Opportunity Makes a Thief

An Analysis of Computer Abuse

AUDIT COMMISSION
The Audit Commission

... promotes proper stewardship of public finances and helps those responsible for public services to achieve economy, efficiency and effectiveness.
1 The Survey

2 Action for Management

3 Appendices
Contents

Preface 3
Summary 4
Introduction 6
  The Audit Commission’s objectives 6

1. The Survey 7
   - What? – The Overall Results 8
     The extent of the problem 8
     Basic controls 11
     Monitoring procedures 11
   - How? – A Detailed Analysis of Incidents 13
     Computer fraud 13
     Other computer abuse 16

2. Action for Management 22
   A Prescription for Action 23
     Internal audit 23
     Who needs to take action? 24

3. Appendices 28
   - Appendix 1 29
     Computer abuse assessment checklist 29
   - Appendix 2 32
     Examples of incidents 33
   - Appendix 3 37
     Detailed analyses 38
Preface

This report is the fifth in a series of triennial surveys on the extent of computer fraud and abuse. It is the result of research carried out by the Audit Commission during the early part of 1994 and relating to the three years ending December 1993.

Over 5,500 questionnaires were distributed to organisations in the public and private sectors, including local authorities, health bodies, government departments, higher and further education and vocational training institutions, as well as a wide range of private sector organisations. The Accounts Commission for Scotland distributed questionnaires on the Audit Commission's behalf to local authorities in Scotland.

The wide range of organisations responding emphasises the value of comparative data. Past reports have received wide support from such organisations as the English Law Commission and the Department of Trade and Industry as well as research organisations and professional bodies. The English Law Commission referred to the surveys and used the Audit Commission's definition of computer fraud in its report which led to the Computer Misuse Act 1990.

The research was undertaken by Chris Hurford and Diane Skinner of the Audit Commission.

The research involved discussions with the Federation Against Software Theft (FAST), H M Treasury's Central Computer and Telecommunications Agency and assistance was also given by the Woolwich Centre for Computer Crime Research at Exeter University. The Commission is grateful to all those who responded to the survey and for the valuable information provided.

Responsibility for the analysis and report, however, rests with the Commission alone.

This report complements the previously published report on fraud and corruption in local government, Protecting the Public Purse, and current research by the Audit Commission into fraud and corruption in the National Health Service.
Summary

As organisations become more dependent upon information technology to support their business activities, there is increased opportunity to misuse those facilities for private gain. Computer crime embraces a range of incidents - fraud, virus infections, hacking, illicit software, theft of data and software, unauthorised private work, invasion of privacy and sabotage - and is becoming increasingly common.

Computer abuse is committed by people, not by technology. Understanding the technology is less important than recognising the importance of the application of fundamental control processes. If management is to respond to the threat of computer misuse, it needs to be well informed about the nature of the risks which organisations face. The Audit Commission undertakes its triennial surveys of computer fraud and abuse precisely to provide information about such risks.

This survey reveals computer abuse as a growth industry. It relies upon the first-hand experience of those who have suffered incidents of computer fraud and abuse. While the Audit Commission survey does not claim to provide a definitive list of computer fraud and abuse in the United Kingdom, it does indicate the risks when organisations depend on IT.

In the 1990 survey 1,537 respondents reported 180 incidents, whereas in 1993 1,073 organisations reported 537 incidents. The percentage which suffered incidents had increased from 12 per cent to 36 per cent. These figures could suggest an overall increase in computer abuse. Other trends include:

- an almost five-fold increase in reported virus infections;
- a 38 per cent increase in the number of reported frauds;
- unauthorised disclosure of personal data being reported for the first time;
- an almost eight-fold increase in the reported use of illicit software;
- a four-fold increase in reported instances of unauthorised private work; and
- a 183 per cent increase in the total value of reported incidents.

All financial systems may be subject to fraud. If the controls are weak, then opportunities may be found to break into the system and defraud the organisation. A decade ago the Audit Commission reported its first survey. It noted that the opportunity to commit computer abuse existed because of a lack of basic controls, rather than particularly sophisticated manipulation of procedures. Now, as then, opportunities are still widespread and weaknesses well-known, but for a variety of undisclosed reasons, management do not impose adequate controls.
Computer abuse is not limited to fraud. While fraud is the traditional risk posed by technology to the business community, an increasing range of other forms of computer abuse must be taken seriously by management. Ever expanding amounts of personal data are subject to exposure. Unauthorised disclosure of personal data researched for the first time in this survey as ‘Invasion of Privacy’ is growing. Organisations may not be making staff aware of their responsibility to use personal data wisely on a need-to-know basis.

The rise in the types of abuse associated with personal computers (PCs) is not surprising considering the rapid growth in PC usage. Widespread abuse is indicated by the dramatic increase in instances of computer viruses and the theft of software through the copying and use of unlicensed copies of programs. Furthermore, the casual attitude of so many towards unprotected and vulnerable business and personal information is quite alarming.

The survey has found that the primary reasons for computer abuse are:

- disregard for basic control safeguards;
- ineffective monitoring procedures; and
- ineffective internal audit.

Management can exercise better control over procedures inhibiting computer abuse.

To help management focus upon the key control areas the report includes a checklist which, when applied effectively, should minimise the risk of computer fraud and abuse. It is suggested that each organisation should identify a senior member of staff who, using the checklist, will be able to review the extent and nature of the risk. This would allow an action plan to be developed to minimise, as far as possible, the likelihood of computer abuse.
Introduction

1. Computer abuse is an umbrella term embracing various types of deliberate criminal acts, each of which calls for different skills and techniques in detection. The term embraces computer fraud, virus infections, hacking, theft of data and programs, sabotage, unauthorised private work, invasion of privacy and unauthorised use of illicit software.

2. As technology becomes more invasive, the risk of its misuse increases. Computer abuse is now well established. Thus, as the use of technology extends, the likelihood of deliberate acts of computer abuse will increase and the impact become much greater. While the tip of the iceberg may be identifiable, the greater and more significant impact may remain hidden.

3. Computer abuse is often carried out at a distance so that detection of the perpetrator is difficult. A hacker sitting in the comfort of his or her own home in the United Kingdom can tap into an organisation’s computer using telecommunication lines and access data in another continent. The reduction in the use of paper and increasing reliance upon electronic records means that some data exists only momentarily during a processing cycle and hard evidence of a particular transaction may be impossible to obtain. As a consequence, electronic audit trails appear confused and less detectable than those of traditional paper-based records. If auditors and managers cannot trace the processing cycle, they may well miss potential computer abuse.

4. Management often fails to understand the risks which computer abuse presents. Comprehending the finer points of data processing in a complex financial environment and the opportunities for diverting funds from one account to another is difficult enough for an experienced computer professional. It is scarcely surprising that senior management often fails to appreciate the risks which accompany the benefits of technology.

5. For management to respond to the threat of computer misuse, it needs to be well informed about the nature of the risks. Because of the absence of authoritative information, the Audit Commission undertakes triennial surveys of computer fraud and abuse with the primary purpose of analysing the nature of risks across all sectors and the likely impact on local government and the National Health Service in England and Wales. This provides valuable information for the Commission’s auditors in helping their audited bodies to minimise the risks of computer abuse.

6. This report analyses the results of the survey and suggests action which management should take to limit the risk of computer abuse.
What? - The Overall Results, illustrates the general scale of reported computer abuse based upon the Commission's survey.

Why? - The General Causes of Abuse, describes the overall reasons for incidents occurring.

How? - A Detailed Analysis of Incidents, details how the various types of incidents occurred.

1 The Survey
The extent of the problem

7. The Commission’s survey aims to assess the extent of computer abuse as defined in Box A. Questionnaires were distributed to all local authorities and NHS bodies in England, Wales and Scotland, to the majority of central government departments and agencies and to a cross section of other public sector organisations as well as a range of private sector organisations throughout the United Kingdom – 5,500 in all. Over 1,000 organisations responded and over 530 incidents of computer abuse were reported, with some organisations reporting multiple incidents over the three-year period ending December 1993. This is a healthy response to a voluntary survey.

8. The Commission’s audited bodies in local government and the NHS provided, not surprisingly, the highest number of responses - around 58 per cent of the total. The public sector was more willing to provide information - an overall 51 per cent response from the public sector (local government, health bodies, central government and higher/vocational education and training establishments) compared with around 10 per cent for private sector organisations.

9. While the Audit Commission survey does not purport to provide a definitive list of computer abuse incidents in the United Kingdom, the reported incidents do provide a valuable indication of the risks which organisations face when depending upon technology to support their business activities. Moreover, it is based on first-hand experience from those who have

<table>
<thead>
<tr>
<th>Box A</th>
<th>Computer abuse</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Definition of incidents</td>
</tr>
</tbody>
</table>
| Fraud | ◆ unauthorised input or alteration of input  
       | ◆ destruction/suppression/misappropriation of output from a computer process  
       | ◆ alteration of computerised data  
       | ◆ alteration or misuse of programs (but excluding virus infections) |
| Theft | ◆ of data  
      | ◆ of software |
| Use of illicit software | ◆ using unlicensed software |
| Using the computer for unauthorised private work | ◆ unauthorised use of the organisation’s computing facilities for private benefit |
| Invasion of privacy | ◆ unauthorised disclosure of data and breaches of data protection legislation |
| Hacking | ◆ deliberately gaining unauthorised access to a computer system usually through the use of telecommunication facilities |
| Sabotage | ◆ interfering with the computer process by causing deliberate damage to the processing cycle or to equipment |
actually suffered incidents of computer fraud and abuse rather than conjecture and estimates. The survey evidence confirms that computer abuse is a growth industry.

10. In 1990, 1,537 respondents reported 180 incidents whereas in 1993 1,073 organisations reported 537 incidents. The percentage which suffered incidents had increased from 12 per cent to 36 per cent. These figures could suggest an overall increase in computer abuse. Other trends include:

- an almost five-fold increase in reported virus infections;
- a 38 per cent increase in the number of reported frauds;
- unauthorised disclosure of personal data being reported for the first time;
- an almost eight-fold increase in the reported use of illicit software;
- a four-fold increase in reported instances of unauthorised private work; and
- a 183 per cent increase in the total value of reported incidents.

11. The over-riding conclusion from the analysis is that no sector is immune from computer misuse and the opportunity for fraud and other forms of abuse presents a very real threat (see Table 1, overleaf). The total value of reported incidents has risen by a significant 183 per cent since the last survey with an average financial loss for frauds per incident of £28,170. This, however, may not be a complete picture as the total loss from frauds is likely to be much higher. For some types of incident, the scale of direct loss will be more difficult to ascertain (invasion of privacy, for example) than for others (fraud and theft, for example).

---

**Exhibit 1**

Reported incidents of computer abuse

<table>
<thead>
<tr>
<th></th>
<th>1993</th>
<th>1990</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illicit software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private work</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invasion of privacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sabotage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacking</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There has been a three-fold increase in the number of incidents reported
Exhibit 2

Reported incidents since 1984

There have been significant increases in the number of reported incidents over the decade.

Note

Theft includes theft of programs and data, illicit software and unauthorised private work; hacking includes sabotage and invasion of privacy.

Table 1

Incidents by type of organisation

No sector has been immune from computer abuse.

<table>
<thead>
<tr>
<th>Type of Organisation</th>
<th>Total responses</th>
<th>Total incidents</th>
<th>Fraud</th>
<th>Virus</th>
<th>Illicit software</th>
<th>Private work</th>
<th>Theft of software/data</th>
<th>Invasion of privacy</th>
<th>Sabotage of privacy</th>
<th>Hacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local government</td>
<td>290</td>
<td>193</td>
<td>63</td>
<td>85</td>
<td>13</td>
<td>17</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Health</td>
<td>334</td>
<td>127</td>
<td>11</td>
<td>69</td>
<td>23</td>
<td>7</td>
<td>7</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Government</td>
<td>24</td>
<td>66</td>
<td>21</td>
<td>40</td>
<td>2</td>
<td></td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td>87</td>
<td>33</td>
<td>11</td>
<td>7</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Finance</td>
<td>58</td>
<td>27</td>
<td>4</td>
<td>17</td>
<td>2</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td>125</td>
<td>27</td>
<td>2</td>
<td>10</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Other commercial organisations</td>
<td>155</td>
<td>64</td>
<td>7</td>
<td>29</td>
<td>4</td>
<td>7</td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1073</td>
<td>537</td>
<td>108</td>
<td>261</td>
<td>54</td>
<td>36</td>
<td>31</td>
<td>16</td>
<td>16</td>
<td>15</td>
</tr>
</tbody>
</table>

Direct losses £

3,196,720 2,904,430 30,485 0 9,530 186,775 0 65,500 0

Indirect losses £

625,493 137,888 224,440 149,850 13,070 35,500 9,400 39,125 16,220

Total losses £

3,822,213 3,042,318 254,925 149,850 22,600 222,275 9,400 104,625 16,220

Note: Direct losses relate to organisation's funds while indirect losses refer to associated labour and other costs of recovering from the situation or prosecuting the perpetrator.
Why? – The General Causes of Abuse

12. The key reasons for computer abuse incidents occurring were:
   ◆ disregard for basic control safeguards; and
   ◆ ineffective monitoring procedures.

Basic controls

13. All of the reasons cited for computer fraud and abuse could be found in any textbook on control mechanisms and a lack of basic controls caused most incidents (see Table 2). There are rarely sophisticated reasons for such breakdowns in controls – just a basic failure to install and maintain sound well-known procedures.

Monitoring procedures

14. A key finding in the last survey was that internal control accounted for the detection of only 23 per cent of incidents. While the situation has improved, with half the frauds being detected through the normal control mechanisms, there is no room for complacency. As Table 3 shows, around 50 per cent of all incidents were detected by pure chance – typically as a consequence of information being received or a customer raising a query.

15. Poor internal control mechanisms result in increased opportunities for computer abuse and the survey has illustrated how perpetrators have taken advantage of such situations. In the 1990 survey, most frauds were committed...

Table 2
Most common reasons for incidents

<table>
<thead>
<tr>
<th></th>
<th>Fraud</th>
<th>Viruses</th>
<th>Illicit software</th>
<th>Hacking</th>
<th>Theft</th>
<th>Private work</th>
<th>Invasion of privacy</th>
<th>Sabotage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inadequate division of duties</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Passwords not changed</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Inadequate control over programs and data</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Poor management trails</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Poor reconciliation procedures</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Output not verified</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Poor controls over exception reports</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Poor access control</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Inadequate virus protection software</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Computer activities not traceable</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>No effective sanctions</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
by those occupying supervisory and managerial positions. As Table 4 shows, the pattern has now changed with administrative staff responsible for 60 per cent of frauds. Nevertheless, supervisory and managerial staff still commit a quarter of all incidents. Where frauds have lasted over three years, two-thirds of the perpetrators were supervisors and had been in the organisation for four years or more.

16. As organisations become leaner and fitter using technology to reduce layers of management, they run the risk of removing the controls and checks which former supervisory and managerial positions would have applied. A key cause of fraud and abuse in this survey and in previous research was poor division of duties – an increasing trend to reduce control mechanisms for the sake of expediency.

17. Respondents were asked to indicate how their organisations dealt with perpetrators of computer fraud and abuse. Over 70 provided information, and around 20 per cent of perpetrators were prosecuted. Other countries have been shown to take a harder line on computer abuse. In a report of a case in China, an accountant who embezzled over £122,000 from the Agricultural Bank of China was executed as a warning to potential fraudsters!

<table>
<thead>
<tr>
<th>Table 3</th>
<th>Detection results</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Most abuse was detected by pure chance</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>per cent</td>
</tr>
<tr>
<td>Internal control</td>
<td>37</td>
</tr>
<tr>
<td>Audit</td>
<td>9</td>
</tr>
<tr>
<td>Security staff/police</td>
<td>2</td>
</tr>
<tr>
<td>Accidental means</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

‘Opportunity makes a thief’
Francis Bacon’s Letter to the Earl of Essex 1598

<table>
<thead>
<tr>
<th>Table 4</th>
<th>Perpetrators of incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>60 per cent of incidents were perpetrated by administrative staff</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>per cent</td>
</tr>
<tr>
<td>Management</td>
<td>25</td>
</tr>
<tr>
<td>Administration</td>
<td>60</td>
</tr>
<tr>
<td>External</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

‘Opportunity makes a thief’
Francis Bacon’s Letter to the Earl of Essex 1598
How? - A Detailed Analysis of Incidents

18. Organisations are at risk from different types of computer abuse and it is important to understand their particular attributes so that appropriate protective measures can be taken. This chapter looks in more detail at the different types of abuse reported in the 1993 survey.

Computer fraud

19. Computer fraud is defined as any fraudulent behaviour connected with computerisation by which someone intends to gain dishonest advantage. The pattern of such reported frauds has been consistent over the past decade, as illustrated in Exhibit 3. The inputting of fraudulent data into a computer system is still the most common means of defrauding an organisation and, taken along with the unauthorised amendment of computerised data, represents 88 per cent of all computer fraud. Clerical staff are well placed to manipulate systems as they are more likely to be aware of the absence of checking mechanisms which could prevent or detect the abuse.

Financial systems at risk

20. All financial systems are prone to fraud and no particular system is immune (See Table 5, overleaf). While each organisation will have systems which present particular risks, the surveys have shown that certain systems attract greater attention from fraudsters.
Claims/Allowances systems

21. On-line systems which provide the opportunity to create records and then generate payments to the claimant are clearly open to misuse if there are insufficient controls over the activities of the terminal operator. This type of system attracted the largest number of reported frauds and reflects the increased dependence upon IT to manage the payment of allowances and claims. With an increasing number of claimants and pressure to respond to claims quickly, it is not surprising that such systems pose real threats. Over £1.2 million was lost through frauds perpetrated on claims and allowances systems with an average loss of around £43,000 per incident.

A clerk in a benefits payments section, who had been in the post for five years, created fictitious claimants records and directed the benefit to be paid into a private bank account in her own name. The eventual loss was £55,626 over a four year period and she was dismissed and prosecuted. Poor division of duties, insufficient tests on the reasonableness of benefits paid and the lack of any rotation of jobs or the compulsory taking of holidays were all cited as the reasons for the fraud being allowed to occur.

Sales/Debtors systems

22. There were twice as many reported cases involving Sales/Debtors systems as in the last survey, with an average loss of a little under £7,000 per incident. These typically involved misusing the computer process by:

- suppressing information which then delayed or prevented collection of a debt (often for the benefit of colleagues or family);
- reducing the amount of the debt due;
- switching funds from dormant accounts;
- delaying or inhibiting the creation of a debtor’s record.

The perpetrator, a temporary employee, accessed both her own and her husband’s personal debtors’ accounts and amended the debts due to reduce...
them. She used a colleague’s workstation which had been left ‘open’ so that the transaction appeared to have been processed by the colleague. The workstations were left ‘open’ because of the lengthy process of logging off and logging back on. The process has now been changed so that the screen clears at the touch of a key and the entry of a password allows the screen display to re-appear.

Cash Collection systems

23. The manipulation of the mechanical process of issuing receipts and dealing with cash adjustments provides the opportunity to retain cash and suppress any record of this activity within the system. Much depends upon management’s checking mechanisms to validate the accuracy of documentation and there were reported cases where control had broken down.

Purchases/Creditors systems

24. In comparison with the earlier survey, the overall number of reported incidents involving Purchases/Creditors systems halved but the overall losses from such incidents remained much the same, with an average loss of almost £50,000. The ease of access to such systems facilitates defrauding an organisation of large sums of money.

25. On-line systems being the norm, the most usual security mechanism to restrict access is the password. This, however, is prone to misuse where there is insufficient control over the user and where the effectiveness of the password relies wholly upon the user devising, changing and protecting the key. The evidence suggests that knowledge of the clerical processes surrounding the computer system rather than detailed technical knowledge of the programming tasks was the key element in effecting a fraud.

Stock systems

26. Where stock systems are computerised, then opportunity exists to defraud the organisation of physical assets rather than cash. Average losses were £48,000 per incident and involved using the computerised system to disguise the theft of goods by altering key system information such as balances, adjustments and valuations.

Payroll systems

27. Payroll frauds are traditionally seen as a lucrative area for fraud. Inflating an individual’s monthly pay, adding ‘ghost’ employees to the payroll, reactivating former employees’ records, all provide opportunities to defraud the organisation. Where staff are located in outposts and the local supervisor has responsibility for notifying head office of starters, leavers and amendments to the system, then, without adequate management oversight, there are particular risks of computer misuse. Although the number of reported cases was similar to those reported in previous surveys, the value of the losses was 22 per cent higher with an average loss of £10,000.

‘Fraud is infinite in variety; sometimes it is audacious and unblushing; sometimes it pays a sort of homage to virtue, and then it is modest and retiring; it would be honesty itself if it could only afford it. But fraud is fraud all the same.’

Lord Macnaghten in Reddaway v Banham 1896
Invasion of privacy

28. Invasion of privacy is defined as the unauthorised disclosure of personal data and has long been seen as a real issue. In an effort to combat the problem in the United Kingdom the Data Protection Act was passed in 1984.

29. While publicity has been given to some instances of abuse of personal data and some organisations have fallen foul of the Act (a few local authorities had to change their data collection activities when dealing with community charge records) there has not been the anticipated widespread interest by the public.

30. The Ninth Report of the Data Protection Registrar, published in June 1993, raises the Registrar’s concerns about allegations of a market in personal data. Where organisations hold personal data about individuals on their computer systems they have a responsibility, both legal and ethical, to ensure it is secure. The practice of browsing through computerised systems, as described in this report, may appear a minor threat but the existence of an information market could raise the profile of such activity and management needs to be aware of the threat and ensure sound systems of controlling access to personal data. HM Treasury’s Central Computer and Telecommunications Agency conducts its own analysis of computer abuse in central government and their view is that information misuse represents around a third of all reported incidents and is a key area of concern.

31. The 16 reported cases certainly represent only a very small part of the whole but as one respondent said about this type of abuse:

‘By far the most serious example of computer abuse is what we call “browsing” where a member of staff looks up an individual’s personal details. Staff have been dismissed in the last 12 months for supplying data obtained through browsing to a third party.’

A member of staff attended a consultant’s outpatients department and the diagnosis was coded and entered into the computer record but with no direct mention of the illness. A nurse knew that the consultation had taken place, accessed the file and diagnosed, from the medical information recorded, the patient’s illness. The nurse told her colleagues, one of whom contacted the manager. The nurse was dismissed and barred from practising in the United Kingdom.

Hacking

32. Hacking is defined as deliberately gaining unauthorised access to a computer system usually through the use of telecommunications facilities. Financial gain may not be the target of the hacker but manipulating personal records or stealing confidential data may prove more damaging to the organisation’s credibility and status. For some organisations the risk is a very real consideration. Within the NHS, for example, there is growing anxiety about computer centres which provide services to both medical schools and related hospitals. Medical schools want access to world-wide research and encourage a free exchange of data while hospitals want to protect patients’ data.
and make it available only on a need-to-know basis. There is an obvious conflict where both use the same computing facilities.

33. This issue will become more acute as the NHS drives towards a national network connecting all purchasers and providers of healthcare. While such technology will undoubtedly bring tangible benefits to patients, there are significant risks to data security which may prove tempting to the unscrupulous.

A nurse hacked into a hospital’s computer system and prescribed potentially lethal drugs for a patient and altered treatment records for others. The prescription changes were spotted by a nurse before the drugs were administered. He used a doctor’s personal identification code, which he had memorised some months earlier, to gain access to the system. He was successfully prosecuted under the Computer Misuse Act for unauthorised modification of computer data. The hospital management said that they never envisaged that a member of their professional staff would misuse the system.

34. The typical hacker is determined, ingenious and motivated by both the opportunity and the challenge. Organisations exist throughout Europe, for example, to foster widespread hacking into public sector and large corporate organisations. The availability of international networks with public access bulletin boards provides the means for the free exchange of techniques for cracking password and access codes. For disgruntled employees this form of abuse provides a means of wreaking revenge.

The virus

35. A virus is the term, originally coined in the mid-1980s, for a program which can, when triggered, produce copies of itself and implant these within other programs – hence the use of medical terminology to describe the virus program and its activities. The virus program has other characteristics: it is hidden from view (usually in a part of the disk which is not displayed on the screen); and it can perform certain functions which may range from being merely irritating (displaying a message on the screen) to malicious damage (erasing data from the disk). There is now an ever-growing, world-wide industry of virus writers, particularly in Eastern Europe and the Far East where the most damaging types of viruses seem to originate.

36. If the conditions are right and precautions have not been taken, it is relatively straightforward to infect unwittingly a PC’s disk. The disk, which may contain a virus program, is loaded into the disk drive of an apparently ‘clean’ machine and the program can, through a variety of techniques, be copied onto the hard disk and then, depending upon its trigger mechanism, it will infect other software. Viruses have become more sophisticated and can lie dormant for a specified period of time or await a particular set of circumstances to arise. Infecting disks is not difficult. Viruses may also be transferred over a network and over communication links if programs are
copied without regard to any restrictions. There is evidence, too, of viruses being found on mainframe computers as well as PCs.

37. The dramatic increase in virus infections is disturbing but not surprising. Media coverage of the subject over the past few years has emphasised how the problem has become almost epidemic in proportion. Several organisations who responded said they had suffered many incidents and were reporting only a selection. It is not surprising, therefore, that viruses account for the largest number of incidents – 48 per cent. Of the 261 virus cases reported, the costs of detection and recovery were around £255,000, giving an average cost per reported virus incident of around £977. One single virus incident caused one organisation to check over 450 machines and 4,000 disks incurring costs of £50,000.

An administrative officer introduced viruses onto three machines after having loaded software from another organisation onto the PC. Since this was in contravention of the organisation’s policy, he was suspended and is subject to a full disciplinary hearing. This incident has cost the organisation £5,000.

38. Over half the number of reported viruses occurred in organisations which gave no computer security awareness training for staff. Staff were unaware of the risks of using potentially infected disks. They are often unaware of the ease by which viruses can infect their data and the disruption and cost involved in reconstituting that data. Viruses are detected by the user when something goes wrong. Identifying the culprit is much more difficult, particularly where the machine is available for general use or where the user accepts disks without checking for viruses.

Illicit software

39. Ignorance of the law on copyright and copying together with poor software inventories and indiscriminate local purchasing of software all contribute to a widespread slackness in controlling a key asset of the organisation. Widespread use of illicit software within an organisation can be costly to rectify. One organisation had to pay £30,000 for new licences, whilst another incurred costs of £100,000. Other organisations have received unwelcome publicity due to such activities.

40. According to statistics released in April of this year by the Business Software Alliance (BSA), the software publishing and distribution industries lost more than £8.5 billion last year due to software theft. Total losses due to software piracy in 19 European countries exceeded £3.3 billion and the figure for the United Kingdom is estimated at £328 million. This represents a ‘piracy rate’ of 49 per cent. The United Kingdom is one of only six countries in the world where legal software exceeds 50 per cent of the market.

41. Concern by software developers who were losing revenue as a consequence of copying led to the formation of the Federation Against Software Theft (FAST) which has done much to heighten the awareness within the business
community of the use of illicit software through their investigations and prosecution of offenders. FAST has seized illegal software to the value of some £25m during the first half of 1994. While it may seem to some individuals and organisations that software theft is not a significant abuse, the customer will eventually foot the bill and so it is in the interests of all organisations to minimise this abuse.

During the investigation of a virus on an office network, it became apparent that there were many floppy disks on site which were not registered and had not been virus scanned, contrary to company policy. Local procedures were issued to reinforce the company procedures but they were still not applied vigorously.

A search of all work areas was undertaken and all unregistered floppy disks impounded. The perpetrator had 20 disks in his possession, all containing illicit software and a further 40 disks were found in his possession at the gate in the evening. He was dismissed and ten other contractors were disciplined. The incident cost the organisation £100,000 and they suffered much unfavourable publicity.

**Theft of data and programs**

42. The theft of portable computing equipment is a growing problem. There is a ready market for PCs, printers and other equipment. While this is an unwelcome loss, however, the theft of data and related software is often more serious. For some organisations the inability to reconstitute lost data could well prove to be the difference between business success or failure and the value of the lost information is certain to exceed the cost of replacing the equipment. Both public and private sector organisations are at risk from this type of abuse.

43. Over half the thieves in the 31 cases of software and data theft were not identified but in 28 per cent of cases they were found to be clerical staff and a further 14 per cent occupied supervisory and managerial positions.

A clerk stole hardware, software and a Mercury PIN number from the organisation and used it to access bulletin boards to view pornographic material in Europe and North America, circumventing the international call-barring facility on the office switchboard. The police recovered much of the software. The perpetrator was a member of the organisation’s security working party and was charged with the task of improving security. He had also volunteered to act as a relief caretaker and therefore had access to the office out of hours. He also controlled the office security access system which was based on card-entry.

44. In the 1993 survey, over £180,000 worth of software was lost in 12 incidents and the costs of recovering lost software for seven incidents was £33,000. Two cases of theft of data incurred costs of £7,000.
Unauthorised private work

45. Using the organisation’s IT facilities for unauthorised private work is regarded by some as acceptable – within reasonable bounds – and by others, as akin to stealing. Much depends upon the extent of the activity but, as many organisations encourage and provide portable IT facilities for use at home and in the office, it is not surprising that the limits of acceptability become blurred. Some organisations report that a limited amount of game-playing may be seen as an acceptable activity to encourage keyboard literacy but attitudes change when this extends to keeping the membership records for the local golf society or the accounts of a small part-time business run by a member of the family.

46. The worst excesses of unauthorised private work are found where the perpetrator uses the organisation’s IT facilities to run a business during office hours.

A member of staff was producing material for a local business, using the organisation’s computing facilities. The abuse was discovered by another member of staff visiting that business and recognising a fault common to all the organisation’s printing. The perpetrator resigned upon discovery.

47. Detection of such abuse is difficult. Evidence on a computer log will not necessarily highlight unauthorised work. An astute programmer, for example, might hide the work as development programs with innocuous names. Hence 53 per cent of instances were discovered by accident or from a ‘tip-off’ and the rest by internal control and internal audit.

48. Where information was provided, positive action appears to have been taken in the majority of cases with two prosecutions, 13 formal warnings and, with the exception of five cases where no action was taken, the remainder either dismissed, downgraded, transferred or allowed to resign.

Sabotage

49. Sabotage can include attacks on both hardware and software and while scant detailed information was provided for many of the 16 reported cases, it did appear that there was a bias towards software attacks.

50. Examples of software sabotage include:

A programmer who left a ‘time bomb’ in a program and timed it to go off on a date after his departure from the organisation;

A director who was dismissed for an incident unconnected with IT. The managing director was warned not to allow the dismissed director back into his office but he failed to comply with this advice. The next day the director’s disk was discovered to have been reformatted.
In four of the reported cases of sabotage, the total costs suffered by organisations were £104,625. The perpetrators were usually clerical and computer staff, though four were in management positions. Eight of the cases were discovered by accident and internal control and internal audit detected the remainder. As for the outcome, eight were prosecuted and/or dismissed.
A Prescription for Action, provides management with positive help to improve the situation.

2 Action for Management
A Prescription for Action

52. Understanding the causes and extent of computer fraud and abuse is the prelude to positive action for minimising the risk of further occurrences. The survey invited all respondents to indicate which preventive measures their organisations employed. The answers provide a fascinating insight into the favoured measures, bearing in mind the risks which organisations face and the incidents which many have suffered.

53. Given the high degree of dependence upon IT by most organisations, it is surprising that:
- nearly a quarter of organisations had no internal audit;
- about one half had no computer audit skills;
- two-thirds had no security awareness training in place; and
- four-fifths practised no risk analysis.

54. It is important, too, to emphasise that the effectiveness of any one of these measures within an organisation has not been assessed. A significant number of organisations have not evaluated the risk they face from computer abuse and have no independent in-house expertise to assist them despite the increasing opportunity for misuse as organisations become more dependent upon IT.

Internal audit

55. As well as effective control procedures, a sound internal audit should ensure that all staff work in a well-regulated environment which minimises the opportunity for any member of staff to commit a fraud. A major finding in this survey is that, while 60 per cent of all respondents rated fraud as a high risk, a quarter did not record internal audit as one of their preventive measures. Internal audit provides an essential ingredient in the internal control mechanism. The previous survey suggested that organisations needed more computer literate auditors and the situation has grown more acute since that
report was published. As organisations rely more heavily upon IT so risks increase and there is a greater need for constructive and cost-effective guidance on how to minimise risk.

56. While responsibility for designing and imposing controls lies with management, auditors are well placed to highlight deficiencies in procedures and make management and users better aware of the risks they face. More vigorous attention may well need to be given to identifying shortfalls in controls and in recommending improvements to management. Internal audit’s contribution to the design and maintenance of and adherence to effective internal control is critical and organisations are placing themselves at high risk if they do not equip themselves with an effective audit resource.

57. All of this calls for auditors to be better aware of the safeguards which need to be in place. While much is common sense, all auditors should be properly equipped with appropriate skills to understand and to evaluate risks and then to suggest practical improvements. Just as many managers and users are unaware of the risks of computer abuse, so many auditors have yet to be trained and equipped with the skills to advise their customers.

Who needs to take action?

58. Given the dependence upon the accuracy and reliability of computerised data, all involved in the management and use of computerised information have a responsibility to protect it. Better control over the use of technology and a sound appreciation of the risks will minimise fraud and abuse. Exhibit 5 overleaf highlights the key issues for action, described more fully in Appendix 1, to minimise the risk of computer abuse.

59. Organisations are urged to charge a senior member of staff to use the checklist to identify areas of concern and to develop an action plan to address them. All levels of management have a role to play and these roles are described below.

60. The chief executive and the management board must be determined to instil an awareness of the importance of computer security and be prepared to act when breaches occur. The Cadbury Report reaffirmed that ‘an effective control system is an essential part of the efficient management’ of an organisation and urged a greater focus on the wider issue of corporate governance.

61. Line management in user departments must ensure that access to facilities complies with the organisation’s standards. As IT moves away from the centre in the direction of departmental control so, too, will responsibility shift to the departmental manager for controlling the IT investment. Responsibility moves with the technology.

62. IT management must assist in defining cost-effective controls which protect the data it is holding and processing on behalf of others. It should also educate users in the need for controls over computerised data.

63. Internal auditors have a key role in monitoring, testing and advising on the adequacy of security and controls across the organisation as a whole. They should bring to management’s attention any shortcomings in the quality of internal control procedures and the adequacy of IT security generally and
emphasise the risks of all forms of computer abuse. Their responsibilities, and those of management, are defined in the CCAB Guidance for Internal Auditors which states:

‘It is a management responsibility to determine the extent of internal control in the organisation’s systems which should not depend on internal audit as a substitute for effective controls. The internal auditor should have regard to the possibility of such (fraudulent) malpractice and should seek to identify serious defects in internal control which might permit the occurrence of such an event.’

64. The Audit Commission’s auditors have a specific responsibility under their Code of Practice to evaluate the adequacy of procedures to minimise fraud. Protecting the Public Purse announced the creation of a fraud unit within the Commission which would focus attention upon the subject of fraud and support the work of the Commission’s auditors. Preventing and detecting fraud is an ongoing commitment. Just as new systems are initiated and new controls put in place, so the potential perpetrator will look for new ways of defeating the control system. Auditors need to be vigilant and ensure that management keeps the risk of fraud and abuse high on the agenda. The Checklist in Appendix 1 has been developed to help focus attention on the key issues.
Conclusions

1 The results of this survey reflect the reported cases. These reported activities are indicative of the risks and opportunities which may be present in any system in any organisation. Computer fraud and abuse incidents fall into three categories:
   - those which are known and recorded publicly;
   - those which are known only within organisations and which will not be brought into the public arena; and
   - those which are, as yet, undiscovered.

2 The Commission’s survey provides an authoritative indication of the nature of the problem but does not claim to define its full extent and it has avoided estimating the likely total cost of computer abuse since such a figure can never be substantiated. The value of this survey lies not in the amount of reported fraud it unearthed. The value lies rather in the demonstration of the wide range of types of computer abuse, the consequent scale of risk that exists and the considerable opportunities that exist for further abuse.

3 As organisations increase their dependence upon technology so it will be attractive to the criminally-minded to focus their energies on new sources of wealth. Computer fraud and abuse is already thought to be a growth area for organised abuse and the opportunity to divert funds or steal sensitive data without the necessity to be on site or handle the money has obvious attractions.

4 As IT becomes a normal part of the employees work patterns there is a risk of almost casual disregard in protecting data. Large volumes of data can be easily stored on pocket-sized disks with little regard for its importance. Managers and users must understand the value of data and protect it before it gets lost or damaged – deliberately or accidentally.
In many organisations, responsibility is devolving downwards from the centre towards the point of service delivery. The costs, in terms of risk and security, and implications of such change in responsibility are:

- local management may be unaware of the need to protect their systems locally, imagining that the centre still retains control;
- local staff training may not have emphasised the need for controls and safeguards or highlighted the requirements of the Data Protection Act with regard to personal data.

The focus of this report has been on the action to be taken by management to exercise better control over procedures inhibiting computer abuse. Resolution of the problem lies in management’s hands. It is no mere technology issue – it is a people issue, too. If management really wants to limit fraud, virus infections, unauthorised private work and other forms of computer abuse then it has the power to do so.
Appendix 1 - includes a checklist to assess key risks and identify protective measures.

Appendix 2 - provides further descriptions of the various types of incident for those readers less familiar with the characteristics of computer abuse.

Appendix 3 - includes additional detailed analyses from the survey.
Appendix 1

The checklist identifies a set of key issues which should be addressed by senior management. The questions which management should be asking of its organisation are highlighted together with a number of supplementary questions which should be pursued.

Do we have an IT security policy?

- Is it endorsed by the Management Board?
- What do we spend on IT security?
- Have we assessed the opportunities for abuse?
- Does the policy recognise the threats from staff and outsiders?
- Is the policy reflected in the terms of employment?
- Do we pursue IT security vigorously?

Typical content of an IT security policy

A code of practice for IT security provides a framework for defining the standards of security relating to the use of information technology within an organisation. Many organisations have produced such codes and one which is particularly relevant is the Code of Practice for Information Security Management - developed by a group of leading United Kingdom companies and organisations and endorsed by the Department of Trade and Industry. The overall policy should be endorsed and promulgated by the Management Board. Individual departments should then develop operational plans to ensure that the policy is actively reflected in the working environment.

The key characteristics of an IT security policy should be:

- a definition of IT security which fits with the business strategy
- a clear statement by management of the importance it attaches to IT security
- a statement of the responsibilities of staff to protect the investment in IT and the computerised data they use
- a statement of the legislation (Data Protection Act and Computer Misuse Act, for example) which must be enforced
- an indication of the steps taken by management to encourage and enforce the adoption of a high standard of security
- the steps which should be taken to minimise the risk of fraud and other forms of computer abuse (ensuring adequate division of duties, the adoption of password and personal identification facilities, for example)
the procedures governing the acquisition of new equipment and of software which should help preserve the completeness and accuracy of processing
the internal control mechanisms for monitoring adherence to the policy
The role of internal audit and any other monitoring agencies within an organisation

Have we assigned responsibilities to our staff for security?
- Who is responsible in our organisation for IT security?
- Is that person experienced in computing and business activities?
- Are all staff aware of the importance of securing data in a computerised environment?
- Do our staff understand the principles of the Data Protection Act and Computer Misuse Act?
- Is a breach of IT security a disciplinary issue?
- Do we screen job applicants to ensure they are not likely to breach our IT security?
- Are all breaches of IT security reported and is action taken?

Does our organisation have the necessary skills to advise upon good controls?
- Do we have an effective internal audit?
- Are our internal auditors sufficiently skilled to audit in a computerised environment?
- Do we use specialist computer auditors?
- Does audit use computer-assisted audit techniques to check the adequacy of our controls and safeguards?

The advantages to organisations of using such techniques are:
- the opportunity to interrogate independently the data as held on the computer rather than having to rely on the normal processing cycle and paper-based reports produced by the organisation;
- the ability to apply tests on 100 per cent of data rather than having to rely upon random and partial tests;
- the opportunity to apply tests which would be too time-consuming or too complex if applied manually;
- the availability of relatively easy-to-use software tools which can be used with minimal training.
Do we operate in a secure computerised environment?

- Are basic control processes in place to ensure that the integrity of our fundamental systems is not breached?
- Do these controls include a regular and complete reconciliation process for financial systems?
- Do we give attention to minimising risks of fraud and abuse by ensuring sufficient division of duties between key control tasks?

Do we have effective controls over access to our various computing environments?

How adequate are our password controls eg:

- Do we always require passwords to be used?
- Is the display of passwords on screens suppressed to prevent unauthorised viewing?
- Do we discourage staff from using easy-to-guess passwords?
- If changes to passwords are carried out automatically through the system, do we ensure that users are notified of such changes confidentially?
- Are passwords shared by individuals?
- Are passwords changed when staff leave or change duties?

How effectively do we control access to PCs eg:

- Do we use a ‘clean’ machine to check specifically for viruses?
- Do we use virus-checking software regularly?
- Do we use access control software on PCs to inhibit the loading of unauthorised programs?
- Do we warn staff about introducing games and other unauthorised external software?
- Do we encourage regular backups to minimise recovery problems?
- Do we use screen-saver software to prevent screens being left ‘open’ for unauthorised use?
- Do we only accept software from suppliers who certify that it is virus free?

When did we last assess the risks of computer abuse and the opportunities for misuse?

- Have we identified those fundamental systems most at risk?
- Have we assessed the scale of the loss or damage which could be caused by each type of computer misuse?
- How regularly do we re-assess this?
- When was the Management Board last made aware of any risks?
- What steps do we take – commensurate with risk and cost – to minimise risk and opportunities for misuse?
- Have we assessed the adequacy of our insurance cover against computer fraud and abuse?
Do we recognise the risk to individuals when personal data is exposed?
- Do we discourage unauthorised browsing through personal data?
- What action do we take if breaches occur?
- Are staff aware of the nature of this abuse?

What steps have we taken to make staff security-conscious?
- What training do we provide for new employees?
- What IT security training is regularly available for all staff?
- What guidance on IT security do we provide for staff?

Have we recognised the threats of computer abuse?
Have we taken positive steps to ensure that:
- frauds are difficult to perpetrate?
- unauthorised ‘browsing’ of personal data is discouraged?
- viruses cannot infect our equipment?
- hackers are denied access?
- only licensed software is used?
- theft of computerised data and software is minimised?

Appendix 2

Examples of incidents

Descriptions of actual incidents were not disclosed in many of the responses but some examples are included here for general interest and for those readers less familiar with the characteristics of computer abuse

Computer fraud

Sales/Debtors systems
- A clerk in a debtors section suppressed the production of a final demand to her boyfriend, a debtor. Her colleagues became suspicious when routinely sending out first reminders. She resigned after discovery of the incident but the organisation incurred costs of detection, her suspension on full pay, a disciplinary hearing and the costs of recruiting another post holder.
- Temporary staff employed in a debtors section were using the online system to suppress recovery action in respect of arrears on their own accounts and those of relatives and friends. The perpetrators were dismissed and, as a result of the fraud coming to light, the system was amended to ensure that only high grade staff could suppress print-outs and even these would be examined by management.
A cashier at a remote office had access to the supervisor’s password to enable her to close down the system and, amongst other things, to initiate contra entries to correct mistakes etc. She used this facility to suppress evidence of takings in respect of account numbers of regular payers who would not normally receive a payment reminder. She then retained the cash. However a customer who had paid (and produced her receipt) complained when she received a reminder and, following an internal audit investigation, the fraud came to light. The loss of £350 was recovered from the perpetrator who was dismissed and prosecuted but given a caution as she was pregnant. The fraud was perpetrated because the daily prints from the cashier were never checked independently to ensure all contras could be accounted for.

A sales assistant in an entertainments complex cancelled sales of Standing tickets (which could be resold without causing concern) and withheld the cash. The incident came to light when an event was cancelled and a customer asked for a refund on tickets which had in fact been cancelled and resold. The transaction log and shift patterns showed who had processed the cancellations but the organisation felt that the jury and prosecuting barrister did not understand the evidence. The suspected perpetrator was acquitted.

Purchases/Creditors

A clerk defrauded the organisation of £38,500 over a period of five years from its Purchases system. Initially the perpetrator added a bogus invoice with a forged approval slip to batches which had already been prepared by Payments division. Then the batching procedures were subsequently changed and batch headers had to be signed and show the number and value of the invoices but the perpetrator responded by switching a bogus invoice for an approved invoice of an identical amount and then submitting the genuine invoice later with a forged approval slip. Internal audit eventually detected the fraud and the perpetrator was dismissed, prosecuted and sentenced to 18 months imprisonment.

A clerk in a student awards payments section managed to obtain, by deception, the system password to gain access to prohibited data files. She used this access to arrange for payments to be made into her own bank account via BACS. The fraud came to light when a payments schedule was queried by one of the colleges which she claimed to be attending. Over £25,000 was defrauded by the clerk who had worked in the organisation for 10 years. She resigned after discovery of the incident and the case is with the Crown Prosecution Service.

A manager ignored the organisation’s security guidelines and left his password to the Purchases system on a note by his workstation. Another employee used the password to arrange payments to fictitious accounts totalling £120,000. The perpetrator was arrested, charged and sentenced to two year’s imprisonment.

A clerk working in an insurance claims section used another’s password to initiate unauthorised payments to himself and defrauded the company of £25,000. The perpetrator was dismissed and prosecuted under the Theft Act.
Acts and was imprisoned and around 75 per cent of the loss was recovered from the perpetrator. The incident was discovered through internal control processes and the primary reasons cited for the fraud occurring were inadequate division of duties, poor management trails and the fact that transactions were not authorised.

◆ The perpetrator was a system administrator in the computer department with full access to all the system’s facilities. He input false student awards claims into the creditor payment system and when the cheques were produced he went back into the system and removed all evidence of the transactions. Some £60,000 was defrauded, discovered when external audit carried out a creditors’ system review and identified the false payments. The payments were queried because student awards were not normally paid through the creditor payments system but the reconciliation procedures were weak and the payments were not identified. An interesting characteristic of this case was that the perpetrator had previously reported the weaknesses in the system to management but as nothing was done, he took advantage of the opportunity.

◆ The perpetrator, a clerk in a section dealing with insurance policies, had managed to access his girlfriend’s insurance policy details and overwritten certain information. The supervisor had become suspicious because the perpetrator turned off his terminal as people approached his desk. After a few days, the supervisor waited until he had gone home and then turned out his wastepaper bin and found a number of screen prints. Internal audit and the DP security officer were immediately informed and a trace put on the perpetrator. After watching his activity on a monitor in the computer room they were certain that the perpetrator was systematically attempting to access files in a manner which was not part of normal processing. The perpetrator was questioned and admitted what he had done. He was immediately escorted from the building and his employment agency notified although he had failed to initiate a fraudulent payment at that stage.

The organisation had failed to notice from his CV that he had experience of the system software used in the organisation and knew therefore the software instructions for accessing the system. Recruitment procedures have now been changed.

Stock
◆ To help with the implementation of a new system, a high level password was granted to a system support member of the computer department. This password was never cancelled when the implementation was completed and the member used the password to access the Stock system and defraud the organisation of £30,000 of trading stock in collusion with others. The perpetrator had been in post for four years and resigned after discovery of the incident.

◆ A stores manager moved stock with the collusion of other employees and altered the computer records to suggest the stock had been sold. The £9,000
loss was recovered from the perpetrator who had worked with the organisation for 20 years.

Payroll

- A supervisor at one of the company's manufacturing branches was paying non-existent canteen staff through the company's payroll system. The fraud, which resulted in a loss of £5,000, was detected when he was on holiday and copies of payslips for non-existent employees were found in his desk. The perpetrator was dismissed.

- A payroll clerk reactivated retired employees' records and changed their bank account details to one of three accounts she controlled (including her own account). Because of a non-deductible allowance being paid to a former employee, the account details had to be altered prior to each pay calculation run and then subsequently corrected. Unfortunately for the perpetrator, being off sick meant that she was unable to correct a payment and so the pay advice was sent to the pensioner who queried the information and the fraud was detected. The perpetrator, who defrauded the organisation of £25,000 and had been employed by them for three years, was dismissed and a prosecution is pending.

Personal accounts

- A trainee programmer left within the two year stipulated period and was therefore responsible for repaying £1,900 for an agency introduction fee and interview expenses which had been incurred. The debtors section discovered when they conducted a periodic balancing of the Sundry Debtors Control Account that the debt had been deleted from the system. Programmers had access to the live programs and data files and the organisation's management were convinced that the trainee programmer had deleted the record from the system before he left.

- A clerk in the Rents Section realised that a high level of credits existed in a suspense account. He gained access to the system by using another's password and transferred a balance from a 'dead' file to a friend's. He then arranged to refund the credit to the friend and to share the proceeds. The member of staff whose password had been used grew suspicious as he was not at work on the day the incident occurred although there was a record of the activity on the log report. Internal audit investigated and identified the culprit but waited until he wrote asking for the refund before challenging him. Although there was no direct loss, indirect losses amounted to £5,000.

- A member of the IT department and her boyfriend accessed dormant accounts in a financial organisation and transferred up to £170,000 investor's funds to bogus accounts.

Virus

- The perpetrator used a salesperson's disk on an organisation's PC which transferred a virus to other PCs across the network. The organisation said they incurred costs of £15,000 as a result of this incident.
A customer of a rental company complained that there was a virus on the disk he had hired and this had corrupted files on his network. The rental company resolved the problem and believed the virus had been left on the machine from a previous customer. They regarded the risk to their business as very significant and compulsory virus-checking is now performed before and after each rental.

Unauthorised private work

The perpetrator developed software which he sold to other organisations on a private basis and when other employees were developing similar (official) software for sale to the same organisations. Initially the perpetrator was dismissed but he successfully appealed to the organisation's appeals committee and was reinstated, given a final warning and transferred to another post.

Sabotage

On 17 December staff could not access the accounting system but the message 'It's somebody's birthday today!' was displayed on the screens. After an investigation it was found that the 'logic bomb' had been inserted into the software nearly two years earlier. The perpetrator was not identified.

Hacking

A student at another university hacked into the college's computer system via access to the JANET academic network. He then found the account and password of a member of the academic staff who had not used the system for some months.

He used the enhanced access rights held by the member of staff to modify their Mail address on JANET and then 'leap-frogged' to another JANET site masquerading as the member of staff.

While no evidence of unauthorised access was then available on the 'home' university's system, his starting point at the other university was identifiable and so the police alerted the other university. The culprit was identified and prosecuted.
## Appendix 3

**Detailed analyses**

### Incidents by type of organisation

A healthy response from a voluntary survey

<table>
<thead>
<tr>
<th>Type</th>
<th>Total Responses</th>
<th>Per cent with Incidents</th>
<th>Total Fraud</th>
<th>Virus</th>
<th>Illicit Software</th>
<th>Private Work</th>
<th>Theft Soft/Data</th>
<th>Invasion Privacy</th>
<th>Sabotage</th>
<th>Hacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local government</td>
<td>290</td>
<td>41</td>
<td>193</td>
<td>63</td>
<td>85</td>
<td>13</td>
<td>17</td>
<td>6</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Health</td>
<td>334</td>
<td>35</td>
<td>127</td>
<td>11</td>
<td>69</td>
<td>23</td>
<td>7</td>
<td>7</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Government</td>
<td>24</td>
<td>46</td>
<td>66</td>
<td>21</td>
<td>40</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td>87</td>
<td>36</td>
<td>33</td>
<td>11</td>
<td>7</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Finance</td>
<td>58</td>
<td>45</td>
<td>27</td>
<td>4</td>
<td>17</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>125</td>
<td>20</td>
<td>27</td>
<td>2</td>
<td>10</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Utilities</td>
<td>10</td>
<td>80</td>
<td>11</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Construction</td>
<td>36</td>
<td>28</td>
<td>10</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Food</td>
<td>16</td>
<td>44</td>
<td>7</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td>12</td>
<td>50</td>
<td>7</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wholesale</td>
<td>18</td>
<td>28</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td>11</td>
<td>36</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marketing</td>
<td>8</td>
<td>50</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chemical</td>
<td>11</td>
<td>36</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail</td>
<td>10</td>
<td>20</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>23</td>
<td>25</td>
<td>8</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1,073</strong></td>
<td><strong>36</strong></td>
<td><strong>537</strong></td>
<td><strong>108</strong></td>
<td><strong>261</strong></td>
<td><strong>54</strong></td>
<td><strong>36</strong></td>
<td><strong>31</strong></td>
<td><strong>16</strong></td>
<td><strong>16</strong></td>
</tr>
</tbody>
</table>

Direct losses £  

<table>
<thead>
<tr>
<th>Type</th>
<th>Direct Losses</th>
<th>Indirect Losses</th>
<th>Total Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local government</td>
<td>3,196,720</td>
<td>2,904,430</td>
<td>6,101,150</td>
</tr>
<tr>
<td>Health</td>
<td>30,485</td>
<td>5,530</td>
<td>35,015</td>
</tr>
<tr>
<td>Government</td>
<td>186,775</td>
<td>9,400</td>
<td>196,175</td>
</tr>
<tr>
<td>Education</td>
<td>149,850</td>
<td>9,400</td>
<td>159,250</td>
</tr>
<tr>
<td>Finance</td>
<td>13,070</td>
<td>3,500</td>
<td>16,570</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>39,125</td>
<td>9,400</td>
<td>48,545</td>
</tr>
<tr>
<td>Utilities</td>
<td>16,220</td>
<td>9,400</td>
<td>25,640</td>
</tr>
<tr>
<td>Construction</td>
<td>222,275</td>
<td>9,400</td>
<td>231,675</td>
</tr>
<tr>
<td>Food</td>
<td>224,440</td>
<td>9,400</td>
<td>233,840</td>
</tr>
<tr>
<td>Communications</td>
<td>9,400</td>
<td>9,400</td>
<td>18,800</td>
</tr>
<tr>
<td>Wholesale</td>
<td>137,888</td>
<td>9,400</td>
<td>147,288</td>
</tr>
<tr>
<td>IT</td>
<td>149,850</td>
<td>9,400</td>
<td>159,250</td>
</tr>
<tr>
<td>Marketing</td>
<td>222,275</td>
<td>9,400</td>
<td>231,675</td>
</tr>
<tr>
<td>Chemical</td>
<td>149,850</td>
<td>9,400</td>
<td>159,250</td>
</tr>
<tr>
<td>Retail</td>
<td>224,440</td>
<td>9,400</td>
<td>233,840</td>
</tr>
<tr>
<td>Other</td>
<td>149,850</td>
<td>9,400</td>
<td>159,250</td>
</tr>
</tbody>
</table>

Total losses £
### Analysis of frauds by organisation

<table>
<thead>
<tr>
<th>Organisation</th>
<th>TOTAL</th>
<th>Input</th>
<th>Output</th>
<th>Program</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local government</td>
<td>63</td>
<td>31</td>
<td>3</td>
<td>2</td>
<td>27</td>
</tr>
<tr>
<td>Health</td>
<td>11</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Government</td>
<td>21</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td>4</td>
<td>3</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Utilities</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wholesale</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Marketing</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>108</td>
<td>62</td>
<td>7</td>
<td>6</td>
<td>33</td>
</tr>
</tbody>
</table>

### Methods of detection for all incidents

<table>
<thead>
<tr>
<th>Detection Method</th>
<th>TOTAL</th>
<th>Fraud</th>
<th>Private Work</th>
<th>Theft</th>
<th>Illicit software</th>
<th>Invasion privacy</th>
<th>Sabotage</th>
<th>Hacking</th>
<th>Viruses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal control</td>
<td>178</td>
<td>48</td>
<td>10</td>
<td>4</td>
<td>19</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>83</td>
</tr>
<tr>
<td>Internal audit</td>
<td>44</td>
<td>8</td>
<td>7</td>
<td>2</td>
<td>19</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>External audit</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Security staff/police</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Claimant/customer enquiry</td>
<td>20</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Accidental means</td>
<td>154</td>
<td>16</td>
<td>8</td>
<td>9</td>
<td>9</td>
<td>0</td>
<td>6</td>
<td>1</td>
<td>105</td>
</tr>
<tr>
<td>Information received</td>
<td>62</td>
<td>15</td>
<td>11</td>
<td>8</td>
<td>4</td>
<td>10</td>
<td>0</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>Confession</td>
<td>18</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>487</td>
<td>97</td>
<td>36</td>
<td>29</td>
<td>54</td>
<td>16</td>
<td>13</td>
<td>13</td>
<td>229</td>
</tr>
</tbody>
</table>
### Perpetrators

<table>
<thead>
<tr>
<th></th>
<th>TOTAL</th>
<th>Fraud</th>
<th>Private Work</th>
<th>Theft</th>
<th>Illicit software</th>
<th>Invasion privacy</th>
<th>Sabotage</th>
<th>Hacking</th>
<th>Viruses</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management</strong></td>
<td>70</td>
<td>19</td>
<td>8</td>
<td>4</td>
<td>13</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>director/snr manager</td>
<td>17</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>manager</td>
<td>30</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>supervisor</td>
<td>23</td>
<td>11</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>Administration</strong></td>
<td>172</td>
<td>78</td>
<td>23</td>
<td>9</td>
<td>11</td>
<td>12</td>
<td>7</td>
<td>5</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>clerk</td>
<td>115</td>
<td>60</td>
<td>12</td>
<td>3</td>
<td>8</td>
<td>9</td>
<td>2</td>
<td>5</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>salespersons</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>temporary staff</td>
<td>14</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>programmer/analyst</td>
<td>12</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>systems support technical</td>
<td>25</td>
<td>5</td>
<td>9</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>audit/security staff</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td><strong>External</strong></td>
<td>43</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>customer</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>consultant</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>suppliers</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>agent</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>engineer</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>285</td>
<td>97</td>
<td>34</td>
<td>14</td>
<td>27</td>
<td>15</td>
<td>13</td>
<td>10</td>
<td>75</td>
<td></td>
</tr>
</tbody>
</table>

### Action taken against perpetrators

<table>
<thead>
<tr>
<th></th>
<th>TOTAL</th>
<th>Fraud</th>
<th>Private Work</th>
<th>Theft</th>
<th>Illicit software</th>
<th>Invasion privacy</th>
<th>Sabotage</th>
<th>Hacking</th>
<th>Viruses</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No action</strong></td>
<td>44</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>9</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>Resigned after discovery</td>
<td>22</td>
<td>11</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>99</td>
<td>12</td>
<td>13</td>
<td>3</td>
<td>16</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>41</td>
<td></td>
</tr>
<tr>
<td>Dismissed</td>
<td>77</td>
<td>48</td>
<td>12</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Resigned before discovery</td>
<td>11</td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Prosecuted</td>
<td>58</td>
<td>45</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>8</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>319</td>
<td>128</td>
<td>38</td>
<td>15</td>
<td>27</td>
<td>17</td>
<td>13</td>
<td>9</td>
<td>72</td>
<td></td>
</tr>
</tbody>
</table>

(note that the actions taken are not mutually exclusive)
### Insurance

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does your General Risks policy cover computer abuse?</td>
<td>34 per cent</td>
<td>66 per cent</td>
</tr>
<tr>
<td>LG</td>
<td>45 per cent</td>
<td>55 per cent</td>
</tr>
<tr>
<td>NHS</td>
<td>23 per cent</td>
<td>77 per cent</td>
</tr>
<tr>
<td>Do you have special computer abuse cover?</td>
<td>12 per cent</td>
<td>88 per cent</td>
</tr>
<tr>
<td>LG</td>
<td>15 per cent</td>
<td>85 per cent</td>
</tr>
<tr>
<td>NHS</td>
<td>9 per cent</td>
<td>91 per cent</td>
</tr>
<tr>
<td>Does your insurance company require specific computer security standards?</td>
<td>15 per cent</td>
<td>85 per cent</td>
</tr>
<tr>
<td>LG</td>
<td>18 per cent</td>
<td>82 per cent</td>
</tr>
<tr>
<td>NHS</td>
<td>9 per cent</td>
<td>91 per cent</td>
</tr>
</tbody>
</table>
HMSO publications are available from:
HMSO Publications Centre
(Mail, fax and telephone orders only)
PO Box 276, London, SW8 5DT
Telephone orders 0171 873 9090
General Enquiries 0171 873 0011
(queuing system in operation for both numbers)
Fax orders 0171 873 8200

HMSO Bookshops
49 High Holborn, London, WC1V 6HB
(counter service only)
Tel: 0171 873 0011 Fax: 0171 873 8200
258 Broad Street, Birmingham, B1 2HE
Tel: 0121 643 3740 Fax: 0121 643 6510
33 Wine Street, Bristol, BS1 2BQ
Tel: 0117 9264306 Fax: 0117 9294515
9-21 Princess Street, Manchester, M60 8AS
Tel: 0161 834 7201 Fax: 0161 833 0634
16 Arthur Street, Belfast, BT1 4GD
Tel: 01232 238451 Fax: 01232 235401
71 Lothian Road, Edinburgh, EH3 9Az
Tel: 0131 228 4181 Fax: 0131 229 2734

HMSO’s Accredited Agents
(see Yellow Pages)
and through good booksellers

£8.50 net
District Auditors were first appointed in the 1840s to inspect the accounts of authorities administering the Poor Law. Auditors ensured that safeguards were in place against fraud and corruption and that local rates were being used for the purposes intended. The founding principles remain as relevant today as they were 150 years ago. Public funds need to be used wisely, as well as in accordance with the law. The task of today's auditors is to assess expenditure, not just for probity and regularity, but for value for money as well.

The Audit Commission was established in 1983 to appoint and regulate the external audit of local authorities in England and Wales. In 1990 its responsibilities were extended to include the National Health Service. For more information on the work of the Commission, please contact:

The Audit Commission
1 Vincent Square
London
SW1P 2PN
Tel: 0171 828 1212