EURIM Briefing No 34

April 2002

E-CRIME – A New Opportunity for Partnership

Introduction

Fear of e-crime is widespread but ill-defined. This fear is undermining the image of the UK (as well as of the Internet) as a good place for e-business and restraining growth in e-commerce. Ministers are being pushed into legislation to address perceived fears without providing the resources to enforce existing law or giving the private sector the frameworks it needs to protect itself.

While hacking, pornography and other Internet crimes may make headlines, real damage is being done by electronically assisted conventional crime. Such e-crime is rarely reported in the popular press, but a recent US survey estimated the global cost of e-crime to be about £1Tn annually. Lloyds of London estimated the global cost of the recent "I Love You" virus to be £10Bn. The UK economy will bear a significant share of this increasing burden.

If a supermarket is burned down, the police investigate and the Judge will be severe. If an e-business is similarly destroyed, the police rarely afford it the same attention and experience. If business collects the evidence, the Crown Prosecution Service will show considerable caution in pursuing the case and, if it does, the Judge may well give only a trivial sentence because nothing tangible was actually stolen.

There are few new e-crimes. It is essential to separate the crime from the method by which it is committed. Computers increase criminal productivity as effectively as commercial efficiency – and reduce the risk of being caught. Governments, individuals and industry of all types and sizes are equally vulnerable to attack from anywhere globally. Laws often prevent prosecution of familiar crimes if committed by electronic means. Ill-conceived legislation is being heavily promoted although it fails to address the real issues, such as electronically assisted fraud, impersonation and theft, while creating unrealistic demands on industry to support law enforcement in areas where the costs, responsibilities and liabilities have not been thought through. The most effective approaches to fighting e-crime will emerge from cooperation between law enforcement, industry and users around the world and need to include new legislative approaches (sharing the experience and capability of all stakeholders) and methods of prevention, deterrence and (where these fail) detection and sanction.

This Briefing outlines what needs to be done to make the UK the best and safest place to do business in the new electronic world.

The Way Forward

Any rush to create new primary legislation is likely to be counter-productive. There are initiatives and pockets of activity that address some issues, but they lack focus. Greater cooperation is needed between all stakeholders to develop a common strategic approach to e-crime, to create a coherent legal environment and to make better use of scarce resources.

Specific recommendations include:

1. The **Home Office** to co-ordinate constructive dialogue between all stakeholders; including industry (as suppliers and users), consumer groups, civil liberties groups, law enforcement agencies, local government and central government departments – developing an agreed national strategy.
2. The **Law Commission** to review existing UK legislation to establish what changes are needed as a matter of priority to ensure that e-crimes can be prosecuted effectively.
3. **EURIM** to facilitate discussion between stakeholders on how best to educate those in the criminal justice system, in industry (including users and suppliers, both large and small) and the consumer community on the need to take e-crime seriously, building on current initiatives.
4. The **National Hi-Tech Crime Unit** to build on work with industry to agree how to co-operate to make best use of skills and resources to combat e-crime.
5. The **Home Office** to encourage direct industry involvement in the development of global initiatives to fight e-crime (including those in G8, OECD, Council of Europe and EU).

What Do We Mean By E-Crime?

There is no simple definition of e-crime. People use different terms with different meanings – cybercrime, hi-tech crime, computer crime, Internet crime. For simplicity this Briefing will use the term e-crime, taken to mean any criminal activity that involves the use of computers or networks in its execution.

It is important to distinguish the criminal act from the means by which it is committed. Just as information technology can improve the productivity of industry, many criminal activities can exploit the particular benefits of computers and the Internet to affect more victims globally in a shorter time than was previously possible. The law should continue to define the criminal act independently of the methods used, and allow effective investigation and prosecution whatever methods are used. There are distinct categories of criminal activity that need to be taken into account:

- *Use of the technology to make existing crimes more efficient*. No new crimes are actually being committed, although current law may prevent the effective investigation and prosecution of crimes committed in such ways. An example is paedophilia, which is a crime. Using computers to create and/or store images, and the Internet to distribute them does not create a new crime, but the law may need amending to allow effective investigation and prosecution where evidence is available only in electronic form.
- *Use of the technology to enable new forms of existing crimes*. An example is unauthorised copying of information in electronic form. This is not theft, as the owner has not been deprived of it, and information has no intrinsic value. However, the trend towards smart card and similar technologies to identify people will accelerate the opportunities for identity theft (impersonation), which is already a major problem in the USA. Definitions of familiar crimes may need to be adapted to cover such situations.
- *Crimes that specifically attack the new technology*. Here new law can be required – and the Computer Misuse Act was a first attempt to address this issue. This needs updating urgently, for example to ensure effective prosecution of those initiating denial of service attacks that prevent legitimate access to information systems.

The same technology can also work to the advantage of law enforcement – for example the computer can act as witness to actions and events through audit trails. The technology can also enable law enforcement bodies to communicate and exchange information more efficiently.

Preventing/Fighting E-Crime Needs New Approaches

There is a perception that e-crime equates to fighting criminal activity on the Internet. In truth an increasing proportion of crime involves information technology in its broadest sense. Most companies, from the very largest to the smallest one-person operation, use computer-based business systems. Individuals use computers to pursue hobbies, for home finance, to purchase goods and services, for schoolwork, and many other purposes. As a result, any criminal investigation can require knowledge of how to investigate information on and to capture reliable evidence from computer systems, as well as evidence gained from use of Internet services such as email, newsgroups and access to web sites.

As a consequence, the ability to handle information systems must become part of the skills required of law enforcement generally – from the constable who knows what to do (and what not to do) when coming across a computer system to the investigating officer who knows when to call in expert assistance to handle complex technical aspects of an investigation. It is vital that the investigation and prosecution of e-crime is not seen as a specialist subject distinct from normal policing activities. The formation of the National Hi-Tech Crime Unit to provide common standards and practices and to provide expert back-up to local police forces is an excellent start, but it will only make a material difference if greater investment is made in the training of local police forces, the Criminal Prosecution Service and the Judiciary, building on current initiatives.

Given the constraints on the public purse, it is unrealistic to assume that law enforcement can be funded to meet all its obligations. Ways of sharing the burden for the investigation and prosecution of e-crime with industry are needed. Common practices and tools should be developed, and appropriate processes agreed, to allow industry to investigate possible crimes, involving law enforcement when prosecution is considered viable. This would build on the considerable investment already made in industry in investigative capabilities, and enable closer cooperation between industry and law enforcement in the prosecution of crime. Better mechanisms need to be developed to allow the sharing of intelligence between stakeholders on potential threats in a secure and confidential way without requiring investigation of possible criminal activities. All this will also need cultural changes.

The current crime reporting process does not record the method used, so there are no statistics showing how many crimes have been committed using computers or the Internet. Indeed, the whole criminal justice system needs adaptation if it is to support effective investigation and prosecution of crimes involving computers and networks, including the proper capture and collection of evidence in electronic form. All too often such criminal activities attract light sentences, or even avoid prosecution altogether as the Crown Prosecution Service and the Judiciary fail to recognise their damaging nature. This is exacerbated by a public perception, reinforced in the popular press, that e-crime does not cause direct damage or injury to those affected, so need not be taken seriously.

A key need is to encourage prevention of e-crime. This can only be achieved through multiple, parallel initiatives. It must start with appropriate education at all levels from primary school through secondary school to higher education and beyond. The need to be good "cyber-citizens" should become a natural part of the education process. The primary objective of computer and network security is to reduce risk, not to catch criminals. The IT industry itself also has a responsibility to provide products that are inherently secure and to develop business solutions that do not encourage their use for criminal activity. The protection facilities provided also need to be more apparent to customers if they are to trust their systems sufficiently to make significant e-commerce transactions.

Do We Really Need More Legislation?

There appears to be little requirement in the UK for totally new laws, but there are areas where existing legislation could usefully be modified to allow effective investigation and prosecution of existing crimes that exploit new technologies. For example, the Computer Misuse Act was developed before the advent of the Internet and needs updating urgently to cover types of crime against computer systems that were not around then. Similarly, the Police and Criminal Evidence Act may need updating to take account of e-crime. Definitions of some crimes need to be updated to reflect their form in the electronic world. New law needs careful drafting to ensure it really does address the intended objectives and can be implemented and enforced in the real world.

As an example, confusion has resulted from the failure to understand the distinction between "communications data" and the "content" of communications in the Internet world, and the extent to which business does not need to retain the former, coupled with failure to resolve conflicting definitions and obligations under the Regulation of Investigatory Powers Act, the rushed Anti-Terrorism, Crime and Security Act, the Data Protection Act, various Telecoms Acts and the Human Rights Act. Collectively, they fail to address many of the practical issues preventing law enforcement from working effectively in some areas while potentially imposing disproportionate costs and obligations on business. Steps need to be taken to resolve these confusions before yet more legislation is created.

There may, however, be areas where new crimes need to be defined extending existing law. For example, it is not possible under English law to defraud a machine. There are also examples where behaviour commonly perceived as criminal is not actually illegal in the UK, although it may be elsewhere. Processes need to be devised to cope with such situations internationally.

If not carefully considered, new law can also have unintended damaging effects. For example, some parts of industry - notably the banking and financial sectors - have developed expensive and sophisticated measures to protect their systems from attack, but have recently been concerned at proposals to introduce legislation for other purposes (for example, protection of intellectual property) that would make some of those protection measures illegal. The result would be business systems more vulnerable to attack. Ironically, recent proposals could even make illegal tools and products used in the day-to-day security management of systems and networks – such as network monitors, auditing systems and remote system management facilities. Care needs to be taken to ensure that legislation drawn up in good faith to address particular concerns is so constructed that it does not unintentionally prevent legitimate use elsewhere. Recent examples of legislation with such side effects include the Private Security Industry Act and the current review of Export Control Regulations.

The Demand On Resources

E-crime investigations tend to make greater demands on skills and resources than conventional criminal investigations – and there are few appropriately skilled people available in police forces. There is a lack of appropriately trained personnel across all parts of the criminal justice system that new training schemes now being developed could take years to rectify. This is aggravated by the lack of incentives for local police forces to invest in such training and the commercial demand for such skills makes it difficult for law enforcement agencies to retain such staff once trained. It will be difficult to fund the additional skilled resource needed within law enforcement to combat e-crime on top of existing obligations at a time when public expenditure is tightly controlled. Meanwhile, large commercial organisations, especially in sectors such as

financial services, have substantial investigative capability but it is focused primarily on protecting corporate assets (crime prevention) rather than supporting criminal prosecutions.

The need is for trusted means by which government, law enforcement and industry can share intelligence on e-crime, establish effective means of measuring the scale of e-crime, and create common training in the skills and processes necessary to combat e-crime. Ways need to be found for industry and law enforcement to work together, making best use of the total skills pool to investigate and prosecute e-crime in large organisations and economically in smaller companies, freeing up resource in law enforcement agencies to combat e-crime in society at large. This needs to be backed by incentives that encourage local police forces to invest in adequate e-crime expertise at all levels from prevention to investigation. Investment is also needed in general e-crime awareness and prevention programmes, backed by industry commitment to more secure products and business solutions.

What Needs To Be Done

It is imperative that action be taken now, before the growth in e-crime overwhelms our capability to combat it and it becomes a major drag on the growth of e-business. The nature of e-crime requires stakeholders to work together in new ways to consider new approaches to prevent, detect, investigate and prosecute crimes that involve information systems and networks. Each can afford to contribute only part of the total solution. More effective means of exchanging information are needed to combat e-crime so that industry can contribute its expertise on how the technology may be misused and exploited, while enabling law enforcement to operate more effectively and policy makers to create a workable legal environment. The objective to make the UK the best and safest place to do business electronically can only be achieved through a broad strategy supported by all stakeholders that includes wider issues of prevention and education as well as technical measures and legal sanctions. The current, often confrontational, consultation processes need to be replaced by more cooperative dialogues where solutions are developed in partnership with all stakeholders, building on bodies such as the Internet Crime Forum, with scarce resources trained, shared and deployed to best effect.

As part of this process, HMG must recognise the international dimension, and support appropriate international initiatives. Greater participation by key stakeholders, notably industry, in such activities must be encouraged. Currently much international activity in this area excludes all but government representatives, leading to proposals that are technically unsupportable or damaging to industry.

Specific actions that build on existing initiatives include:

- The **Home Office** to lead an open process for the development of a national strategy for combating e-crime (including prevention and education) that involves, and has the explicit support of all stakeholders. This should focus initially on developing a common understanding of the nature and extent of e-crime and coherent and proportionate strategies to prevent, detect, report, investigate, prosecute and sanction such crimes supported with adequate resources.
- The **Law Commission** to undertake an urgent review of existing legislation, identifying priority areas where legislation (such as the Computer Misuse Act) needs adapting to allow effective investigation and prosecution of e-crime and where new legislation is unavoidable.
- The **National Hi-Tech Crime Unit** to develop the case for appropriate levels of skill and resource in law enforcement agencies to enable the effective investigation and prosecution of e-crime, building on existing initiatives with industry to agree where that burden can best be shared to reduce the demand on public funding.
- The **Home Office**, in co-operation with other government departments (such as the DTI and e-Envoy's Office) and regulators (such as Oftel and the FSA), to set an example to the international community by involving all stakeholders, especially industry, in international activities on e-crime in the European Union, the Council of Europe, the G8, the OECD and elsewhere.

EURIM can best help by facilitating discussions between all stakeholders to agree the way forward on:

- Better ways of developing policy and legislation relating to e-crime.
- The scope of, and programmes for, education of those in the Criminal Justice System, across industry and in society at large on the significance of, and their own responsibilities relating to combating e-crime.