Cybercrime Essentials

1 February 2007

Table of Contents

1. Introduction 1
2. The Risks for FE & HE Institutions 1
3. Legislation - The Computer Misuse Act 1990 – what it says. 3
4. Fraud and Theft 3
5. Harmful Content – Pornography 4
6. Extreme Material 4
7. Sexual Offences involving the Internet, and 'grooming' 4
8. Intellectual Property Offences - Copyright Crime 4
9. Responsibilities for FE and HE institutions 5
10. Conclusion 5

1. Introduction

Computer crime may be classified into the following categories:

- Content related crime, for example, child pornography and criminal copyright infringement.
- Traditional crimes committed by means of a computer, for example, harassment, fraud and theft.
- Attacks on computers and computer systems, for example, hacking.

This sort of crime is also often referred to as cybercrime, e-crime or hi-tech crime.

Many of these crimes can be prosecuted within the existing criminal justice system as they would be if the offence were committed where no computer was involved. Others however are addressed directly under the Computer Misuse Act 1990 and this will be explored in some detail below.

2. The Risks for FE & HE Institutions

The prevalence of computer related crime means that FE and HE institutions are affected in many of the same ways as other businesses, organisations and individuals.

For institutions serious incidents might involve illegal materials in particular the viewing, possession, making and distribution of indecent images of children or serious stalking or harassment facilitated by communication technologies.

Where individual students or staff engage in illegal activity it is unlikely that the institution would be held liable except where it had actual knowledge of unlawful activity or unlawful materials (or its suspicions should have been raised) and it took no action to prevent it. Further information on such risks is available in the JISC Legal paper entitled "Legal Risks and Liabilities for IT Services in Further and Higher Education" by Christine Cooper on our website at - http://www.jisclegal.ac.uk/publications/legalRisks.htm. Although it is the offenders, as individuals, that would face criminal prosecution an institution could suffer reputational damage if it is not seen to be acting responsibly.

Discovery of illegal materials within an institution's computer network, whether pornographic in nature or racist in nature, is a serious situation and should always be reported to the police. Incident handling guidance is available on the UKERNA JANET website in a document entitled 'Dealing with Computer Crime – FACTSHEET - http://www.ja.net/services/publications/factsheets/index.html.

FE and HE Institutions must ensure that they have appropriate strategies in place for responding to crime which takes places by means of their computer systems.. 'Effective Incident Response - Guidance Notes' are available on the JANET website at - http://www.ja.net/services/publications/technical-guides/index.html

Security

In terms of external threats FE and HE institutions should adopt technology security appropriate to the current risk level. From an infrastructure perspective this involves well established practice:

- build it secure
- educate users to operate it securely
- and encourage high risk users to invest in matching preventative measures where appropriate

The UCISA Information Security Toolkit is intended to support UK Further and Higher Education Institutions in producing Information Security policies to address (and to demonstrate that they are addressing) threats to the confidentiality, integrity and availability of information systems for which they are responsible, and to help meet audit requirements. Details of the Toolkit can be found on the UCISA website at - http://www.ucisa.ac.uk/ist.

Separate detailed information on 'Inappropriate use of computers - the technical investigation process' is available on the JISC Legal website at - http://www.jisclegal.ac.uk/publications/Inappropriateuse.htm.

Hacking

Virtually all hacking activities are offences under the CMA 1990. Hacking can cause serious disruption to institutions who, in addition to suffering financially (e.g. through system downtime), have to deal with the security breach which may expose individual

users to further crime. It is also possible that such a breach of security could result in the unlawful disclosure of the personal data of individuals in breach of an institution's obligations under the Data Protection Act 1998.

Denial of Service attacks

Usually directed at the institution 'Denial of Service' (DoS) is the name given to attacks involving hackers preventing the normal flow of internet traffic to a web site or e-Business. Denial-of-Service attacks, where hackers overload networks with data in an effort to disable them, have risen 50%, a March 2006 security report says - http://news.bbc.co.uk/1/hi/technology/4787474.stm.

Assistance with handling 'Denial of Service' attacks can be found in 'Guidance Note' on 'Investigating a denial-of-service attack' on the UKERNA JANET website at - http://www.ja.net/services/publications/technical-guides/index.html

3. Legislation - The Computer Misuse Act 1990 – what it says.

The Computer Misuse Act 1990 (CMA) (and now amended by the Police And Justice Act 2006) was introduced primarily to deal with computer hacking. It contains three main offences to do with unauthorised acts relating to computers:

- Section 1 contains the basic 'hacking' offence of gaining unauthorised access to any program or data held in a computer.
- Section 2 makes it an offence to commit a Section 1 offence with a view to commit, or facilitate the commission of, a further offence.
- Section 3 contains the offence of doing any unauthorised act in relation to a computer with intent:

    - to impair the operation of any computer; or
    - to prevent or hinder access to any program or data held in any computer; or
    - to impair the operation of any such program or the reliability of such data;
    - to enable any of the things to be done.

    knowing that any modification intended to be caused is unauthorised. The intent need not be directed at any particular computer or any particular program or data.

Maximum sentences for these offences range from six months imprisonment and/or a £500 fine to ten years imprisonment and/or an unlimited fine.

4. Fraud and Theft

Computer-related fraud can be defined as private gain or benefit by:

- altering computer input in an unauthorised way;
- destroying, suppressing, or stealing output;
- making unapproved changes to stored information; or
- amending or misusing programs (excluding virus infections).

In addition to being crimes in terms of existing criminal legislation, such fraud and theft may also involve "unauthorised access" or "unauthorised modification" both of which are classified as crimes in the Computer Misuse Act 1990 as amended.

5. Harmful Content – Pornography

Unlawful content is usually material that may lead to civil disputes such as defamation and copyright infringements. Illegal content is usually material that is illegal to possess such as child pornography.

The problem of illegal, harmful, distasteful or offensive content on the computer systems or the internet is of course not restricted to pornography. However in the case of child pornography, which in its nature features the sexual abuse of children, the view is taken that the phenomenon is so offensive that possession as well as circulation of offending images should be criminalised. The Sexual Offences Act 2003 amended the criminal law in the UK so that possession or publication of 'indecent images' of children less than eighteen years of age is a criminal offence.

6. Extreme Material

A proposal to make illegal the possession of a limited range of extreme pornographic material featuring adults is currently being considered by the Home Office. The proposal is to create a new offence of simple possession of pornographic material which is graphic and sexually explicit and which contains actual scenes or realistic depictions of serious violence, bestiality or necrophilia. For further information on this proposal you can access the document "Consultation: On the possession of extreme pornographic material" – online at - news.bbc.co.uk/1/shared/bsp/hi/pdfs/30_08_05_porn_doc.pdf.

7. Sexual Offences involving the Internet, and 'grooming'

The Sexual Offences Act 2003 (applying in England and Wales and Northern Ireland) came into force on 1 May 2004 and has created an offence of meeting a child following sexual grooming. The Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005 delivers similar provisions for Scotland. It is now a crime for an individual to befriend a child on the internet or by other means and to meet or intend to meet the child with the intention of abusing them. The maximum sentence is ten years imprisonment. Any knowledge by an institution of such activity must be reported to the police right away.

8. Intellectual Property Offences - Copyright Crime

Copyright law provides for criminal sanction in certain situations. In the UK generally civil remedies provide compensation to wronged intellectual property rights holders and most of the copyright criminal offences, contained in s.107 of the Copyright, Designs and Patents Act 1998 (CDPA), are concerned with commercial activity. Further information on intellectual property crime, including counterfeiting and piracy, can be found on the Patent Office website at - http://www.patent.gov.uk/crime.htm.

9. Responsibilities for FE and HE institutions

Although it is unlikely that the same duty to protect users is required by FE and HE as that required in the school environment for children there remains the responsibility to ensure the health and safety of students and staff.

In addition FE and HE institutions have a right and sometimes a duty to ensure that their computer systems are not being used for inappropriate purposes. One such example is the obligation to prevent pornographic images of minors being stored on computer systems.

There is no general duty in UK law for institutions to actively monitor the information made available via or on their computer systems – to do so, in fact, increases the risk of liability in respect of any unlawful or illegal material which is there.

If for nothing more than preventing damage to reputation there is an obligation on FE and HE institutions to have in place appropriate security technology to ensure the confidentiality, integrity and availability of their computer systems. This requires ongoing sophisticated up to date infrastructure protection systems.

10. Conclusion

- The prevalence of computer related crime means that FE and HE institutions are affected in many of the same ways as other businesses, organisations and individuals.
- FE and HE institutions have a legal duty to provide a healthy and safe environment for students and staff. This duty extends to providing a non-threatening environment where students can study and be protected from harassment or criminal activity.
- From a legal standpoint the duty to ensure that computer systems are not being used for inappropriate purposes is optimally fulfilled by notice and take-down procedures rather than actively monitoring in general which is likely to draw increased liability upon the institution.
- There is increased acceptance that cybercrime should not be treated in isolation and that computers, as well as facilitating crime, can themselves become the target of criminal activity.
- Even with all the prevention policies and technological solutions in place, there may nonetheless be occasions when misuse of information technology and the internet occur.
- At the operations level, what is ‘acceptable use’ should be strictly enforced and a culture of legal use predominant. Many difficulties originating from within an institution can be confronted and avoided by ensuring that students and staff users adhere to strict conditions of use of IT facilities. It is, for example, the responsibility of each FE and HE institution to foster a culture of computer use which complies with the JANET ‘Acceptable Use’ guidelines.

John X Kelly
1 February 2007