NOVEMBER 2018

PARLIAMENT STREET

partnership in policy

HACK ATTACK:
POLICE UNDER PRESSURE

INTRODUCTION

The police forces in the UK work tirelessly to keep crime to a minimum and the public safe. Working nationally and regionally, police forces have a complicated job of ensuring national security is adhered to. With continuous cuts to the policing sector, ensuring public safety is becoming more of a demanding task.

As we move into a digitally led civilisation, new threats to national security and individuals are beginning to emerge. Cybercrime in particular is not a new threat to the 21st century but is certainly something that is becoming a bigger issue for police forces across the country.

Arguably, one of the largest and dangerous threats to emerge from the cybercrime age is hacking. In recent years, we have seen a multitude of hackers and viruses steal organisations and individuals' data to cause disruption, commit fraud and make money.

The most intrusive attack to hit the UK was the WannaCry virus which inflicted itself on the NHS in 2017, causing a multitude of issues to our health service including almost 20,000 appointments having to be cancelled and 600 computers at GP surgeries were locked.

Whilst this caused tremendous damage to health services, we are also seeing individual consumers become affected by organisations with poor security. More recently, this year Ticketmaster was found to have been subject to a hack which affected 40,000 customers who had bought tickets over a three-month period.

It is apparent that hacking and cybercrimes are certainly on the rise. Large and small businesses are a clear target, but also, individuals are becoming victim to these malicious crimes.

METHODOLOGY

Parliament Street's team of researchers issued Freedom of Information (FOI) requests on reported hacking crimes to all police forces in England in August 2018. Overall, a total of 14 forces responded to the request in full.

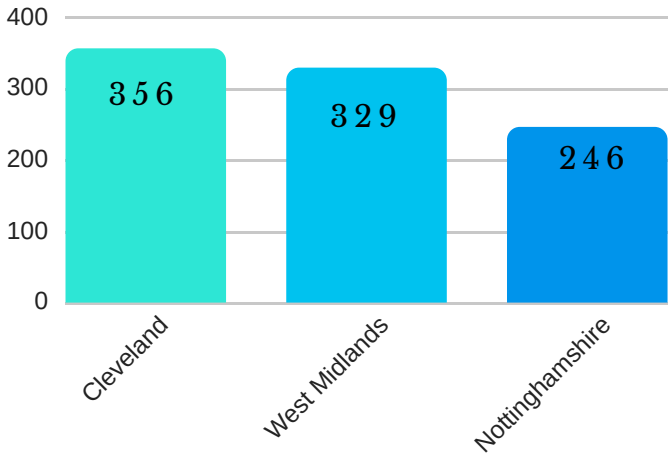
We asked for detail on the number of crimes which fall under the Computer Misuse act in the last two financial years which mention hacking, smart device or connected device.

We also asked to be provided with notes as to what these crimes were specifically.

The data has been collated and analysed to produce this report.

KEY FINDINGS OF RESEARCH

Incidents of hacking logged by UK Police forces in FY 17-18



19%

Increase in hacking in the West Midlands

2,547

Number of hacking crimes under investigation

From the results collated, it is clear that individuals are beginning to report crimes of hacking to their local police force, understanding that this is an issue that falls under their department.

Our research found that 2,547 crimes were reported over the course of financial years 2016/17 – 2017/18. For 2016/17, 1,193 hacking crimes were reported, compared to a jump to 1,354 crimes reported in 2017/18. Out of those who gave us a full breakdown of figures for the last two financial years, we found that there was an increase in hacking crimes of 14%.

The police force topping the list with the largest overall figure for the last financial year was Cleveland who reported a staggering total of 356 hacking crimes reported. Second to this was the West Midlands which reported 329 incidents, followed by Nottinghamshire which reported 246 cases of hacking.

The largest increase of reports between these two years was the West Midlands police force with an increase from 277 crimes reported to 329 – an increase of 19%. Second with the largest increase was Nottinghamshire with 204 reports in 2016/17, rising to 246 in 2017/18.

Despite the crimes increasing overall over the last two years, some police forces saw a decline in the reported figures. The largest decrease of crimes reported was the Metropolitan police force which disclosed 77 crimes in 2016/17, decreasing to 49 in the last financial year.

The second largest figure to drop was Cumbria police force which reported 79 in the last financial year, compared to 81 in the previous year. The decrease of hacking crimes reported could potentially be blamed on a lack of solutions for reporting the crimes or individuals taking the issues into their own hands.

KEY FINDINGS: POLICE NOTES

As well as official statistics, we also asked the various police forces for notes into what cybercrimes were reported.

From this, we saw a clear trend of malicious hacking into individual's social media accounts which led to the hacker posting content and messages under the user's profile.

An example of this is the Derbyshire police force who reported that in 2017, a hacker managed to get into someone's Facebook account and proceeded to steal photographs which were later distributed.

As well as this, Leicester police force reported that an unknown person hacked into a personal email account and posted photographs of emails through his girlfriend's post-box.

Although hacking personal accounts has been a clear trend from the notes, there were also many cases reported of business accounts and servers being subjected to hacking.

For example, Norfolk and Suffolk police force specifically referenced a crime whereby a virus was deployed into a businesses' server which had encrypted personal data files.

The virus would then demand a ransom of 1,087 bitcoins to remove it. Dorset police force also reported suspicious online behaviour with a business website being hacked, the suspect was believed to be identified but there was not enough evidence to prosecute.

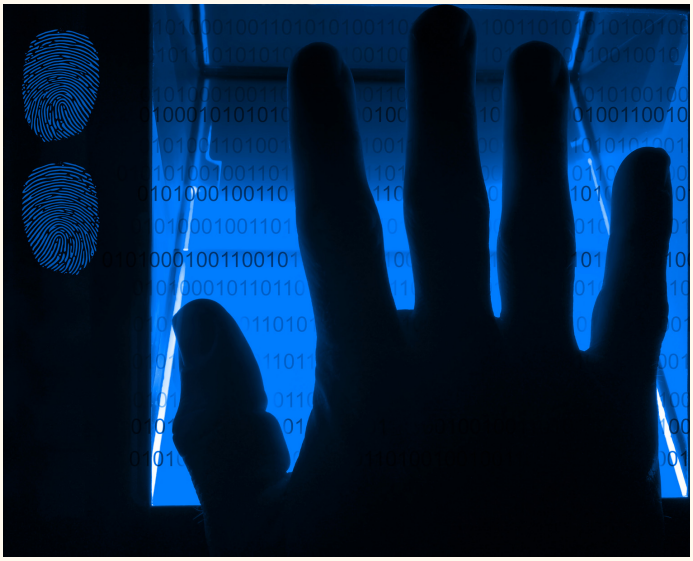
.

"Ex-partner has hacked into mobile account and sent indecent photos."
- Derbyshire

"Complainent states that offenders are setting up fake profiles which is affecting their business."
- Derbyshire

"Cyber Crime - Business Email Has Been Hacked."
- Dorset

"Hacking of company website."
- Leicestershire



RECOMMENDATIONS

OUR FINAL THOUGHTS

Whilst the rise of cybercrime is nothing new, the impact these incidents is having on police forces across the UK is significant in terms of resourcing. With high levels of violent crime and particularly knife crime taking place across the country, hacking investigations are diverting resources away from these incidents. It is therefore important that police forces have the necessary cyber skills available in-house to tackle these incidents.

Moving forward, we would recommend the following three policy steps to reduce time spent on cyber fraud and hacking investigations:

1.) Mandatory national cyber training for officers and staff
Ensuring all new entrants to police forces have been properly accredited with nationally recognised cyber standards. These courses could include flexible e-learning initiatives, workforces and collaboration with the National Cyber Security Centre (NCSC).

2.) Industry must provide more support for police forces
It is clear that social media sites and technology giants could and should do more to support police in tracking down perpetrators of hacking crimes. This should include offering more collaboration on initiatives, offering training for officers on how to navigate technology to identify evidence and capture the culprits.

3.) Increase recruitment of STEM qualified officers

It's time for police forces to dramatically increase the recruitment of highly qualified officers. As well as working closely with universities and training colleges, industry organisations should also offer placement years and consultancy to ensure that police forces are fully equipped to deal with this threat.