EU Forum steps up the fight against cybercrime

Report by Alan Pedersen

INTERNET CRIME HAS BECOME a $4.1 trillion global problem. But cracking down on criminals poses a threat to individuals' right to privacy and throws up some major financial issues for the communications industry. PL&B looks at how the new EU Forum on cybercrime is addressing the problem.

The increasing use of the Internet for terrorist purposes, crimes against children, vandalism and fraud, is forcing many governments to take a hard line against computer related crime. It is generally accepted that law enforcement agencies are currently at a disadvantage, and measures for tackling cybercrime are both ineffective and taking far too long. Whilst a criminal act can be perpetrated in just seconds, the criminal investigation that follows can take anything up to eighteen months.

Privacy groups and industry, however, have expressed fears that knee-jerk reactions to media hysteria could have serious repercussions on civil liberties and the financial stability of business. The Council of Europe's Cybercrime treaty, adopted in November 2001, has attracted a great deal of criticism for its lack of transparency, accountability, and democratic values, yet already over 30 countries have signed up to it.

URGENT NEED FOR BALANCE

Fortunately these concerns are now being addressed through the European Union's Cybercrime Forum, which held its first plenary session on November 27th 2001. The Forum was set up following a recommendation by the Commission in January 2001. Consisting of Internet Service Providers (ISPs) and telecom operators, law enforcement agencies, civil liberty and consumer groups, data protection authorities and other relevant parties, the aim of the Forum is to promote a balanced and effective approach to tackling internet crime. By improving communication, promoting best practice and codes of conduct, and through the sharing of knowledge, the Forum aims to ensure the right balance is struck between network security, law enforcement powers, and the protection of privacy and personal data.

> Today's new generation of Internet networks may be faster, more powerful and reliable, but it comes at the expense of monitoring and surveillance.

The EU Enterprise and Information Society Commissioner, Erkki Likannen, reinforced the importance of the Forum when addressing its November session. "I believe an open exchange between the various stakeholders," he said, "is vital to achieve an effective, coherent and balanced policy approach, and to assure confidence and trust among European citizens in the Information Society."

It is a sentiment echoed by the Article 29 Working Party, which expressed grave concerns that the Commission has placed too much emphasis on repressive measures whilst not looking far enough into creating effective preventative solutions. Although it recognises the importance of a safer information society, the Working Party argues that tackling crime should not "serve as an excuse to set up major citizen surveillance techniques without having given proper consideration to alternative strategies." Because of these concerns, the Working Party has welcomed the creation of the EU Forum on Cybercrime, seeing it as crucial in giving a voice to experts and relevant parties.

During last November's plenary session, Likannen outlined the range of issues that lie ahead for the forum. These will include discussions on a number of proposals put forward by the Commission, including framework decisions for combating child pornography and serious attacks against information systems. He also outlined the promotion of research and development into reducing the vulnerability of the Internet.

Although some major conflicts still exist between the parties present at the EU Forum, there was a consensus of opinion of a greater need for effective co-operation and communication between the various groups. The concept of sharing knowledge has already been discussed in a March 2001 statement by Swedish telecoms operator, Telia. It expressed the need for law enforcement agencies to understand the difficulties in combating crime in what is a rapidly and constantly evolving environment. Today's new generation of Internet networks may be faster, more powerful and reliable, but it comes at the expense of monitoring and surveillance. Whilst data on the old circuit-switched networks was relatively easy to trace, Telia argues that new technology has created ease of anonymity over the Internet.

Retention of data

The Forum's session concentrated on what is still the most contentious topic affecting the represented parties; the retention of data. Under the current EU Data Protection Directive, telecom operators are able to hold onto data only for specific purposes, such as billing. Any unnecessary data should either be destroyed or anonymised immediately. Law enforcement agencies can get access to this data on a case-by-case basis, but the evolution of the Internet is threatening their access to information. The emergence of flat-rate billing, where customers are charged a non-metered monthly fee, renders the need to retain data for billing purposes redundant.

If data is stored for short periods, law enforcement agencies stand little chance of accessing it on a case-by-case basis. The odds are that by the time they see a need for investigating an individual's internet use, the data will have already been destroyed.

During the session, Stefan Kronqvist, Head of Sweden's IT Crime Squad, illustrated his concerns by pointing to a successful case in which a paedophile was traced and then caught through accessing data held by a telecoms operator. "Without access to the traffic data," he said, "it would have been practically impossible to monitor and investigate this type of particularly serious crime."

ISPs present at the Forum indicated some willingness to retain data, albeit on a limited timescale (for example the three months recommended by the Article 29 Working Party), but they were deeply concerned over the financial implications that the retention of data will have on their business. The impact of storing all data traffic will lead to higher operational costs in terms of storage space, equipment, and personnel required for managing the data. Electronic Data Systems (EDS) added that further costs would be incurred if the information were needed for use in prosecutions. Technology such as time stamping, authentication capabilities, and data imaging may be required if the information is to be made admissible as evidence in court proceedings.

In statements made to the Forum, telecoms operators such as Spain's Telefonica and the Netherlands' KPN called for these costs to met by the public sector. EDS concurred, citing section 5.2 of the Commission's Communication on a *Safer Information Society...* which states: "Industry should not be confronted with measures that are unreasonably costly." Even Alexander Patijn, from the Netherlands' Ministry of Justice, conceded that "claims that the government pays the costs of retention can hardly be rebutted."

Harmonisation essential

Probably one of the most important points discussed - one that will act as a springboard for future discussions – was the need to harmonise regulation and codes of practice across Europe. MEP Charlotte Cederschiold, Vice-president of the Europe Parliament's Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, outlined the existing imbalances. She explained that whilst some member states currently reimburse ISPs for data retention, others do not. Standards and harmonisation, she added, are therefore "vital so as not to distort competition in the single market or create competitive disadvantage."

The idea of a harmonised approach is not just beneficial to business, but to all parties concerned. Telefonica believes that the creation of uniform standards for information requests will help law enforcement agencies by ensuring the "efficient and expeditious response to legal requirements."

Effective partnerships

The comments made during the Forum's session have revealed a number of conflicts and misconceptions that need to be addressed. Communications providers feel they are being pulled in two different directions. On the one hand, they are obliged to obey data protection directives, whilst at the same time they are asked to do the opposite by law enforcement agencies. Police forces too, rightly or wrongly, perceive communications providers to be obstructive when dealing with data access requests.

Legislation alone is unlikely to be sufficient in combating cybercrime. If the parties concerned are to be successful, they will have to place a stronger emphasis on working together in order to remove the barriers that exist.

i

The EU Cybercrime Forum has created a provisional website at www.cybercrime-forum.jrc.it/default. Comments and statements from the first plenary session have been posted on their noticeboard and the Forum will issue a full report at a later date. The new site also acts as a research tool for cybercrime related topics. Visitors can post their comments and opinions onto the site, and access the minutes of Forum meetings.

The Commission's Communication on "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime" can be found at www.europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html

The Article 29 Data Protection Working Party's response to the communication was published on November 5th. See www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm