Cybercrime & Security Update: Prosecutors confirm 702 hacking cases charged

Date : November 24, 2014

Cybercrime and security is a topic that is rarely out of the news and new EU rules on cyber security are making their way through the EU legislative pipeline. But what has the UK been doing about the fight against cybercrime, notably hacking?

The term “hacking” is a colloquial one and doesn’t exist under UK legislation by that name as such. Instead, the rather less prosaic notion of gaining unauthorised access to data in a system or a computer is used under the Computer Misuse Act 1990 (“the 1990 Act”). This concept essentially means access by a person who is not entitled to control access or does not have the consent of the person who is entitled to do so. It should also be noted that other “hacking” legal concepts also exist under other UK legislation, e.g. the criminal offence of knowingly or recklessly obtaining or disclosing personal data or information contained in personal data without the consent of a data controller under the UK Data Protection Act 1998.

The 1990 Act is a very early piece of UK cybercrime legislation. It was introduced partly in response to a particular case which demonstrated the difficulties of trying to prosecute hacking under UK forgery and counterfeiting legislation. It consists of four main offences, namely: unauthorised access to computer material; unauthorised access with intent to commit or facilitate the commission of further offences, e.g. fraud; unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer etc., e.g. practices such as denial of service attacks or distributing viruses; and, making, supplying or obtaining articles for use in the above-mentioned three other offences.

All of these offences are sanctioned by imprisonment or fines, e.g. unauthorised access to computer material attracts a penalty of up to 1 year in prison or a maximum fine of £5,000 (US $6,400) at the (lower) Magistrates’ Court level, and, up to 2 years in prison or an unlimited fine at the (higher) Crown Court level.

We thought it would be interesting to know how many computer misuse criminal prosecutions have actually been brought before the courts in the UK. We therefore made a request under the UK’s Freedom of Information Act 2000 to the Crown Prosecution Service (CPS), who bring prosecutions under the Computer Misuse Act 1990 in England & Wales (Scotland and Northern Ireland have different prosecution authorities).

The CPS provided information for the years 2008 to the first half of 2014 concerning offences charged and which reached a hearing in the Magistrates’ courts. Information on the final outcome or whether the charge was the final charge maintained is not provided, nor is it known if any matters went higher to the Crown Court.

The CPS confirmed that they had prosecuted all 4 offences. Unauthorised access to computer material is by far the most enforced offence with a total of 460 prosecutions over six and a half years. 2013 was a key year with a total of

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2021 Cordery. All rights reserved.

218 prosecutions for all 4 offences. Making, supplying or obtaining articles for use in the above-mentioned three other offences is the least prosecuted offence with mostly either 0 annual prosecutions or just 1 annual prosecution. The grand total of prosecutions for all offences over six and a half years is 702.

The number of prosecutions brought for unauthorised access to computer material is perhaps the most surprising statistic and would seem to indicate a higher rate than might have been expected, although, as indicated above, it is not known how many went all the way to a conviction.

As already mentioned, proposed new EU rules on cyber security are coming (they are currently before the EU Council, consisting of all the EU Member States) under which, in short: an EU-wide common level of network and information security ("NIS") will be set up; EU Member States will have to put in place a minimum level of national capabilities by, establishing NIS national competent authorities ("NCAs"), setting up Computer Emergency Response Teams ("CERTs"), and, adopting national NIS strategies and national NIS cooperation plans; NIS NCAs will have to exchange information and to cooperate to counter NIS threats and incidents.

Under these new rules, operators of critical infrastructure, e.g. energy, transport, banking, stock exchange, healthcare, key Internet enablers such as e-commerce platforms, social networks, etc., and, public administrations will in effect be required to assess the risks they face and to adopt appropriate and proportionate measures to ensure compliance. One key impact will be that companies will have to ensure they have suitable IT security mechanisms in place down the supply-chain. Further, these entities will also be required to report to NCAs about incidents with a significant impact on core services provided. The incident reporting obligation will also add to the growing number of breach/incident reporting including under the new proposals including the new EU Data Protection Regulation. Final agreement (between the EU Council and the European Parliament) and then entry into force of these rules is not expected until next year 2015 and EU Member States will then have 18 months to implement them into national law.
Andre Bywater is a lawyer with Cordery in London where his focus is on compliance issues.

André Bywater Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2021 Cordery. All rights reserved.