



Short report and actions arising from EURIM-IPPR E-Crime study group meeting (and associated e-mails) on Reporting Issues, 14th September 2004, at 1200-1300, NHTCU

SUMMARY OF MAIN POINTS

1. Debate has moved on since this time last year but most of the underlying problems remain the same. Until recently many law enforcement agencies were reluctant to receive reports of crimes they had no hope of clearing up while few victims are willing to spend effort reporting for statistical purposes only, unless this provides a crime book number that can be used for an insurance claim. Recent moves towards "ethical reporting" to ensure that police have a full picture on crime in their "area" are intended to change this but the "area" in which an Internet enabled crime was committed may often be unclear.
2. Easy-to-use reporting systems are likely to be swamped with reports that they cannot handle unless these are received in a form suitable for automatic collation, analysis and data mining (e.g completion of web-forms or electronic files of structured submission from "trusted" sources which have already pre-validated the necessary information, e.g. Banks or ISPs on behalf of their customers).
3. The US National White Collar Crime Centre (NW3C) gives an example of the scale of problem in prospect while the UK Money Laundering Reporting systems is said to be a classic example of a reporting structure created without the necessary systems to support the automatic collation and analysis of information.
4. The IC3 (Internet Crime Complaint Centre) was set up as partnership between the FBI and the NW3C to "receive, develop and refer criminal complaints regarding the rapidly expanding arena of cybercrime. IC3 gives the victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory authorities at the federal, state and local level IC3 provides a central referral mechanism for complaints involving Internet related crimes." The ease of reporting electronically to IC3 where crimes are sorted manually has meant that 70 staff are needed to handle the volume - which includes a wide variety of incidents, including violent crime in progress, reported by those unable to contact local police by other means.
5. In the UK suspected money laundering is reported by fax because e-mail is "insecure". Reports are commonly photocopied from spreadsheets onto forms printed from ADOBE for faxing. Some organizations report any transaction that could possibly be money laundering (99.9 % of which are not) others report only those that they believe cannot be anything other than money laundering. One of the latter reports an average of one multi-million pound incident a month and says that none has been acknowledged, let alone investigated. The team handling the reports is said to be swamped with reports and unable to cope.
6. Internet Crime is location independent and much of that likely to be reported is matter for civil or regulatory action rather than criminal investigation. The need is therefore for a joint-law enforcement - industry process to automatically structure, acknowledge and re-route reports for the attention of the relevant service provider, regulator or law enforcement agency (local, national or overseas) as appropriate, at the same time as recording for intelligence and analysis purposes.
7. The Internet Crime Forum has looked at the concept of such a one-stop-shop, primarily to enable those manning help desks to identify to whom to pass enquires. Scaling up such a

service for live operation will, however, be neither cheap nor easy and will almost certainly lead to a transformation of crime reporting in general. The reporting operation should not therefore be treated as an add-on function to an existing organization with its own reporting agenda but as part of the phased development of a new structure for handling Internet related crime as a whole.

8. In that process it will be important to manage expectations on the part of all concerned, whether reporting crime, wanting analysis or intelligence or tasked to respond. It will also be necessary to handle those who will wish to refuse to accept that for which they believe (correctly or otherwise) they lack the resources to respond
9. There are a number of pilots and precedents which can be built on and. In the mean time, the best way of identifying the scale and nature of e-crime and its impact relative to conventional crime, is almost certainly via the British Crime Survey or an add-one to the NHTCU annual survey.
10. **Action:** the current discussion paper needs to be edited, revised and restructured to bring out the points above.