Computer Misuse Act 1990

Anti-hacking legislation
Background

- No laws specifically to deal with computer crime prior to 1990
- Other laws tried instead
- Examples.
  - Cox v Riley 1986 (Criminal Damage Act 1971)
  - R. v Whitely 1990 (Criminal Damage Act 1971)
  - R. v Gold and Another ( Forgery and Counterfeiting Act 1981)
Background 2

- The case of *R. v Gold and Another* was highly publicised
- Defendant released on appeal
- Lead to Law Commission produced report
  - Report No.186, Computer Misuse
- Michael Colvin’s (MP) Private Member’s Bill
- This became the Computer Misuse Act 1990
Problems

• Original bill specifically aimed at hackers
• Many amendments during passage through parliament
• Eventual legislation very broad based, lost much of the original intent
Offences

- The Act specifies 3 offences
- In summary these are:-
  - Unauthorised Access
  - Unauthorised access with intent to commit another offence
  - Unauthorised modification of data
Penalties 1

- Unauthorised Access is called a *summary offence* and penalties are limited to
  - 6 months imprisonment
  and/or
  - a maximum fine of £5000
Penalties 2

• The other two offences
  – Unauthorised access with intent…
  – Unauthorised modification …

• Are more serious and carry jail terms of up to 5 years and unlimited fines
Examples 1

Scenario 1

• A student hacks into a college database to impress his friends - unauthorised access

• Later he decides to go in again, to alter his grades, but cannot find the correct file - unauthorised access with intent...

• A week later he succeeds and alters his grades - unauthorised modification of data
Examples 2

Scenario 2

• An employee who is about to made redundant finds the Managing Director’s password; logs into the computer system using this and looks at some confidential files - unauthorised access

• Having received his redundancy notice he goes back in to try and cause some damage but fails to do so - unauthorised access with intent...

• After asking a friend, he finds out how to delete files and wipes the main customer database - unauthorised modification
Problems

• While there has been a rise in hacking
  • more computers/Internet gives greater access

• Prosecution are rare and punishments small
  – Examples
    • Defendant causes firm to lose £36,000 - Fined £1,650; conditional discharge
    • Defendant destroys £30,000 worth of data - Fined £3000; 140 hours community service
Reasons

• Very complex
  • Offences difficult to prove
  • Evidence difficult to collect - firms do not co-operate with police
  • Firms embarrassed by hacking - particularly banks
  • Employees often simply sacked/demoted
  • Police lack expertise; time; money
  • Offence perceived as ‘soft crime’ no one injured/hurt
The Bedworth case

- This case in 1991 caused great concern and it was suggested that further prosecutions under the act would be unlikely to succeed
  - Defendant (and others) hacked into a variety of systems and caused damage
  - Defence stated that defendant ‘addicted to computers’ so could not help hacking
  - Not guilty verdict returned by jury
Current situation

- Hacking has increased both at hobby and professional levels
- A few high profile cases
- Offenders often in other countries with no equivalent legislation
- Some ‘international task forces’ set up but no real progress
- Current estimated costs of hacking - £5 billion per year world-wide
The End