the vulnerable, for example from targeted ‘scamming’.
- Work in partnership with Action Fraud at the City of London to share information, co-ordinate response and collaborate in the national battle against the growth of fraud and cybercrime.
- Provide strong and resilient specialist police support service for major crime, serious and organised crime, forensics and other areas through collaboration with Forces in the east Midland region.
- Work with local authority partners, the health service and voluntary and community organisations to identify and support the vulnerable in our communities so that they do not become the victims of crime, bullying or intimidation, for example supporting those on ‘sucker lists’ of fraudsters, being victims of ‘mate’ crime or the elderly tricked by doorstep conmen.

Just as the types, and methodologies of cybercrime are varied, so too are the potential and identified victims. Victim profiles span a broad spectrum of the population and include both businesses and individuals, each of which is often targeted for different offence types and different methods of offending.

Where individuals are the victims of cybercrime, particularly cyber enabled crimes (such as fraud or distribution of indecent images), they are often within categories of people who are deemed to be, to some degree, vulnerable. They are often targeted for their vulnerability and susceptibility to these types of offences and they often have a significantly detrimental impact on them and their day to day lives. Therefore, it is not simply a traditional approach to targeting offenders and detecting offences which will be prioritised but also a focus on prevention of offences and provision of support and guidance to victims to prevent them from becoming a repeat victim.

However, it is not just vulnerable individuals who can become victims of this offence type. Essentially any users of technology or digital devices can be susceptible to becoming victims of these offences.

Recent figures provided by the NFIB highlight the scale and potential for increase in cyber related offences as follows:

- 82% of adults in the UK used the internet daily or almost daily in 2016
- At least 6% of adults experienced an incident of fraud in the year to 30 September 2016
- In 39% of incidents where money was taken or stolen from the victim, the loss was £250 or more in the year ending 30 September 2016
- 103% increase in ‘card not present’ fraud, including over the internet, between 2011 and 2016, to 1.4 million cases

The Office of National Statistics reports that, of an estimated 11.8 million crimes reported nationally in the year to 30 September 2016, 16% (1.9 million offences) were cyber related frauds. This does not take into account other cyber related offending which would increase this figure substantially to an estimated 47% according to figures from NFIB. They also show that the number of reported frauds is likely to be less than 20% of the actual number of frauds committed. Whilst these are national figures, the percentages are likely to be largely reflective of the situation in Lincolnshire.
What is Cyber Crime?

In its simplest form, cyber crime is any offence which is committed through, or enabled by, the use of technology, whether or not the offence is predicated solely on the technological element or whether the technology merely assists the perpetrator in the commission of the offence.

The spectrum of offences which the term cyber crime encompasses is incredibly broad and, dependent on the offence itself can have a significant impact on the welfare, health and reputation of the victim. Victims can be either individuals, who are usually victims as a result of some social engineering, or businesses who are targeted victims for significant financial loss through the cyber dependent ‘hacking’ and malware type offences.

### Cyber Spectrum

<table>
<thead>
<tr>
<th>Digital Footprint</th>
<th>Internet Facilitated</th>
<th>Cyber Enabled</th>
<th>Cyber Dependent</th>
</tr>
</thead>
<tbody>
<tr>
<td>The trail of data left behind by users of digital services, both through device signatures and online activity</td>
<td>Traditional crimes where the internet and digital devices are a component in the facilitation of crime</td>
<td>Existing crime types transformed in scale, speed or reach by use of the internet and computers</td>
<td>Committed using computers, computer networks or other information communication technology (ICT).</td>
</tr>
</tbody>
</table>

**Typical crime types:**
- Homicide
- Burglary
- Robbery
- Fraud

**Typical crime types:**
- Harassment
- Stalking
- Commercial burglary
- Purchasing illegal items

**Typical crime types:**
- Fraud
- Child Sexual Exploitation
- Distribution of indecent images

**Typical crime types:**
- Malware
- Viruses
- Denial of Service (DOS)
- Hacking

Cyber crime reporting is increasing, both nationally and within Lincolnshire with figures from NFIB indicating that 47% of all crime is cyber or fraud related. It is becoming increasingly difficult to separate fraud from cyber as the technological enablers of email and mobile devices have increased the potential for offending in this way exponentially, not to mention making it harder for the offenders to be identified and caught as they can now commit offences anywhere in the world.
What are our aims and objectives?

By 2021 Lincolnshire Police will:

1. Prevent and reduce the amount of, and harm caused by, cybercrime in Lincolnshire
2. Prepare Lincolnshire Police, other organisations and the public to recognise, resist and respond to cybercrime appropriately.
3. Pursue those responsible for committing cybercrime, bringing them to justice and recovering their criminal assets.
4. Protect and safeguard victims of cybercrime.

<table>
<thead>
<tr>
<th>PREVENT</th>
<th>Understand the risk and threat we face from cybercrime by maintaining a current threat and risk assessment, engaging with key partners to help inform this.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prevent individuals from being drawn into, or continuing with, cyber criminality by:</td>
</tr>
<tr>
<td></td>
<td>• Engaging with schools, communities, partners and businesses to share messages around cyber criminality</td>
</tr>
<tr>
<td></td>
<td>• Promote Cyber-Security Information Sharing Platform and Cyber Essentials programme to local businesses</td>
</tr>
<tr>
<td>PREPARE</td>
<td>Equip all staff with a relevant level of training around cyber-crime that will ensure a competent and professional investigation, ensuring that national and regional learning is assessed and embedded locally.</td>
</tr>
<tr>
<td></td>
<td>Build access to a variety of technical equipment and other software that will support investigations and intelligence gathering, referring to and accessing resources within the Regional Cyber Crime team.</td>
</tr>
<tr>
<td></td>
<td>Achieving accreditation of Digital Forensics Unit in accordance with ISO 17025 to ensure equipment and processes withstand scrutiny in a criminal court.</td>
</tr>
<tr>
<td></td>
<td>Work with partners, other organisations and the public to ensure key messages are distributed to the public, to assist them in identifying and addressing vulnerabilities as well as identifying possible cyber attacks and knowing how to respond.</td>
</tr>
<tr>
<td>PURSUE</td>
<td>Ensure internal information management systems are equipped to manage cybercrime.</td>
</tr>
<tr>
<td></td>
<td>Ensure staff identify all opportunities to pursue cyber criminality and bring offenders to justice wherever possible.</td>
</tr>
<tr>
<td></td>
<td>Utilise specialist resources within the region and nationally to escalate the most serious and complex of cyber investigations.</td>
</tr>
<tr>
<td></td>
<td>Ensure local specialist support is available for all investigations and that SIOs and OICs are aware of the digital investigative opportunities in all crime, considering this at the earliest opportunity within an investigation.</td>
</tr>
<tr>
<td>PROTECT</td>
<td>Deliver an effective tactical response that will raise public confidence in and awareness of cybercrime investigative capabilities by maximising media opportunities and good news stories.</td>
</tr>
<tr>
<td></td>
<td>Work with local communities to raise cybercrime prevention and mitigation through increased messaging through traditional and social media, ensuring bespoke packages are available and delivered to the most vulnerable groups.</td>
</tr>
<tr>
<td></td>
<td>Fully understand the impact of cyber offences on victims and allow their experiences to inform and improve our responses by debriefing victims, offering prevention advice and utilising victimology information provided by Home Office Segmentation and other data.</td>
</tr>
</tbody>
</table>
How we are meeting our objectives

Prevent

With the ever increasing opportunities and methodologies for offenders to commit crime through the use of technology, and the opportunities the internet provides for offences to be committed on a world wide scale, detection of offences, whilst important, is a disproportionate use of finite resources when attempting to protect the communities of Lincolnshire against this crime type effectively.

It is estimated that 80% of cybercrime is potentially preventable. Based on this, prevention is the focus for the cybercrime strategy with a view to protecting the public and businesses of Lincolnshire from the possibility of people committing offences against them.

Additionally, work around preventing individuals from entering into cyber criminality is just as key. As the population are increasingly computer literate, with resources readily available to them for hacking. Whilst this often seems like harmless fun or personal challenges amongst friends, the impact and significance of their offending is often not realised by them.

Understand the risk and threat we face from cybercrime by maintaining a current threat and risk assessment, engaging with key partners to help inform this.

In order to be able to provide meaningful and current crime prevention advice and guidance to residents, communities and businesses within Lincolnshire it is important that we actively seek to research and understand emerging trends, new methodologies of offending and improvements in cyber security which can be passed on to the public in order to reduce their vulnerability to cyber criminals.

There are a number of existing websites and services available with resources for prevention advice and awareness and education surrounding cybercrime. Efficiency would dictate that we link in with these other organisation and provide consistent, existing advice to communities to reinforce predetermined good advice where this is appropriate. Lincolnshire Police is using Get Safe Online who provide up to date, relevant advice and deliver this to local business forums and engagement events. They will also support training of frontline staff to assist in increasing their knowledge to further disseminate good practice around cyber security.

Prevention campaigns will be targeted based on analysis of offending within the county. This will mean that victimology work will identify those groups of our community who are most vulnerable to specific categories of cybercrime and advice, guidance and delivery of the same will be focused to ensure that the impact of the message is as wide reaching as possible whilst remaining relevant to its intended audience.

Targeted campaigns will also be addressed towards the business community. Although only approximately 5 % of our reported offences are from businesses, there is evidence that businesses are significantly less likely to report offences of this nature than individual victims. In addition to this, business victims are likely to have a considerably higher financial loss, as well as compromising customers details and company reputation, all of which has a substantial impact on the local economy. In order to address this, Lincolnshire Police will promote the Cyber-Security Information Sharing Platform and Cyber Essentials programmes to local businesses.

The Cyber Security Information Sharing Platform is a government initiated scheme which delivers a key component of the UK’s cyber security strategy in facilitating the sharing of information on cyber threats in order to make UK businesses more secure in cyberspace.

The partnership includes the introduction of a secure virtual ‘collaboration environment’ where government and industry partners can exchange information on threats and vulnerabilities in real time. The Cyber Security Information Sharing Partnership will be complemented by a ‘Fusion Cell’ which will be supported on the government side by the Security Service, GCHQ and the National Crime Agency, and by industry analysts from a variety of sectors. They will work together to produce an enhanced picture of cyber threats facing the UK for the benefit of all partners.
Cyber Essentials is another government backed initiative which guides businesses through the basic cyber security measures they should be employing to protect themselves against cyber attacks. Once implemented, they offer an Assurance Framework which enables the company to prove and promote their cyber security to their customers.

By promoting this scheme and working with businesses to join the partnership, Lincolnshire Police will assist companies in becoming their own capable guardians and safeguarding their systems and assets from cyber attacks to the best of their ability.

Prevention campaigns will be launched, not just by Police, but in conjunction with partner agencies through a co-ordinated communication strategy to ensure maximum reach and impact is delivered.

**Prevent individuals from being drawn into, or continuing with, cyber criminality**

With computer science an increasing part of the school age curriculum and youths’ knowledge of technology and computer literacy increasing, they are ever more vulnerable to being drawn into cyber criminality, whether intentionally with malicious intent or through naivety, personal challenge or manipulation by others. This is, therefore, a key piece of work to educate individuals about the potential consequences of such offending, together with raising awareness of what constitutes a cybercrime.

Work is already ongoing with local policing teams in schools, both primary and secondary schools, across the county through initiatives such as JPCSOs and Mini Police as well as regular engagement and inputs around key themes.

Cybercrime has not, historically, formed part of these educational inputs, however this will be amended, with PCSOs and local policing officers receiving training from Get Safe Online in order to raise their awareness of this area of business to enable them to deliver the basic information to youths.

**Engaging with schools, communities, partners and businesses to share messages around cyber criminality**

Local policing teams are engaging with these communities on a daily basis providing crime prevention advice in relation to a broad spectrum of offences. Cybercrime inputs and awareness are increasingly forming part of these inputs but there is still work to be done in this area.

Get Safe Online have been employed by Lincolnshire Police to support this delivery of education and prevention within the county. They do this through training inputs to local staff and also through delivery of engagement events to local business forums and community groups in conjunction with crime prevention teams and local policing.

Lincolnshire Police aim to make cyber awareness part of mainstream policing in keeping with the increasing prevalence of this offence type. In doing so, the continued dissemination of crime prevention advice, with campaigns adapted and delivered in bespoke ways to their intended audience, based on victimology profiles, will assist in raising awareness and vigilance, target hardening and reducing offences within the county.
Prepare

Equip all staff with a relevant level of training around cyber-crime that will ensure a competent and professional investigation, ensuring that national and regional learning is assessed and embedded locally.

As cyber criminality and reported offences of cyber dependent and cyber enabled crime grow, combined with the scale of influence technology growth and development has on traditional crime types becoming internet facilitated and having a significant digital footprints, it is inescapable that cyber offending is becoming mainstream in terms of investigative opportunities.

As a consequence of this, the knowledge, awareness and training of frontline staff needs to meet this demand and investigators need to be suitably equipped to provide an appropriate and proportionate investigation and service to the victims of these crimes.

Continual training to provide initial, and updated, awareness around investigative opportunities, emerging threats and trends and evidential requirements is in progress across the force area. Inputs are delivered by Digital Media Investigators to a number of training courses provided by Learning and Development including Initial Police Training, PCSO training, CID training courses and supervisors development courses.

Further inputs are delivered at relevant and appropriate seminars and pro active engagement by DMIs to the wider organisation on a case by case basis is also delivered.

The Lincolnshire Cyber Crime Unit utilise resources from within the Regional Cyber Crime Unit to access information about emerging trends, new developments and learning from other organisations. This information is shared with the wider organisation through a number of communication channels to maintain continual updating of professional competence of officers in this arena.

Build access to a variety of technical equipment and other software that will support investigations and intelligence gathering, referring to and accessing resources within the Regional Cyber Crime team.

Lincolnshire Police has invested in mobile telephone kiosks which allow frontline officers to download evidence from mobile telephones to support them in their day to day routine investigations.

For more complex and specialist examination of digital devices the Digital Forensics Unit is capable of examining computers and mobile phones to a more in depth level.

In addition, other specialist, covert measures can be utilised should the criteria be met to obtain the relevant authorities based on the nature and circumstances of the investigation.

Digital Media Investigators continue to be an important conduit for digital investigations and provide specialist advice and guidance to officers both within the force and also by referring cases to the Regional team or elsewhere as may be appropriate.

Achieving accreditation of Digital Forensics Unit in accordance with ISO 17025 to ensure equipment and processes withstand scrutiny in a criminal court.

Accreditation under ISO 17035, as assessed by UKAS, is a requirement of the Forensic Science Regulator to ensure that processes and procedures, along with training and competence of staff are reliable and trustworthy. This is, without doubt, key to providing successful outcomes at court and ensuring that offenders are brought to justice.

Lincolnshire Police Cyber Crime Unit are working with the East Midlands Special Operations Unit Forensic Services (EMSOU-FS) to formalise processes and complete successful assessment under UKAS.
This process seeks to formalise existing processes and provide an accredited standard by which evidence can be assessed and compared in a court of law, ensuring that the evidence provided by each Digital Forensics Unit in the country is of a comparable standard.

Work with partners, other organisations and the public to ensure key messages are distributed to the public to assist them in identifying and addressing vulnerabilities as well as identifying possible cyber attacks and knowing how to respond.

Lincolnshire Police understands that preparedness for cyber attacks is not something which is effectively achieved in isolation of other organisation or the wider community.

Pursue

*Ensure internal information management systems are equipped to manage cybercrime.*

*Ensure staff identify all opportunities to pursue cyber criminality and bring offenders to justice wherever possible.*

As the use of technology in day to day life increases and becomes an intrinsic and integral part in the way people do business, shop and interact with one another, there are myriad opportunities to utilise these digital footprints throughout the course of an investigation, regardless of the offence which has been committed.

There remain very few, if any offences, which do not have a digital footprint of some description and investigation into cyber offences is becoming more mainstream. As such, it is important that frontline officers are able to identify the potential digital investigative opportunities and know how to progress these through the appropriate and proportionate channels.

Lincolnshire Police utilised existing good working relationships with a number of key partners, including Lincolnshire County Council, Victim Support, Educational establishments and Business Forums, together with the voluntary sector to maximise dissemination of key messages and advice to key audiences. In sharing this responsibility and working in partnership the public of Lincolnshire have best opportunity to be aware and prevent themselves from becoming victim of this type of crime.

The Cyber Crime Unit work closely with regional counterparts and other internal departments and continue to forge and foster such relationships in order to enhance the provision and reach of this service within the community.

Utilise specialist resources within the region and nationally to escalate the most serious and complex of cyber investigations.

In addition to the resources available in Lincolnshire, Lincolnshire Police have access to additional cybercrime resources and investigators both regionally and nationally.

East Midlands Serious Operations Unit have a regional Cyber Crime team who are able to assist with, and investigate, larger scale cyber dependent offences. Lincolnshire Cyber Crime Unit maintain a close working relationship with this team to both learn from them and their expertise and also to ensure that appropriate cases are referred to them for investigation in a timely and efficient manner to ensure that evidence is captured quickly, maximising the opportunities for identifying the offender and preventing loss, or further loss, to the victim.

For investigations within Lincolnshire which may have a national implication, EMSOU can progress this investigation through to the National Cyber Security Centre, whereby Lincolnshire resources will support the investigation with local enquiries and investigative actions.
**Ensure local specialist support is available for all investigations**

With the increase in identification of digital investigative opportunities by frontline officers, it is important that the specialist resource within the Digital Forensics Unit is able to meet the demand that will be placed upon them, not only for cyber enabled offences but also for cyber dependent offences, which are also likely to increase in terms of reporting as the awareness and vigilance increases through proactive engagement and prevention work within the community.

Lincolnshire Police, in addition to enhancing our own capability in this area through development and training of our staff, will seek to explore opportunities for increased collaboration with regional forces in the interests of increased specialist capacity and capability.

**Ensure that SIOs and OICs are aware of the digital investigative opportunities in all crime, considering this at the earliest opportunity within an investigation.**

---

**Protect**

**Deliver an effective tactical response that will raise public confidence in and awareness of cybercrime investigative capabilities by maximising media opportunities and good news stories.**

Through the education of frontline officers and the mainstreaming of cyber investigation throughout the organisation, the initial response to reports of cybercrime will continue to improve.

Officers will continue to develop their knowledge and expertise around digital investigative opportunities and, where this is beyond the scope of their skills and remit, they will be able to identify opportunities, seize devices and submit them for appropriate examination to secure evidence of the offence.

Where appropriate, Digital Media Investigators will attend crime scenes with frontline officers in order to secure evidence at the scene, continually improving the service provided to victims of this crime type.

All available media opportunities will be taken as part of a wider communications strategy to highlight the good work conducted within the organisation. The intention of this will be threefold:

- to improve the confidence of the public of Lincolnshire in our ability to effectively investigate cybercrime
- to raise awareness within the communities of Lincolnshire that, despite us being a rural county, cybercrime is still prevalent in the area
- alert would be cyber criminals to the fact that Lincolnshire Police will pursue all criminals, including cybercriminals and will, wherever possible, bring offenders to justice.
Work with local communities to raise cybercrime prevention and mitigation through increased messaging through traditional and social media, ensuring bespoke packages are available and delivered to the most vulnerable groups.

With an increase of training of local officers and frontline staff, a logical progression is for this to be incorporated in day to day business and interaction with local communities, whether through formal, pre-planned engagement events or ad hoc individual interactions.

Local policing staff are key to identifying vulnerabilities within their community, or identifying those within their communities who are most at risk of becoming victims of cybercrime based on the victimology and analysis conducted both within the organisation and by national bodies such as NFIC and Office of National Statistics.

It is insufficient to simply identify these groups and, in conjunction with Crime Prevention officers, local policing staff will ensure that appropriate messages are disseminated in the most appropriate manner to meet the target audience, thereby target hardening key communities and reducing the opportunities for them to become victims.

Fully understand the impact of cyber offences on victims and allow their experiences to inform and improve our responses by debriefing victims, offering prevention advice and utilising victimology information provided by Home Office Segmentation and other data.

Op REVIVE and Op REPEAT are both Community Safety and Crime Reduction initiatives which run within Lincolnshire Police, led by the Crime Reduction Team.

Both of these operations are crucial to providing safeguarding advice and support to victims of crime. Through their visits to victims of cybercrime (predominantly frauds) they are able to identify vulnerability issues and ensure that appropriate referrals are completed. Their feedback from these conversations will allow the organisation to continue to develop and tailor prevention messages and options available to us to reduce offending of this type within the county.
Lincolnshire response to cybercrime, under any of the four key areas highlighted within this document is, and will continue to be, an ever evolving task. This is essential to ensure that we continue to meet the demands of cybercrime and also to get upstream of offending through appropriate and timely horizon scanning to enable prevention to remain the focus and protect the communities of Lincolnshire.

As with any other crime type, cybercrime cannot be effectively tackled by Lincolnshire Police in isolation and we will, therefore, continue to develop relationships with partners, businesses and communities to ensure that, as far as possible, cyber criminality will be increasingly difficult to commit against residents of Lincolnshire.