COM6655 Professional Issues
Autumn 2022-23

Computer misuse and computer crime (part 1)

Professor Guy Brown
Department of Computer Science, University of Sheffield
g.j.brown@sheffield.ac.uk

Aims of this lecture

- To explain the scale and seriousness of computer crime
- To review different kinds of computer misuse
- To explain offences relating to computer fraud

Introduction

Context

- **IT has changed the way in which crimes are committed. Why?**

Context

- **IT has changed the way in which crimes are committed. Why?**
- Valuable assets are stored as computer data
- The Internet has broadened the geography of crime
- Computers have given rise to a new range of criminal activities such as computer hacking, viruses and ransomware

- **Yes, but is it really a big problem?**

Cyber crime – sources of UK data

- Data on computer crime was collected by the Audit Commission until April 2015, when it was replaced by a collection of other agencies.
  - http://webarchive.nationalarchives.gov.uk/20150421134146/http:/www.audit-commission.gov.uk/
- Now available from the Office for National Statistics
  - https://www.ons.gov.uk/
- Advice and guidance is available from the National Cyber Security Centre:
  - https://www.ncsc.gov.uk/section/about-ncsc/what-we-do
- Cyber crime is handled by the National Crime Agency:
  - https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

Cybersecurity breaches survey July 2022

- 39% of businesses and 30% of charities report a cyber security breach or attack in the last 12 months.
- Increasing prevalence of attacks on high-income charities.
- Most common attacks are:
  - Phishing (83%)
  - Impersonating organisation in emails or online (27%)
  - Virus, spyware, malware (12%)
  - Denial of service attacks (10%)
  - Hacking of online bank accounts (8%)
- https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

Computer misuse

What is computer misuse?

- In the late 1980s there was growing concern about hackers and the damage they could cause.
- Two studies:
  - Scottish Law Commission (reported 1987)
  - English Law Commission (reported 1989)
- The 1987 Scottish Law Commission report identified eight different categories of computer misuse.
- Prompted the **Computer Misuse Act 1990** (CMA).
- Computer misuse could also give rise to liabilities under civil law.

Reminder: basics of English criminal law

- Most criminal offences are set out in Acts of Parliament: e.g. Theft Act 1968, Fraud Act 2006, Computer Misuse Act 1990.
- Some common law criminal offences remain, e.g. murder.
- Elements of an offence can be analysed in terms of
  - **Mens rea** (mental element, intention)
  - **Actus reus** (actual behaviour)
- Some offences ('strict liability offences') do not involve mens rea
  - e.g. driving at night with faulty rear light is an offence even if the driver did not know the light was faulty.

Types of computer misuse (Scottish Law Commission, 1987)

- **(1) Erasure or falsification of data or programs to gain a financial or other advantage**
  - This category deals with fraud or theft
- **(2) Obtaining unauthorised access to a computer**
  - Hacking and unauthorised use of an employer's computer by an employee.
  - Hackers who damage computer systems often have no intention of doing so. Without mens rea, there is no crime.
  - This loophole has been addressed by the CMA.

Types of computer misuse (Scottish Law Commission, 1987)

- **(3) Eavesdropping on a computer**
  - This involves the use of equipment to pick up radiation emissions from a computer screen.
- **(4) Taking information without physical removal**
  - Legal problems arise here since 'information' is not a physical thing; it cannot be stolen.
  - Dealing with this problem would require changes to the law of theft; a major undertaking.
  - Copyright, patents and law of confidence offer some protection.

Types of computer misuse (Scottish Law Commission, 1987)

- **(5) Unauthorised borrowing of computer material**
  - Borrowing of computer media does not constitute theft.
- **(6) Denial of access to authorised users**
  - A user of a computer system could prejudice other users by denying them access to the computer or data, e.g., DDOS attacks, ransomware.
- **(7) Unauthorised use of computer time/facilities**
  - Authorised users of a computer could use them for unauthorised uses, such as private research and development which is competitive with their employer.
- **(8) Malicious or reckless corruption or erasure of data or programs**
  - Could cause financial loss, damage to the environment or loss of life.

Computer fraud

Computer Fraud

- Computer systems are often vulnerable to fraud.
- **R v Sunderland (unreported) 1983**
  - An employee of Barclays Bank used bank's computer to find a dormant account, forged the holder's signature to withdraw £2,100.
  - Sentenced to 2 years imprisonment, but illustrates vulnerability of such systems, especially from within an organisation.
- Developments in IT have made it easier to report fraud:
  - https://www.actionfraud.police.uk/report_fraud

Types of computer fraud (Audit Commission)

- Entry of an unauthorised instruction (**input fraud**)
  - Unauthorised alteration of data prior to it being input into a computer.
  - Probably common.
- Alteration of input data (**data fraud**)
  - Data held on a computer system is modified for fraudulent means.
- Suppression of data (**output fraud**)
  - Output from a computer system is destroyed or altered. The motive is usually to conceal criminal activity.
- **Program fraud**
  - Alteration of a computer program. Sophisticated, and therefore hard to detect
  - Example: salami fraud

Fraud offences

- Fraud is a collection of similar offences, some of which were covered by the Theft Acts 1968 and 1978.
- **Obtaining property by deception**
  - A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it, shall on conviction on indictment be liable to imprisonment for a term not exceeding ten years.
- **Q. is this offence applicable to computer crime?**

Two issues here

A person who by any deception dishonestly obtains property belonging **to another**, with the **intention of permanently depriving** the other of it, shall on conviction on indictment be liable to imprisonment for a term not exceeding ten years.

Implies deception of another person, not a computer

When data is taken, the owner is not permanently deprived of it

Oxford v Moss (1978)

- Student 'borrowed' an examination paper before the exam.
- Was prosecuted for theft of confidential information.
- But acquitted on grounds that information cannot be regarded as property and so cannot be stolen.
- The magistrate ruled that … "*confidence consisted in the right to control the publication of the exam and was a right over property rather than property in itself*." https://en.wikipedia.org/wiki/Oxford_v_Moss

R v. Lloyd, Bhuee & Ali (1985)

- Projectionist in a cinema and 2 others took films from cinema, and copied them but returned them.
- The pirated copies were sold at a considerable profit.
- Originally found guilt of conspiracy to steal …
  - … but overturned on appeal. No intention to permanently deprive.
- A conspiracy is an agreement between two or more persons to carry out an unlawful act.
- Conspiracy to defraud (common law) may be applicable to computer fraud, since deception need not be proven.

Accessing computer systems

- **Theft Act 1968**
  - Unauthorised access will result in some consumption of electricity
  - This could be regarded as theft
  - But will have to demonstrate that the person realised they were being dishonest
- **R v Ghosh (1982) Ghosh Test**
  - Need to determine whether the defendant himself realised that what he was doing was (by ordinary standards of reasonable and honest people) dishonest.

Attempts

- To be charged with an attempt, a person must have done an act which is *more than merely preparatory to the commission of an offence*.
- A computer fraud which is not completed may still be an attempt to steal money.
- Confusion over this argument is one reason why section two of the Computer Misuse Act 1990 was enacted (next lecture).
- Also addressed by Fraud Act 2006 (next section).

Fraud Act 2006

Fraud Act 2006

- Deals with deficiencies of Theft Acts 1968 and 1978, especially ICT fraud.
- A person is guilty of fraud if in breach of any of the following:
  - Fraud by false representation
  - Fraud by abuse of position
  - Fraud by failing to disclose information (e.g taxation, less relevant here)
- Penalties:
  - Summary conviction (Magistrates court): imprisonment for up to 12 months and/or fine
  - Conviction on indictment (Crown court trial by jury): imprisonment for up to 10 years and/or fine

Fraud by false representation

- **Fraud Act 2006, Section 2**
- Occurs when person dishonestly makes a false representation, intending to make a gain for himself or another, or to cause loss to another, or to expose another to risk of loss.
  - **Phishing** - obtaining information such as bank account details by sending email (or SMS) purporting to be from that person's bank
  - **Pharming** - redirecting traffic from genuine website to bogus one

Unlike Theft Act 1968 ("permanently deprive"), no need for actual gain or loss, or for it to be permanent.

Fraud by abuse of position

- **Fraud Act, Section 4**
- Applies when a person occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person.
- Examples:
  - Employee uses his position to make unauthorised copies of his employer's software to sell for his own benefit.
  - Employee sells an email containing confidential information belonging to the employer to a rival company.

Articles for use in fraud

- Section 6 of Fraud Act 2006: offence for a person to have in his possession any **article for use in connection with a fraud**.
  - Might include decryption software if intended to be used for fraud
  - Summary conviction: up to 12 months imprisonment and/or fine, on conviction in indictment: maximum penalty 5 years imprisonment
- Section 7 of Fraud Act 2006: offence if a person **makes, adapts, supplies, or offers to supply any article intending it to be used to commit fraud**
  - e.g. software to circumvent copy protection of copyright works ('crack').
  - Summary conviction: up to 12 months imprisonment and/or fine, on conviction in indictment: maximum penalty 10 years imprisonment

Obtaining services dishonestly

- Fraud Act 2006, Section 11: offence committed by person who obtains services for himself or another by dishonest act where:
  - the services are made available on the basis that payment has/will be made for them
  - he obtains them without any payment having been made for them, or without payment being made in full, and this is done with intent
- Maximum penalty on summary conviction, imprisonment not exceeding 12 months, and/or fine, on conviction on indictment, imprisonment not exceeding 5 years and/or fine.

Summary

- Computer crime is a serious and growing problem.
- In the UK, there is a much higher incidence of computer crime than is reported to the police.
- Computer misuse can take many different forms.
- Fraud is commonly linked to computer crime.
- The Fraud Act 2006 has fixed some issues with previous fraud legislation in terms of their application to computer crime.