Notes - NHW Conference of 22nd October 2016

1. Introduction

John Fuller, Chairman of Cambridgeshire Neighbourhood Watch, introduced himself and welcomed all attenders. He then outlined the programme for the morning, covering the Conference and the subsequent Annual General Meeting.

The conference would cover four topics: –

1. A review by Jason Ablewhite, the Cambridgeshire Police and Crime Commissioner, of his first five months in post and his plans for the future.
2. Chief Superintendent Vicky Skeels, Cambridgeshire Territorial Policing Commander would review the challenges and necessary changes to policing in the County.
3. Cybercrime: guidance from Rebecca Tinsley, Cambridgeshire Constabulary Cyber Security Adviser, on how to avoid becoming a victim.
4. No Cold Calling Zones in Cambridgeshire: an introduction and updating on current policy by Charlotte Homent, Manager of Community Protection, Cambridgeshire County Council.

The following notes give the key points that the speakers made.

2. Jason Ablewhite

The PCC started by highlighting some of the significant eye openers that he had received when "shadowing" Police patrols including a number of full night shifts. These patrols showed him the significance of alcohol-related crimes particularly on Saturday nights. What he saw emphasised the role of volunteers assisting the police, in particular the Street Pastors at 3 AM in the morning. Two other specific mentions were "naked trampolining" at Huntingdonshire's 'Secret Garden Party' and patrols in Cambridge City centre over the weekend when England were playing in the Euro's.

Significantly, experiences with the police patrols showed that many of the pressures on the Police come from areas that are not visible to the general public. Though not widely discussed, the facts are that most of Cambridgeshire has some of the safest places in the UK, while at the same time having some of the most deprived. Parts of Peterborough are slipping below Luton and Edmonton in term of criminality. Inevitably, there is a mismatch between what resident organisations and NHW volunteers want, and the overall demands on the Police force.

In addition, Cambridgeshire Police force has lost £16 million from the budget over recent years and is now faced with taking another £7 million from the budget.

The challenges include mental health, domestic violence, child sex exploitation, and hate crimes. These very real issues can only be tackled effectively with joint action involving the Councils, the NHS, The Fire Brigade, and other agencies. Across the county, the Police spend 50 man-hours a day in Accident and Emergency departments supporting people with mental health needs. These hours could be considerably reduced if the individuals were handed over to medical staff within 15 minutes.

There have been massive increases in the number of domestic violence and cases of child sex exploitation that are now being reported. This is another area where the nature of policing is having to change.

Exposure to these realities of current policing made very clear that what residents want of their police is very different from what Society needs. However, Mr Ablewhite said that he would "protect the "Front Line" come hell or high water". To do this, Cambridgeshire Police are working with their counterparts in Bedfordshire and Hertfordshire to share high cost specialised services, not least the mobile firearms units, dog units. Also, through joint purchasing the target is to save 20% of total purchase costs. Additionally, a seven Force initiative with other East Anglian, Essex and Kent forces could collectively save in the region of £190m per year.

Another initiative is that of "leveraging assets". For example, the Cambridge Parkside Police Station space is currently only 25% utilised and the station occupies extremely valuable real estate. In addition, the custody unit at Parkside is not fit for purpose and could just as easily operate at a different location.

Another area of increased demand is that of support for victims and witnesses of crimes. The establishment of the Victims Hub has generated considerable progress in this area.

Overall, Mr Ablewhite said that he had seen how extraordinarily professional the police are even when at personal risk. He was heartened by the involvement of Neighbourhood Watch and the large numbers of volunteers. He had held discussions with the Chief Constable on how best to support volunteers and leverage their input. The significance of the volunteer efforts is shown by the fact that Speedwatch now has over 2000 trained volunteers across the County and that Countryside Watch is also very active. He said "I thank each and every one of you and your associates for your input". He was funding a full-time support staff member to work with and support volunteer groups.

In addition to the existing challenges, new ones are emerging, not least "Cybercrime". Already, residents are more likely to be affected by cybercrime than by street mugging or burglaries. The police force needs to react and is indeed doing so as you will hear later this morning.

He mentioned his determination to break down silos between emergency services and welcomed the opportunity to take on responsibility for the Fire Service and called for much closer working and sharing of resources between emergency services.

Question: Our local PCSO is demoralised because there is no time for community policing.

Answer: the PCC said that Vicky Skeels would deal with the operational aspects but that he should point out that community policing involves more than just the police. There is a pilot multi-agency approach in Peterborough involving community safety organisations.

Moreover, in Cambridge, 90% of the crime occurs in just five areas. More visible policing in those areas will clearly offer greater benefit than street patrols in areas of negligible crime.

The PCC reported that so far his office had received 3½ thousand responses to the survey which is providing input to the 'Policing Plan'. The responses will be collated to provide directions for the strategic plan also.

Question: How are the police now using "technology"?

Answer: Cambridgeshire is believed to be on the "frontline" in the use of some new technologies, for example tablets. Frontline officers now carry tablets to allow completion of documentation without the use of paper. This has reduced the typical time taken to record incidents from90 minutes to 20 minutes. The introduction of new technologies of course is challenging.

Question: The Police: 101 system is still not working effectively: recently I had five calls that failed before I made contact with a call handler.

Answer: The PCC acknowledged that the questioner was "absolutely right". However, there are two issues. First that there has been a steady loss of trained call handlers who are poached by commercial call centres. Second, while the Cambridgeshire call centre is now at full strength (following the recruitment of 13 staff) further recruitment is on hold during exploration of the practicality of having a three-county centre. The PCC said that it is essential that 101 works well and "I commit to a good service" and will visit the centre next week.

3. Chief Superintendent Vicky Skeels:

Territorial Policing Commander Cambridgeshire Constabulary

VS started her talk with a message of appreciation and thanks from the Chief Constable, Alex Wood, for all that NHW does.

She then gave a brief overview of her career since her Beat Police Constable start at Parkside as graduate (then rare) in 1988. Subsequently, much of her career has been associated with Cambridgeshire.

VS emphasised that the Constabulary is working hard to be an open and transparent organisation. NHW and other organisations are helping that task and despite some of the negative stories, most of the Force staff have a clear view of the requirements of modern policing and public service. This has been confirmed by staff surveys.

Policing is now massively different from 1990. Then, there were no computers, no armed response units (though there was a greatly increased rate of "Ram Raids" carried out by brazen gangs), there was a very high volume of car crime, and all pubs closed by 11 PM. The changed environment also includes –

- terrorism, which remains very likely
- requirements for the police to be involved in public disturbances such as those related to Halloween, bonfire night, et cetera., and, of course, the sudden emergence of "Killer Clowns" (20 reports so far across the County raising concerns about Halloween)
- supporting vulnerable people
- great reductions in "acquisitive crime"
- child protection and other Crime Prevention areas
- cybercrime - a particular challenge since many officers are not computer literate.

As an illustration, she pointed out that at the start of her career, if a car was stopped the police would check the tax disc and whether the tyres were bald. Now they are much more likely to ask two men in the front why there are two young girls in the back.

These changes require a different mind-set.

Demand is not reducing with 450,000 calls last year. 70% of policing now involves some aspect of public concern or welfare elements and are often very urgent. The result of this is that frontline staff, who might have been en route to give a presentation at a school, might have to be diverted to address an urgent call. 7% of calls are related to domestic violence, 13% of calls are mental health-related and, again, this is an area where most police are not well trained, 5% relate to alcohol, and between 4% and 5% relate to vulnerable people and children.

These challenges mean that inevitably traditional "officers on the beat" policing is now under massive pressure.

New technology is being the used effectively. Expertise with DNA is proving vital: for example, forensics (including examination of materials left on the soles of shoes), Automatic Number Plate recognition (APNR) coupled with data connections to the Licensing authority (DVLA), and the Armed Response Units. The Force is working with Bedfordshire and Hertfordshire on such expensive resources, also including traffic patrols and dogs.

The vulnerable are now a significant part of community policing. The vulnerable groups include the old, those with learning difficulties, the mentally ill, those with mental disabilities, those demonstrating alcohol and/or drugs dependency, and the infirm. The Police are unable to address these challenges alone and depend on the support of PCSOs, the public, and other service groups.

The PCSOs are now receiving more appropriate training and are assigned to specific locations with defined objectives: for example where there are victims to be supported, being present on streets where burglaries have occurred, and dealing with ASB issues including cycling.

The Force is now consciously seeking to build trust with communities through interaction with young people and ongoing contacts at an individual level on streets, not least with minority and marginalised groups.

The force continues to be committed to supporting Neighbourhood Watch and will explore how better to achieve that through contact and discussions with volunteers.

Question: Please can we have a more visible presence of PCSOs in the villages?

Answer: We are retaining about 150 PCSO positions across the county. However, the Force needs to ensure that their focus is "fit for purpose". Moreover, they need to work in cooperation with, for example in the community safety staff as in Peterborough. The structures are now in place to direct police officers to the locations where they are needed.

Question: One of our problems is that the police personnel seem to move-on as soon as we have got to know them: this applies at all levels.

Answer: The aim is for staff to stay in post for a reasonable period with a three year target. However, individuals have their own career objectives and many will apply for new positions within that time. These forces cannot be resisted but we do recognise the residents' frustration.

Question: Incidents involving people with mental health problems need support from ambulance staff: can they patrol together?

Answer: We sometimes operate joint patrols and we now have three mental health staff working in the control room. We are also looking to get more assistance from the Fire Brigade who are better equipped to gain access to properties if there are concerns about the people who are living there.

Question: You mentioned the challenge of young girls being found in cars along with older men: what should concerned residents do if they have a hunch that a vehicle falls into that category?

Answer: Anyone with such concerns should use 101, or alternatively, Crime Stoppers.

Note that the Police will not always respond immediately to such calls since some may be appropriate to be referred to other county or city authorities.

4. Rebecca Tinsley: Cyber Crime Security Adviser

The Cambridgeshire Cyber Crime Investigation Unit was set up at the end of 2015 in response to the Government declaring cybercrime to be a Tier 1 national threat. It comprises three teams: one investigating cyber dependent crime, one addressing serious and complex fraud, and the cyber security adviser.

Rebecca Tinsley's presentation was structured by the slides that she used that are summarised in the Appendix.

RT illustrated the scope of the challenges with examples of recent crimes: –

- Distributed Denial of Service (DDoS) caused by thousands, perhaps millions, of computers which have been "captured" by criminals and used to send vast numbers of messages to a website or server. The target company becomes overloaded and is unable to operate. Recently, Twitter and other international services were subject to this form of attack and went off-line for several hours. This attack is thought to have been aided by the use of household Wi-Fi enabled equipment such as web cams and thermostats.
- A variety of techniques are used to enable criminals to take control of computers and servers. USB memory sticks, loaded with malware, have been dropped in car parks. Reportedly, around 60% of those finding such memory sticks will connect them to their computers to see what is on the stick. Malware will automatically compromise the computer, and enable control of their computer by the criminals.
- Criminals search social media to collect data about individuals and this enables them to send very plausible emails that persuade the recipient to take actions which give the criminals the openings they need to commit their fraud.
- Free Wi-Fi is becoming increasingly available in public places such as buses, café's, and hotel public rooms. This generates two key exposures. First, criminals are known to have set up their own Wi-Fi base within an area where there is such a service. When their signal is stronger than the service signal, this will attract users. Anyone using that Wi-Fi will give the criminals full access to their computer/phone/tablet. They can then access and copy data, or simply monitor transactions and collect IDs and passwords. One defence is to use BT FON which is widely available: another is to ensure that only legitimate Wi-Fi signals are accessed.
  Second, criminals can sit in the service area and pick up the signals passing between users' computers and the service Wi-Fi base. This will enable them to monitor and copy transactions and Passwords. The only protection is to access only "https:\\" websites: these encrypt all communications to and from the user's PC.
- The number of cyber crimes committed during 2015 has been estimated as between two and six million. So the message could be that it is not a question of if, but when, you might be a victim.

The good news is that at least 80% of these crimes could have been prevented if all computer users following some simple rules. RT's three key pieces of advice were: –

1. Use strong passwords: where allowed, these should involve upper and lowercase letters, numbers, and symbols.
   Use a different password for each site that requires one.
2. Install, and keep up to date, good security software.
3. Always install application and operating system software updates: most updates are issued to correct known weaknesses that have been used by criminals.

In addition, RT referenced the five guidelines from the banking industry. This was endorsed by an attender who recommended the guidance from Norwich and Peterborough Building Society. See the last page of the Appendix.

Rebecca ended her presentation with an invitation for volunteers to be trained to deliver a three-hour session for others who are interested in cybercrime prevention.

Question: Are the wallets and pockets that are being sold to protect the credit cards that are radio enabled worth the money.

Answer: They are effective, but before purchasing, consider the risk of having the card compromised. Putting a layer of aluminium (cooking) foil around the card or cards would be similarly effective. Also, when the card is actually being used, it is also potentially at risk.

5. Charlotte Homent - No Cold Calling Zones (NCCZ)

Community Protection Cambridgeshire County Council

Charlotte Homent(CH) introduced herself as the Manager of the Community Protection section of Cambridgeshire County Council. The County Council established the team in April 2016 to work in parallel with Trading Standards.

The 144 existing NCCZs were set up by Trading Standards against specific criteria. However, once set up they received little or no support. The County has decided that existing schemes will be encouraged and supported through the appointment of a 'co-ordinator/champion who will support the scheme similar to NHW co-ordination. In areas where there are NHW schemes NHW co-ordinators are being invited to include them in their coverage. Where there are no NHW co-ordinators able to take on role new community members are being sought. This also presents opportunities to increase NHW coverage.

There will be no new NCCZs set up. From past experience, it is believed that community led action would be more effective. Consequently, volunteers are needed to deliver leaflets, stickers, posters, et cetera. So the Community Protection team need a volunteer for each named street on a list that is available. The volunteers should live in or close to the named streets and must have an email address. This community role would not be onerous.

Also, there will be a "Good Neighbour Scheme" for which there will be no threshold criteria. CH's team will provide posters but no street signs.

Comment: The advice that Neighbourhood Watch had received in Peterborough was that street signs and window stickers were counter-productive because the displays would attract villains.

Answer: That advice may be correct that the people within the zone will feel empowered and safer.

Here is the content from the key slides that Rebecca Tinsley presented.

Note the links provided for further information and for registering experiences of cybercrime.

Is Cybercrime really such a big problem?

- An estimated 2 million cybercrime offences were committed last year
- We are now living our lives increasingly online
- We are an affluent country with a generally poor cyber security culture
- We are more likely to take precautions offline than we are online
- This makes the UK an attractive target for cybercriminals

What is Social Engineering?

"When talking about online safety and security, 'social engineering' means the act of manipulating or tricking people into certain actions including divulging personal or financial information … a kind of confidence trick. Social engineering exploits human nature and often plays on victims' willingness to be helpful, or please others. It is a factor in many types of fraud."

Get Safe Online, January 2016

Examples of Social Engineering

- Fraudulent emails encouraging you to follow a link or open an attachment – (*Phishing*)
- Fraudulent phone call asking you to confirm details – (*Vishing*)
- Being advised to hand over payments cards etc. to a courier – (*Courier Fraud*)
- Fraudulent phone call requesting remote access (i.e. Microsoft Scam)
- USB/DVD left lying around or given to you which contains Malware – (*Baiting*)
- Fake social network profiles trying to be your friend
- Online Dating Scams – (*Romance Fraud*)

The Dangers of using public Wi-Fi:

- Wi-Fi may not always be secured
- If it isn't secured then it is most likely not encrypted
- Unencrypted wireless networks enable unauthorised people to intercept **anything** you are doing online
- This includes capturing your usernames and passwords

Latest advice from www.GetSafeOnline.org

- Unless you are using a secure web page (*beginning with* https:), do not send or receive private or financial information when using public Wi-Fi.
- Wherever possible, use well-known, commercial hotspot providers such as BT OpenZone or T-Mobile.
- Business people wishing to access their corporate network should use a secure, encrypted Virtual Private Network (VPN).

Cambridgeshire Fraud and Cyber Investigation Unit

Established late 2015 in response to Government making cyber crime a Tier 1 national threat

Team comprises:

- Cyber team investigating Cyber Dependent crime
- Fraud team investigating serious and complex fraud
- Cyber Security Advisor

How do I report Cyber Crime?

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

0300 123 2040

Urgent Incidents – 999 or 101 (local Force response)

Non urgent incidents – 101 / Action Fraud

Non urgent in office hours – Local Force Cyber Crime Unit

Always report any financial loss to your bank, card company or financial institution as well as the police.

So, how can we protect ourselves?

- Cultural Change
- Accept that it is "*When*" not "*If*"
- Cyber & Information Security is *not always about technology*
- 80% preventable with *very simple steps*
- Always consider the home life/work life blend of good practice

Three simple pieces of Advice

1. **Use strong passwords**
   A strong password is your first defence against hackers and cyber criminals
2. **Install security software**
   Security software such as anti-virus helps protect your devices from malware and hackers
3. **Download and install software updates**
   Software updates contain vital security upgrades that help keep your devices secure

Contact us:-

Rebecca Tinsley - Cyber Security Advisor - Cambridgeshire Constabulary
07738348544 rebecca.tinsley@cambs.pnn.police.uk

Fraud and Cyber Investigation Unit (FCIU)

cybercrime.mailbox@cambs.pnn.police.uk ecu@cambs.pnn.police.uk

How to Protect Yourself

Advice from Norwich & Peterborough Building Society

Be cautious if someone contacts you unexpectedly to confirm personal details. If you doubt that the call is genuine, then arrange to call number that you have independently obtained.

If possible, use a different phone and if this is not possible wait for several minutes before calling back. Alternatively, call a friend to ensure that the phone line has been disconnected from the original call.

Always remember that a building society or bank will never ask you for your PIN, whole security number, or password over the phone or via email.

Never pay fees or give your personal details or financial information in order to collect a prize or competition winnings that the caller states you have won.

Never hand over your card and PIN to a courier who is claiming to act on behalf of your building society, bank or card scheme provider.

Never let anyone use your account to deposit funds on behalf of a third party who is perhaps offering to pay you for your trouble. Often these funds are the proceeds of criminal activity and you could be held responsible for money-laundering.

Check your bank, pass books, and credit card statements regularly. If you see an entry is wrong tell your bank as soon as possible.

See the Norwich & Peterborough Building Society leaflet for more information or visit www.NandP.co.uk/Scams.

Remember

1. Treat all callers as bogus until you can be 100% certain that they are genuine.
2. Fraudsters are very plausible and are skilled in persuasion.
3. You cannot win a prize in a competition that you have not entered.
4. Only ever send money to a person who you know and can trust.
   Ensure that you know, for certain, that you are sending it to the tight person by a secure route. Mix validation methods, for example phone, Skype, Royal Mail, email, WhatsApp, etc.
5. Anything that appears too good to be true, almost certainly is.