

## **E-Crime / Cybercrime**

### **Driver – Political, Economic, Social, Technology**

Related Drivers – Organised Crime, Recession, Counter Terrorism, Collection and Storage of Personal Information, Fraud, Data Mining, Information Sharing

#### **Background**

E-Crime, or cybercrime, is defined by the British police as the use of a computer network for crime.<sup>1</sup> The Council for Europe defines it as any criminal offence committed against or with the help of a computer.<sup>2</sup> Despite reference to computers and networks e-crime can encompass a whole raft of traditional crimes – such as identity theft, financial fraud, offences against a person, computer misuse and sexual offences. It is estimated though that 80% to 90% of e-crime is fraud related therefore creating overlap between the cross-cutting themes of Fraud and E-Crime / Cybercrime. Therefore this particular driver will focus the skills associated with detecting crimes related to computers and online activity.

#### ***Political Context***

In 2007, a report on e-crime by the Metropolitan Police Service (MPS), which deals with the majority of e-crime in the UK concluded that specialist e-crime units can no longer cope with all e-crime. The report, written by Detective inspector Charlie McMurdie, of the Metropolitan Police computer crime unit, concludes: "The ability of law enforcement to investigate all types of e-crime locally and globally must be 'mainstreamed' as an integral part of every investigation".<sup>3</sup>

It was announced in June 2009 that regional 'cybercrime' units are to be set up across the country through a national strategy which to date, has not been formally signed off by ministers and senior officials.<sup>4</sup> This strategy is the first stage in developing a more consistent approach to e-crime across UK police forces, increasing the skills and capacity for law enforcement officers to tackle such criminality and to mainstream e-crime into everyday policing and law enforcement activities.<sup>5</sup>

It is thought that the units will be based near the Association of Chief Police Officers' (ACPO's) counter-terrorism units in Manchester, West Yorkshire and West Midlands, as well as the MPS in London. The strategy plans were designed and will be headed by Deputy Assistant Commissioner in the Specialist Crime Directorate and lead of Metropolitan Police Central e-Crime Unit (PCeU) Janet Williams.

The move comes with the Government poised to launch a national cyber security centre to help to protect the UK from online attacks. The centre will advise Whitehall departments and companies on defending against hacking by foreign powers, organised criminals and terror groups. It will form the centre piece of the new national security strategy to be launched by Gordon Brown (ca July 2009).<sup>6</sup> The changes will see the Cabinet Office co-ordinating anti-cybercrime efforts across Government.

Some highlights of the new cybercrime initiatives include training all officers on how to respond to cyber crime complaints, co-ordination between investigators and specialists, and the development of new regional police squads that are specially trained to deal with cyber crimes. Efforts will also focus on creating relationships between the police and businesses that are often involved in online fraud, such as banks and other members of the finance industry.

In May 2009, US president Barack Obama said that fighting cybercrime is seen as a "national security priority", vowing to create a cyber security office in Washington.<sup>7</sup>

## **Economic Context**

The scale of e-crime is thought to be around £50 billion a year worldwide. President Obama recently cited an industry report that put losses to Americans from cybercrime at \$8 bn (£4.9bn) over the past two years.<sup>8</sup>

Statistics published by APACS, the UK payments association, showed for the six months to June 2008:

- Online banking fraud losses totaled £21.4m – a 185 per cent rise on the 2007 figure. Although this increase seems marked, it is in keeping with a gradual increase seen from the second half of last year, when online banking fraud losses increased to £15.1m (during July to December 2007). The increase is largely due to criminals targeting online banking customers through phishing and spyware scams - because the banks' own systems have proved difficult to attack.
- The number of recorded phishing attacks continues to increase, with more than 20,000 fraudulent phishing websites set up in the first half of 2008 – an increase of more than 180 per cent from the same period last year.<sup>9</sup>

Analysis of fraud trends during the first quarter of 2009 by CIFAS, the UK's fraud prevention service, show an increase in people being impersonated in the same period last year by 40%, as well as a rise in facility takeover frauds and false insurance claims.<sup>10</sup> The recession has been cited as reason for the increase in fraud. Pundits feel that the financial pressures created by the recession can serve as motivation for employees, customers and criminals to commit fraud.<sup>11,12</sup>

## **Social Context**

The impact and influence of the Internet over the past ten years has been immense. During that time, access to the Internet has grown enormously. In 1996, 3.4 million UK adults were online; by 2006 this had expanded to 28.5 million. The rise of this networked society has expanded the range of information available to individuals. However, the Internet has proven to be an influence on criminal, as well as legitimate activity.<sup>13</sup>

Recent research carried out by CIFAS, the UK's fraud prevention service, state that their members view online, staff and identity fraud as the highest priority threats during the current climate. In addition, consumer awareness of financial crime risks and how individuals may

be targeted by criminals does not appear to have kept pace with the change in criminal use of technology, and the 2008 FSA consumer survey shows that the level of consumer awareness of financial crime remains poor.<sup>14</sup>

Cyber security has become a large issue lately, as attacks are no longer targeted only at businesses or individuals. Three London hospitals and one police force have recently been attacked. Reports in 2007 said that hackers, believed to have come from China's People's Liberation Army, hit the network of the Foreign Office and other key departments. Chinese hackers were also thought to be responsible for shutting down the House of Commons computer system in 2006. Successful cyber attacks could bring down essential computer systems, including defence systems or allow foreign governments to access them.

Moreover, the nature of the Internet, and its relative anonymity enables individuals to behave in ways that they would consider to be unthinkable in the physical world. It has been suggested that the moral boundaries relating to technology are at odds with the moral standards of the physical world. In essence, the lack of tangibility in the technological realm suggests that the ethical considerations relating to personal property and privacy in the physical world do not apply in the electronic world. Moreover, computer misusers tend not to consider their actions as immoral. This lack of virtual moral consensus has been referred to as 'toxic disinhibition': arising from the very nature of the interaction of the individual with the technology.

## ***Technology Context***

E-Crime is notoriously difficult to detect and punish because of its sheer technical complexity and because unseen attackers can strike victims from hundreds or even thousands of miles away. Due to the nature of e-Crime, and its ability to evolve with technology, new threats are emerging with an alarming degree of regularity. E-criminals continually adapt their tactics as new defences are implemented by software and anti-virus vendors. As web-based technologies become increasingly diverse e-criminals will use these services to access and exploit victims and conceal their activities.<sup>15</sup>

The FSA Outlook paper indicates that criminals appear to be changing the way in which they commit financial crime, indicating an increasing sophistication as they require more complete data to commit such crimes. For example, CIFAS reports that 'current-address fraud' now surpasses instances of 'previous-address fraud' comprising two-thirds of all identity fraud cases filed by its members in the first quarter of 2008.<sup>12</sup>

Developments in the criminal use of technology allow easier and faster access to valuable personal data, providing an increased opportunity for committing e-crime. APACS reports that the number of phishing attacks and money mule advertisements continue to rise. The number of fraudulent phishing websites set up in the first half of 2008 increased by 180% and the number of money mule advertisements rose by 33% (when compared to the same period in 2007).<sup>16</sup>

The most significant e-crime activities take place within multi-skilled, 'virtual' criminal groups, whose structures are different to traditional organised crime groups. 'Virtual' criminal groups are often centred on an online meeting place, either a web forum or Internet Relay Chat

(IRC) channel. These groups often consist of 10 to 30 online identities, with different roles (e.g. spamming, compromising victim machines, trading compromised private data, etc.) divided within the group. Each group will typically have an inner circle of more technically advanced and/or experienced members who control access to the attack tools and are responsible for dividing up the work.

## **Legal Context**

Changes introduced as a result of the Fraud Act 2006, mean that as of 1 April 2007, victims of bank fraud must notify the financial institution directly rather than the police. The institution will then decide whether to report the details on to the police.

Therefore in straightforward low-value cases, the financial institution will generally make good the financial loss without the involvement of the 'traditional' law enforcement agencies.

'Identity theft' is not a criminal offence in itself, but could give rise to liability under the Fraud Act 2006, the Theft Act 1968 and the Computer Misuse Act 1990

The Computer Misuse Act 1990 encompasses both basic and aggravated hacking (where a system is accessed without authorisation with the intent to commit further offences) and the unauthorised modification of computer material, such as might happen as a result of a virus attack. Reporting and prosecution level are extremely low for instance it is estimated there were 144,500 cases of computer misuse during 2006 but an estimated 6 million viruses incidents took place with only 100 prosecuted.

The European Commission is planning to impose harsher penalties for people who use the internet to commit crimes. New rules could see jail sentences for cybercrimes increased to more than five years, from about one to three years at present.

In addition to stronger laws, the EU is looking to set up a pan-European reporting system where member states can contact each other quickly to notify one another of attacks. The Commission would also like to create a unified system that would allow EU countries to report cyber attacks and prosecutions. Also, the Commission is updating the Council Framework Decision on Attacks Against Information Systems, which came into force in 2005. The update is expected to be published at the end of 2009. EU countries are not bound by law to follow the decision, but in the past most have adopted its recommendations.

## **Potential Skills Needs**

**Analytical skills** – to visualize, articulate, and solve complex problems and concepts, and make decisions based on available information

**Collaborative working skills** – working effectively with colleagues and other law enforcement agencies

**Computer forensic skills** – analysis of information contained within and created with computer systems and computing devices, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved

**Cybercrime intelligence gathering skills** – to scan multiple data sources and follow leads regarding cybercrime

**Electronic evidence collection skills** – capture, seize, preserve, and record electronic evidence for the investigation of e-crime cases

**Financial intelligence analysis skills** – analyse financial transactions and other financial related criminal intelligence

**Financial investigation skills** –investigate complex financial transactions combined with an in depth knowledge and understanding of the current and relevant legislation relating to financial investigations

**Fraud investigation skills** – investigate cases of fraud with an in depth knowledge and understanding of the current and relevant legislation relating to fraud investigations

**Intelligence information sharing skills** between police forces, other intelligence and security agencies

**Inter-agency working skills** – to work effectively with two or more governmental agencies

**IT skills** – general awareness and understanding of current ICT environment and changing landscape

**Network investigation skills** – conducting investigations where part or all of the crime is conducted over, or against, networks

**Multi-agency working skills** – to work with other agencies to protect the UK

**Partnership working skills** – to work effectively with other agencies to a common goal and standards

<sup>1</sup> [http://news.bbc.co.uk/1/hi/english/static/in\\_depth/uk/2001/life\\_of\\_crime/cybercrime.stm](http://news.bbc.co.uk/1/hi/english/static/in_depth/uk/2001/life_of_crime/cybercrime.stm)

<sup>2</sup> Definition derived from the provisions of the Council of Europe Convention on Cybercrime (ETS No. 185) 8 November 2001.

<sup>3</sup> [The Independent Online, 24 January 2007, 'Police struggling to cope with rise of cyber-crime'](#).

<sup>4</sup> [The Times Online, 24 June 2009, 'Plans to crack down on online criminals with 'cybercrime' units'](#).

<sup>5</sup> [The Register Online, 24 June 2009, 'UK police chiefs mull regional cybercrime squads'](#).

<sup>6</sup> [FT.com Press Release, 23 June 2009, 'Police chiefs plan cyber crime squads'](#).

<sup>7</sup> [FT.com Press Release, 30 May 2009, 'Obama responds to cyber threat'](#).

<sup>8</sup> [FT.Com Press Release, 14 June 2009, 'EU plans tougher cybercrime laws'](#).

<sup>9</sup> [APACS Press Release, 25 September 2008, 'APACS announces latest fraud figures'](#)

<sup>10</sup> [CIFAS Press Release, 26 January 2009, 'Fraud Trends 2008: Fraud on the increase'](#)

<sup>11</sup> [CIFAS Press Release, 27 April 2009, 'Fraud trends and recession go hand in hand'](#).

<sup>12</sup> [Financial Services Authority \(2009\) \*Financial Risk Outlook 2009\*. London: Financial Service Authority.](#)

<sup>13</sup> [https://www.garlik.com/press/Garlik\\_UK\\_Cybercrime\\_Report.pdf](https://www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf)

<sup>14</sup> [CIFAS Press Release, October 2008, '\*CIFAS figures confirm that the UK's fraud landscape has changed\*'.](#)

<sup>15</sup> [Serious Organised Crime Agency \(2008\) \*The United Kingdom Threat Assessment of Serious Organised Crime 2008/09\*. London: Serious Organised Crime Agency.](#)

<sup>16</sup> [APACS Press Release, 1 October 2008, '\*APACS announces latest fraud figures\*'.](#)