A Parliament Street Policy Paper

POLICING AND CYBERCRIME

PARLIAMENT STREET

partnership in policy

Introduction

The UK has some of the finest police forces in the world. Policing is a dangerous job, with many officers regularly putting their personal safety and well-being at risk to keep our society safe and bring criminals to justice.

Whether its tackling knife crime, violent disorder, domestic abuse or complex criminal networks, in many ways as a society we fail to hold the men and women who police our streets with the respect and high regard they deserve.

One the biggest challenges with tackling crime is that the nature of it can change suddenly, without fair warning.

The internet has brought many wonderful things to Britain, bringing communities closer together but also opening a fresh avenue for a new way of crime. From cyberstalking, online fraud, identity theft to revenge pornography the horrors of online criminal activities are both concerning and horrifying.

Official data from the Office of National Statistics (ONS) has revealed that incidents involving computer misuse and malware against businesses have increased significantly.

The ONS also reported that there were 4.7 million incidents of fraud and computer misuse in the 12 months to September 2017, a 15% decrease from the previous year when measured against the latest crime figures for England and Wales.

"We can only properly protect UK cyberspace by working with others with the rest of government, with law enforcement, the Armed Forces, our international allies and, crucially, with business and wider society."

- Ciaran Martin, CEO, National Cyber Security Centre

Other reports have estimated that 17m were Britons targeted by phishing, ransomware, online fraud and hacking in 2017. In addition, security firm Norton estimated that £130bn was stolen from consumers last year.

Cybercrime is on the rise and will continue to pose a serious threat to UK businesses, consumers and critical national infrastructure. This in turn, places huge pressure on our Police forces to ensure that officers, staff, new recruits and trainees are fully prepared to handle increasingly complex investigations.

This report is designed to examine some of the preparations police forces are making to ensure officers are fully equipped to tackle the rising ride of cybercrime.

The report will provide detail on the individual allocation of financial resources, courses and the number of police staff underdoing training. It will also offer some recommendations for building a more cyber-savvy police recruitment programme.

Methodology

The Parliament Street research team issued Freedom of Information (FOI) requests to every Police force in the UK, the majority responded. Several were unable to provide specific data around training costs but could identify how many officers and staff had experienced the training programmes available.

It is important to note that the information disclosed in this report is for educational purposes only, to illustrate the preparations being made by individual forces. We also make it clear that these figures do not necessarily represent all resources allocated for cyber training, with many police training programmes overlapping.

For transparency, the exact wording submitted in the FOI requests to each police force has been included below.

1. We would like a breakdown of the total number of employees who have been through cybercrime training over the last three years 2017, 2016 and 2015

2. Estimated expenditure on cyber training/courses
- Please note employees refers to ALL staff (serving officers and non-operational)

Please note that ‘police forces’ includes British Transport Police and the Ministry of Defence police service.

Analysis of the data

Our research revealed that in terms of training budgets specially for cybercrime training, police forces have spent a total of £1,320,341 on 39,438 officers and staff in the last three years.

The highest level of spending was North Wales Police which told us they had spent £375,488 on training for officers and staff between 2015 and 2017. This included a dedicated five day 'Main Stream Cyber Training' course for 147 key staff, totaling £160,000. Other key spending included a two-day cyber train and trainer courses for four officers at a cost of £2,000

There was also a one-day cyber-crime input course for all new Initial Police Learning and Development Programme (IPLDP) recruits for 183 officers which cost £29,900. An additional £52,300 was spent on a similar course for 68 CID officers.

West Mercia and Warwickshire Police submitted a joint response, totally £125,633, followed by Lincolnshire which stated it had spent £119,834.

This was followed by West Midlands Police on £91,200 and Police Scotland on £83,121.

In terms of detail, Norfolk and Suffolk police forces provided information on their combined spend of £71,100. This included sending 3,882 staff on a Cyber Crime and Digital Policing First Responder (MCCT1/NCALT) course. 147 staff members were sent on a digital media investigator course costs £6,500. £15,000 was also spent on an open source level 2 course for 87 members of staff.

South Yorkshire Police sent 71 officers on its Sy-Mainstream Cyber Crime training programme. Other courses it offered included on entitled Sy/Hp-Cyber Hacking Inside The Minds Online Criminals.

Police Force	Training Budget	Staff Trained
North Wales Police	£375,488	1,043
West Mercia & Warwickshire	£125,633	263
Lincolnshire	£119,834	1,443
West Midlands	£91,200	413
Police Scotland	£83,121	97
British Transport Police	£77,500	250
Merseyside	£77,098	683
Leicestershire	£70,800	499
Norfolk and Suffolk	£70,100	12,540
Gwent	£45,420	302
West Yorkshire	£42,000	8,118
Cumbria	£40,000	260
Lancashire	£33,000	274
South Yorkshire	£25,475	78
Ministry of Defence Police	£21,000	14
The Port of Dover	0	0
Cheshire	N/A	2,979
City of London	N/A	448
Hampshire	N/A	290
Derbyshire	N/A	251
Gloucestershire	N/A	11
Greater Manchester	N/A	320
Northamptonshire	N/A	96
Northumbria	N/A	2,483
Staffordshire	N/A	2,244
Humberside	N/A	1,002
Surrey	N/A	1,434
Dorset	N/A	1,434
Dyfed-Powys Police	N/A	169

The Port of Dover, a small Policing group told us, “The Port of Dover Police have not had any Employees undertake cybercrime training over the specified time period or at all. There has therefore been no expenditure incurred.”

Conclusions and recommendations

Whilst occasionally police forces are working together to develop cyber crime training programmes, the clear majority are working alone in this process. Whilst we appreciate that individual forces have varying challenges in terms of crime, headcount and volume of citizens to protect, it would make sense to develop a more standardised approach to cybercrime strategy.

Our key recommendations for consideration include:

1. Establish a national police cyber strategy – this would enable security specialist companies to provide an agreed standard of training for all officers and staff across the country. It would also prevent variation of standards and skills between forces.

2. Increase recruitment of officers with existing cyber skills – work closely with schools, colleges, universities and private companies to ensure a pipeline of highly skilled workers are encouraged to join the police.

3. Sharing of key security training services – if a specific police force has developed a respected training course on cybercrime, it should be made available to other forces or replicated to share best practice.