Battling the rise in cybercrime—looking at the latest cybercrime statistics

05/09/2016

Corporate Crime analysis: According to the latest figures from the ONS, there have been over 5.8 million 'cybercrime' offences in the 12 months to the end of March 2016. Matthew Richardson, barrister at Henderson Chambers, breaks down the figures and explains what the trends mean for lawyers and their clients.

Original news

Crime in England and Wales: year ending Mar 2016 Office for National Statistics, Statistical bulletin

What are the most significant statistics in terms of cybercrime in the latest figures? What do they tell us?

It is very important for us to distinguish between the two types of cybercrime that comprise the 5.8 million crime headline figure. Firstly there is genuine cybercrime—that is to say cyber dependent crime that cannot be committed without a computer—of which most offences are covered under the Computer Misuse Act 1990. Secondly, there is 'traditional' crime that is facilitated in cyberspace, cyber-enabled crime—these offenses are things like online fraud, cyber harassment, intellectual property crimes and revenge porn. These two types of cybercrime are revealed in the statistics but not explicitly.

Approximately two million crimes within the statistics are cyber dependent crime, the majority of which are virus related crimes accounting for 1.3 million crimes. The remainder of cyber dependent crimes are hacking related crimes accounting for about 0.65 million crimes.

The cyber-enabled crimes are largely comprised of various types of fraud, accounting for 3.8 million crimes. Additionally, there are smaller numbers of harassment, including new categories of offence such as malicious communications online, social media abuse and revenge porn, but alarmingly the numbers of these types of crime have nearly doubled since last year from 82,000 to 156,000.

There is strong suspicion, however, that these numbers are soft, as so much cybercrime goes undetected. There are two types of companies—those that have been hacked and those that don't know that they have been hacked.

Are there any particular types of online offences that appear to be becoming more common? What changes are we seeing in the types of online offences being committed? Is the law able to keep pace with these changes?

The types of fraud that are in vogue vary from month-to-month. Phishing, pharming and email spoofing are still universally popular types of online fraud. Phishing is masquerading as a trustworthy person or business electronically or even by phone to fraudulently acquire sensitive information, such as passwords and credit card details. Pharming occurs when a hacker redirects website traffic from a legitimate website to the hacker's fraudulent website. Email spoofing is similar to phishing but via email specifically, often from a hacked 'zombie' computer, giving the impression of genuine email correspondence from a known source.

As members of the public become more aware of these types of scams, they are becoming less effective and eventually will either become massively more sophisticated or be eradicated completely, like '419' fraud or as it is sometimes called 'Nigerian Prince' fraud. As a result criminals are becoming more creative, which has given rise to other new types of fraud, like 'ransom' fraud, in which data is encrypted or stolen by a hacker and ransomed back to the owner for money that must usually be paid in an untraceable cryptocurrency, like Bitcoin.

How are law enforcement and prosecuting authorities approaching online crime? Are they experiencing any challenges with doing so?

There is work to be done. Last year, it was reported that the government claimed that its massive investment in tackling cybercrime had resulted in an increase of 34% in cybercrime prosecutions. However, this only represents a jump from 45 to 61 prosecutions in real terms; an actual increase of just 0.003% in terms of the total number of reported cybercrimes. While there is no criticism to be made of the hard work undertaken by members of enforcement agencies and prosecuting authorities, the current resources dedicated to this area by central government are arguably inadequate (on the basis of these figures) to deal with the growth in criminality.

The main challenges to the enforcement agencies and prosecuting authorities are that criminals massively outpace them in resources and training. Some hacking collectives are state sponsored and can afford to pay hundreds of thousands of pounds to employ computational science PhDs, thus allowing them to defraud on a massive scale and focus solely on that task. This dwarfs the resources of the 'good guys' in the police, the National Crime Agency (NCA) and the Crime Prosecution Service (CPS), all of whom are paid a fraction of the money made by the criminals, while also managing a huge caseload. Likewise, there are very few officers and prosecutors with the specialist training to detect and understand the complicated issues involved with cybercrime. The lead-time to train such officers must be around three years, and although there is some forward planning in the government's cybercrime policy, it simply isn't enough. It is easy to see how cybercrime slips through the cracks in favour of other meatier crimes, which, happily, have been reducing nationwide, the survey reveals.

Add to this the jurisdictional problems, and enforcement and prosecution authorities are faced with a practically impossible task of making any meaningful contribution to the policing of cybercrime. There are strong incentives for diverting efforts away from enforcement to focus instead on providing better training, education and resources directly to the public to protect themselves from cybercrime.

What does all this mean for lawyers and their clients?

While cybercrime has the ability to effect vast swathes of the public, the chances of any individual being successfully prosecuted are still fairly low. So what can individuals and corporates do to protect themselves, to prevent cyberattacks or to mitigate damage caused by cybercrime?

Cyber insurance is a good idea, and although the market is relatively under developed, it still provides some level of protection for losses suffered from cybercrime. However, it is probably not possible to compensate for all losses suffered as a result of a hack. Consider the lesson of Target, the US retail giant that lost 10% of its stock value overnight as a result of a well-publicised customer data theft.

Therefore, the smartest move for a lawyer is to protect you and your clients with as much cyber security and training as possible, to minimise the risk of hacks and cyber frauds. Corporates and individuals alike can consider consulting cybersecurity experts or appointing specialist personnel. Prevention is key in this growing area. If corporates or individuals find that they have been a victim of cybercrime, they must report it both to raise awareness and protect individuals from onward attacks. If a cybercrime has taken place lawyers can advise on the way forward procedurally. If public prosecutors are unable to prosecute individual instances, it may be possible for individuals or corporates to bring private prosecution or civil proceedings against those responsible.

How do these statistics fit in with other developments in this area? Do you have any predictions for future developments?

It is likely that this problem will get worse before it gets better—consumers and businesses need to do more to protect themselves in terms of personal security and the government needs to increase its training and resourcing of enforcement and prosecuting agencies. Hopefully, these statistics will provide a greater incentive to the government and public as a whole to act faster. Unfortunately, the reality is often that until people are the victims of a cyberattack personally, it is unlikely that anyone will really do anything. The difficulty for those of us specialising in this field is that we know the reality is most people have probably already been hacked, and just don't know it.

Interviewed by Alex Heshmaty.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor

CLICK HERE FOR A FREE TRIAL OF LEXIS®PSL