



Romel Cabling ▾



Home

Home > My courses > Social And Professional Issues > 04 Aspect Of Computer Crime > Lesson Proper for Week 4

Lesson Proper for Week 4

ASPECTS OF COMPUTER CRIME

What is Computer Crime?

Computer crime can be broadly defined as a criminal act that has been committed using a computer (or computer-based hardware) as the principal tool. When most people talk about computer crime, they are usually referring to the fact that a computer has either been the object, subject, or instrument of a crime. As summarized in Figure 3.1, a further distinction can be made between crimes where the role of the computer is purely incidental, and those where the computer is an essential part of the crime. In the first category are computer-assisted crimes, many of which were committed long before the advent of computers. These include electronic versions of 'traditional' crimes, such as fraud, forgery, extortion and theft. In the latter category are crimes that could not have been committed without a computer and which require some degree of computer knowledge and expertise. This definition of computer crime is a narrower one, and includes 'new' cybercrimes which are specific to computers, such as hacking, virus attacks, and identity theft.

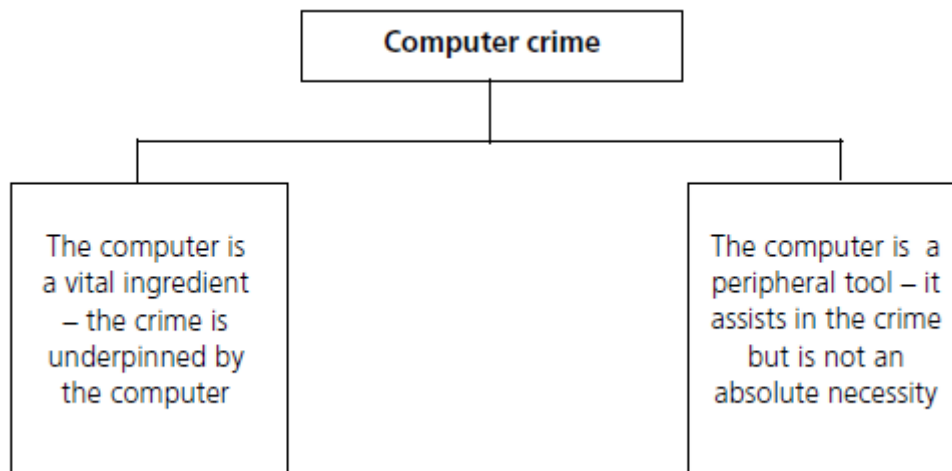


Figure 3.1: In terms of computer crime, a computer (or computer-based hardware) may facilitate the crime or may play a fundamental role.

Types of Computer Crime

The field of a computer crime is highly fluid – many new crimes, and new versions of more traditional crimes, are continually emerging. This section looks at some of the different types of computer crime. The areas we discuss are indicated in Figure 3.2.

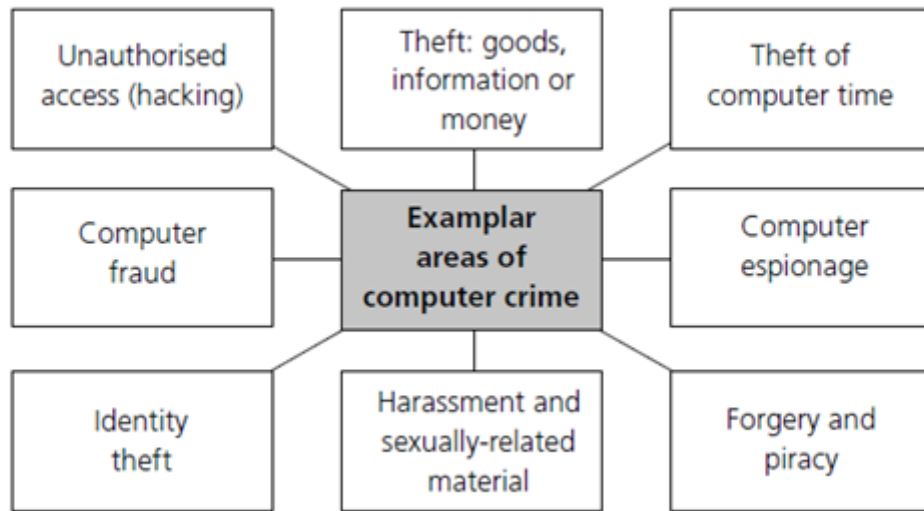


Figure 3.2: Examples of computer crime that are briefly described in the text.

Unauthorized Access

There are three main forms of ‘unauthorized access’ that constitute criminal offences under the Computer Misuse Act, 1990. These are:

- Unauthorized access to computer material
- Unauthorized access with intent to commit further offences (such as blackmail)
- Unauthorized modification of computer material (for example, distributing viruses).

In the previous lesson, we also looked at some of the techniques for gaining unauthorized access, such as Trojan horses, as well as other malicious and destructive programs, such as viruses and worms. Other techniques of gaining unauthorized access include ‘piggybacking’, which refers to tapping into communication lines, and ‘riding’ into a system, behind a legitimate user with a password.

Theft of Goods, Information or Money

Computer technology has enabled new kinds of theft, for example theft of goods (e.g. diverting goods to the wrong destination) and theft of information (e.g. unauthorized tapping into data transmission lines or databases). Commonly used techniques include data 'diddling', swapping one piece of data for another, so it is, for example, almost impossible to tell that funds have been stolen; and scavenging for stray data or garbage, for clues that might unlock the secrets of a system or information that might be used for criminal purposes.

Theft of money can take various forms, such as transferring payments to a bogus bank account. Embezzlement is one of the most common crimes, and refers to the fraudulent appropriation of funds by a person to whom those funds have been entrusted.

With the use of a computer, trusted employees can steal hundreds of thousands, and in some cases, millions of pounds from their employers. The victims are banks, brokerage houses, insurance companies and other large financial institutions. A common technique here is the 'salami', which involves theft of tiny sums of money from many thousands of accounts. For example, a bank clerk might shave a few pennies off many customers' bank accounts (like slices of salami) depositing them in their own account. The haul is thus spread over a large number of transactions and eventually accumulates as a large sum. For example, Forester and

Morrison [1990] describe the 'Flying Dutchman':

On Christmas Eve, 1987, a 26 year old clerk at Lloyds Bank in Amsterdam, Frans Noe, ordered that sums of \$8.4m and \$6.7m be transferred from the Lloyds branch in New York to an account he had opened with the Swiss Bank Corporation in Zurich. The young Dutchman then flew to Switzerland to collect the money. But owing to an unforeseen computer malfunction, the transfer failed to go through. Returning after Christmas, fellow employees saw the failed transaction on their screens and reported it. Noe was subsequently arrested and returned to Amsterdam. In May 1988 the "flying" Dutchman was jailed for 18 months for breaking into a computer system and his two accomplices received 12 months each.

Computer Fraud

Con artists and criminals of many sorts have found new opportunities on the Internet to cheat unsuspecting users. Some scams are almost unchanged from their pre-Internet forms – for example, pyramid schemes, chain letters, sales of counterfeit goods, and phoney business investment opportunities. Stock fraud is an area of criminal activity that has been adapted to the Internet. In one particular case, an employee of a US company called PairGain Technologies created a fake web page to look like the site of the Bloomberg financial news service. The site featured a positive but false announcement about PairGain. The employee also posted messages about the 'news', with a link to the fake site.

People copied and e-mailed the link, spreading the false information quickly, and causing PairGain stock to rise more than 30%. The perpetrator was traced and caught within a week. Another area of fraudulent activity has been web auction sites, like eBay, founded in 1995, and perhaps the largest and best-known online auction site. Approximately \$400 million of goods were sold on eBay in 2000. In one month in 2001, 24 million people visited the site. But problems soon arose. Some sellers did not send the items people paid for, or they sent inferior goods that

did not meet the online description. Dishonest sellers also engaged in 'shill bidding', that is, bidding on one's own goods to drive up the price. Some 'old' crimes, like extortion, have been given a new lease of life in the electronic environment. Len Hynds of the National Hi-Tech Crime Unit (discussed later) cites the example of hackers accessing companies' systems, for the purpose of downloading databases, then contacting their victims to offer security patches for their software in order to put things right again.

Corporate Espionage

Corporate computer systems contain a great deal of information of interest to competitors, including product development plans, customer contact lists, product specifications, manufacturing process knowledge, and strategic plans. Corporate espionage and theft is a rapidly growing area of computer crime which involves the theft of these corporate assets or trade secrets from competitors.

Identity Theft

One of the fastest-growing computer crimes is identity theft which involves not just the theft of credit card numbers, but also national insurance or social security numbers, bank account details, addresses and any other personal data that a person might use to verify their identity. This data can be pieced together to either form a fake identity or to impersonate someone by usurping their identity, whether for purposes of theft, fraud or other malicious activities. It has been suggested that identity theft is the fastest-growing white-collar crime in the UK, generating a criminal cash flow of £10 million a day. In 1999, there were 20,264 reported cases of identity theft in the UK; by 2002, that figure had reached 74,766, an increase of 50% from the year before. These figures accounted only for reported cases. It is estimated that approximately 80% of this type of fraud goes unrecognized, is kept quiet, or is written off as bad debt (*Guardian Weekend*, 25 Oct, 2003).

Forgery and Piracy

Computers have been employed to assist forgery, using desktop publishing software, high-resolution scanners and laser printers to produce counterfeit money, fake cheques, passports, visas, birth certificates, identity cards, degree certificates and corporate stationery, to name but a few examples. Software piracy is a major area of criminal activity, involving the distribution of illegal software and other intellectual products.

Harassment and Sexually Related Material

Computer technology, and the Internet specifically, have assisted a range of sexual crimes, from the distribution and consumption of child pornography via pedophile rings, to electronic forms of sexual harassment and cyber stalking (the use of e-mail and other electronic media to harass or threaten a person repeatedly).

Computer Criminals

There is a commonly held view that the typical computer criminal is something of a 'whizz kid', with highly developed computing skills and a compulsive desire to 'beat the system'. However, not many crimes demonstrate high technical ingenuity on the part of the perpetrator. Most exhibit an opportunistic exploitation of an inherent weakness in the computer system being used.

Early research into computer crime showed that the vast majority of crimes involving computers were carried out by employees or insiders from within an organization or business. These were invariably opportunist crimes perpetrated by managers, supervisors, clerks or cashiers who had little in the way of technical skills and were mostly first-time offenders (Hynds [2002]). This picture is changing, however, and the trend is away from insider crimes, towards crimes committed by outsiders – from external, remote, locations. This has been accompanied by a general rise in new types of 'high-tech' cybercrime committed by organized criminals, working across national borders.

The motives of computer criminals are many and varied, ranging from crimes committed as a means of easy financial gain, to those motivated by vengeance or grudges. As with hacking, some crimes are committed purely for the intellectual challenge. One of the attractions of computer crimes is that they involve very little physical risk, compared to crimes such as bank robbery. Most computer crimes can be committed anonymously, without having to confront the victims; this touches on the 'invisibility factor' of computing technology. Moreover, computer crimes can often appear not to be 'criminal' acts – shuffling numbers around in a remote and abstract way is not quite the same as handling huge piles of paper money. This partly explains why many perpetrators do not consider their crimes to be 'dishonest'.

A number of factors have contributed to the general increase in the amount of computer crime. Hynds argues that these include the availability of point and click interfaces that are much easier to use by the technically less competent, and the availability of software which can be easily downloaded from the Internet and used for criminal purposes. In addition, there has been a general increase in computer literacy in the wider population, and greater access to computer technology.

Computer crimes are increasingly carried out from remote locations, like Internet cafes, and from mobile sites, with the greater availability and power of laptop computers, personal digital assistants (PDAs) and mobile phones. This, and the fact that crimes are committed across national borders, increases problems of detection for law enforcement agencies. Computer crimes can also be committed alone, without talkative associates, thus further reducing the risk of detection.

Another factor that has contributed to computer crime is the fact that the Internet is above all a network and, as such, facilitates connections between like-minded people. On the Internet it is possible to inhabit a niche world populated solely by others whose experiences, values and beliefs are approximately the same as one's own. The benign aspect of this is the plethora of newsgroups, websites and chat rooms tailored to specific interests and hobbies, from 'hip-hop' to gardening. The malevolent side is that these technologies allow networking and communication among various kinds of criminals, from fraudsters to terrorists. This has, arguably, encouraged crimes such as pedophilia by facilitating the growth of networks of sex offenders which would be far more difficult to form in the physical world Hynds [2002].

Although it is generally agreed that computer crime is a large and growing problem, many experts believe that the amount of computer crime is much greater than is estimated. There are two main reasons for this:

- Firstly, many crimes go completely undetected and are often only discovered by accident. This is because computer crimes, by their nature, are very hard to detect – it is not always easy to know when someone has gained unauthorized access to a computer system. This is compounded by the problems of tracing and tracking down computer criminals because of the anonymous, remote and increasingly transnational nature of the crimes concerned.
- Secondly, many crimes go unreported. This is partly because there is often very little perceived benefit for the victim. The law is unlikely to be able to undo the damage caused, and the criminal is unlikely to be convicted. In addition, much staff time is likely to be tied up assembling evidence – even if it can be collected at all. More importantly, perhaps, wider knowledge of the crime is likely to harm the future prospects of the organization that has been the victim of the crime. Very few computer frauds, for example, are made public because companies, especially banks and other financial institutions, are loath to admit that their security systems are fallible. Such bad publicity makes them look less than competent. Publicity of this nature is disastrous for public relations and could lead to a major loss of customer confidence.

Combating Computer Crime: The Hi-Tech Crime Unit and the Serious Organized Crime Agency

To counteract the rapid growth in computer crime in the UK, the National Hi-Tech Crime Unit (NHTCU) was launched in April 2001 as a specialized agency within the National Crime Squad. Its brief was to combat serious and organized hi-tech crime both within the UK, and outside (in cases where crimes have an impact upon the UK).

Crimes targeted include software piracy, hacking and virus attacks, fraud, blackmail and extortion, online pedophilia, and identity theft. Although a relatively small unit, the NHTCU, within two years of being launched, had already accumulated over 3 terabytes of evidence (BBCi, 3 Oct, 2003). The NHTCU comprised four sections:

- **Investigations**, which gathered evidence and secures prosecutions
- **Intelligence**, which delivered tactical and strategic information
- **Tactical and technical support**, which acted in a consulting capacity alongside local law enforcement

- **Digital evidence recovery**, which undertook forensic work.

Note that the NHTCU was incorporated into the Serious Organized Crime Agency (SOCA) (www.soca.gov.uk) in 2006, as a part of a wide-ranging reform of policing activity.

Computers present new challenges for the detection and prosecution of computer crimes. To prove that a criminal act has been committed (for example, that a suspect has downloaded child porn images) requires the gathering and processing of new kinds of evidence. The field of collecting evidence from computers is called computer forensics. Computers seized from suspects act as a virtual crime scene. Computer forensics specialists retrieve evidence from the hard disks of such computers. Many offenders are unaware that Internet usage leaves footprints that can be traced, and that files, e-mails and images can be recovered even after they have been 'deleted'.


Seizure of computers, however, presents particular problems for both law enforcement and suspects because of a computer's multipurpose use. For a computer to be seized and removed from a suspect's premises, a warrant is required; but such warrants can only be granted to search for specific material on a computer. Investigators may suspect that a hard disk contains files of illegally obscene material, material that infringes copyrights, stolen credit card numbers or evidence of other crimes. The problem is that a computer also contains many legitimate, legal files, many of which belong to other people.

Crime detection work often involves the use of similar kinds of technologies to those used by hackers, in order to apprehend suspects. In France, 74 suspected pedophiles were apprehended using Internet technology and networking tools. Police managed to access a registry of 150,000 pedophile websites, a move that would be impossible to achieve in an offline context. Another strategy employed by security professionals and law enforcement agents is to set up 'honeypots', websites that look attractive to hackers, but are closely monitored so that everything a hacker does at the site is recorded and studied in order to trap suspects.



Navigation

Home

 Dashboard

Site pages

My courses

Capstone Project 1

Network Attacks: Detection, Analysis & Counter...

Ojt/Practicum 1

Social And Professional Issues

Participants

General

01 Law And Government


02 Overview Of Computer Ethics

03 Computer Hacking

04 Aspect Of Computer Crime

 Preliminary Activity for Week 4

 **Lesson Proper for Week 4**

 Analysis, Application, and Exploration for Week 4

 Generalization for Week 4

 Evaluation for Week 4

 Assignment for Week 4

System Integration And Architecture 2

Courses



Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for **free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.**

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.



Activities



Assignments



Forums



Quizzes



Resources

Bestlink College of the Philippines
College Department

Powered by [eLearning Commons](#)