

yourbusiness@risk

An update on IT Abuse 2001

The incidence of IT abuse within the UK has been reported every three years by the Audit Commission since 1983. Based upon surveys of both the public and private sectors, the reports provide a snapshot of the level of IT abuse, the reasons for its occurrence and the risks that organisations need to address.

Organisations have got better at establishing anti-fraud frameworks, cultures and strategies...

- more than three-quarters have an up-to-date information security policy
- one-half have established anti-fraud strategies
- almost two-thirds encourage whistle-blowing

...but failures in basic controls are still a problem...

- many cases of IT abuse are made possible because of a lack of supervision
- control over who can gain access to information is still too weak



...and new risks associated with the upsurge in the use of new technologies have not been sufficiently addressed.

- almost all organisations use e-mail facilities and the Internet
- but controls over the use of these facilities are often inadequate

Consequently, IT abuse continues to rise and respondents to the survey generally feel more vulnerable in their use of IT.

- 80 per cent of organisations report an increased risk of IT fraud

Business disruptions have grown...

- virus infections continue to be a significant problem
- hacking and sabotage are still a real threat

...and reputational damage is emerging as a significant threat.

- the downloading and distribution of pornographic material has increased
- new legislation and ways of working increase the risk of an inadvertent breach of the law

Financial losses and associated costs remain high.

- the average value of detected IT frauds is £36,000

Confidence in the technologies that are influencing the way we live and work is being eroded. Organisations must address the issues contained in this report if the explosion in the use of new technology is not to be matched by a similar increase in IT abuse.

Contents

	Introduction	3
1	The Consequences of IT Abuse	6
	Survey results and key conclusions	6
	Business disruption	7
	Reputational damage	10
	Financial loss	13
2	The Increasing Risk of IT Abuse	17
	Technology dependency	17
	Increasing IT literacy	18
	The Government's technology agenda	18
	E-commerce	18
	Citizens' expectations	21
	Rise in e-crime	22
3	Prevention is Better than Cure	23
	Why incidents happened	23
	Most targeted systems	24
	Measures to prevent IT abuse	24
	Security ethos	26
	Policies and protocols	26
	Review of IT security procedures and processes	27
	References	29

© Audit Commission 2001

First published in September 2001 by the Audit Commission for Local Authorities and the National Health Service in England and Wales, 1 Vincent Square, London SW1P 2PN

Printed in the UK for the Audit Commission by CW Print Group

ISBN 1 86240 289 2

Photograph: Telegraph Colour Library

New technology has had a significant impact on the way we live and work over the last 20 years.

Introduction

1. New technology has had a significant impact on the way we live and work over the last 20 years. Improvements in information and communications technology have increased the demand for more and better information, which has led to a rapid growth in information-related services. However, these changes have brought with them an increased risk of abuse [BOX A].

BOX A

IT abuse: definition of incidents

Virus

Distributing a program with the intention of corrupting a computer process.

Introduction of unsuitable material

Introducing subversive or pornographic material, for example, by downloading from the Internet.

Private work

Unauthorised use of the organisation's computer facilities for private gain.

Fraud

Private gain or benefit by:

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

Hacking

Deliberately gaining unauthorised access to an information system.

Use of unlicensed software

Using unlicensed copies of software.

Invasion of privacy

Breaches of data protection legislation.

Theft

Theft of information.

Sabotage

Interfering with the computer process by causing deliberate damage to a processing cycle or to equipment.

Source: Audit Commission

The main objective in all of the Commission's surveys has been to identify the risks associated with the use of technology across all sectors...

2. In 1981, the Local Government Audit Inspectorate published the first UK report on computer fraud and abuse. It created widespread interest both in the UK and abroad.

3. Three years later, the Audit Commission, the Inspectorate's successor body, revisited the topic and discovered that the incidence of fraud and abuse had increased and that new risks had emerged. The Commission has continued to review the situation every three years. The last report, *Ghost in the Machine* was published in February 1998 and concluded that (Ref. 1):

- computer crime was on the increase;
- key risks identified in previous surveys still posed a significant threat;
- new risks, such as accessing unsuitable material, were emerging;
- some organisations had responded positively to the challenges posed; but
- some were still not taking the risks seriously enough.

4. When our first report was published, almost twenty years ago:

- most information systems were processed in large, centralised computer centres;
- the personal computer was seen as a games machine rather than a business tool;
- the Internet was known only to a few people;
- the 'computer virus' had still to enter our everyday vocabulary; and
- widespread use of mobile technology was years away.

5. The main objective in all of the Commission's surveys has been to identify the risks associated with the use of technology across all sectors and to assess the particular impact upon local government and the NHS in England and Wales. However, the surveys provide valuable information, comparative data and practical advice which managers in other sectors will find helpful.

6. For this report, questionnaires were sent to all local authorities and NHS bodies in England, Wales and Scotland, as well as to central government departments and agencies. Other public sector bodies covering the education and housing sectors were also included, as were a range of large companies throughout the UK.

7. This report is based upon responses from 688 organisations from the public and private sectors of which 460 reported that they had suffered some form of IT abuse during the last three years – that is, 1997 to 2000. It shows that the percentage of organisations reporting incidents increased by almost one half since our last survey [TABLE 1].

TABLE 1

Responding organisations – percentage with incidents

The percentage of organisations reporting IT abuse rose by 49 per cent.

	Number of organisations	Percentage with incidents		Percentage change
		2000	1997	
Local government	211	72	50	+ 44
Health	242	68	45	+ 51
Central government	9	67	42	+ 60
Education	80	76	59	+ 29
Total public sector	542	71	49	+ 45
Manufacturing	10	60	21	+ 185
Other commercial	86	58	32	+ 81
Finance	50	38	45	- 16
Total private sector	146	51	35	+ 46
Total for all organisations	688	67	45	+ 49

Source: Audit Commission

This report highlights the risks that face local government and NHS bodies as they implement the e-government agenda.

8. This report highlights the risks that face local government and NHS bodies as they implement the e-government agenda. It considers the lessons from the past, and draws upon conclusions from other, similar surveys. It looks at the changes that are needed to facilitate electronic service delivery and suggests the precautions that managers should take.

9. The guidance and recommendations contained in this, and previous Commission reports, are intended to help local government and NHS bodies to minimise the risk of IT abuse. A self-assessment checklist is provided at the centre of the report for this purpose. It may be pulled out and copied for distribution throughout your organisation.

10. We are grateful to all those who responded to the survey and for the information and case study material that they have provided. Responsibility for the analysis and results, of course, rests solely with the Commission.

1

The Consequences of IT Abuse

Survey results and key conclusions

11. The use of new technologies by organisations has increased over the last three years. The increased number of incidents of IT abuse indicates that the implementation of effective controls has not kept pace [EXHIBIT 1].

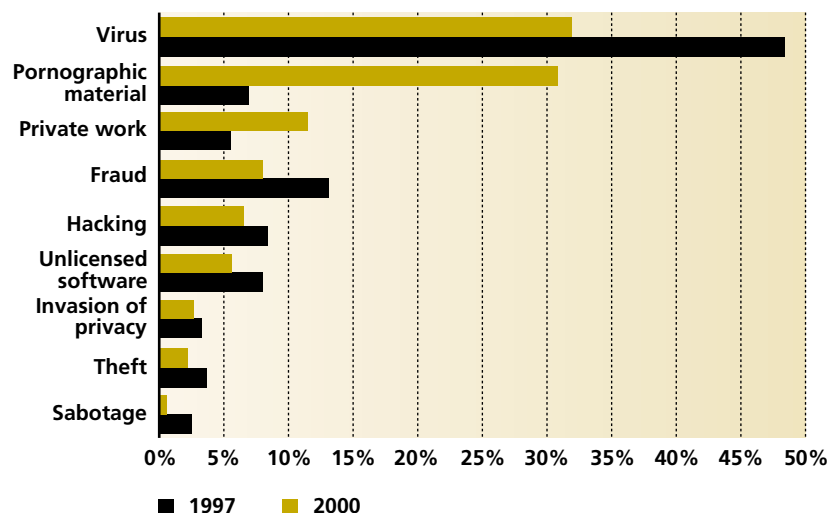
12. Our previous two reports *Ghost in the Machine* and *Opportunity Makes a Thief* highlighted the fact that virus infections were the most prevalent form of IT abuse (Refs. 1, 2). This current survey shows that this is still the case with viruses representing almost one-third of the incidents reported. The figure is probably understated since a number of respondents said that they had suffered a number of infections but reported only one.

13. There has also been a large increase in the percentage of respondents reporting incidents involving the processing of pornographic or other unsuitable material. Our last report highlighted a number of cases for the first time and identified this as an emerging threat. In 1997 such cases represented less than 10 per cent of incidents, they now account for 31 per cent of all incidents.

EXHIBIT 1

Percentage of reported incidents by type

Virus infections and the downloading or transmission of unsuitable material are the most prevalent form of IT abuse.



Source: Audit Commission

14. The level of IT fraud continues to fall, as a percentage of all reported incidents, over the period covered by our previous two reports. This survey shows that IT fraud has reduced from 13 per cent to 8 per cent of reported incidents. This ought not to be taken as an opportunity to reduce vigilance. There are still many lessons to be learned from those incidents that are reported and they are outlined later in this report.

15. IT abuse, such as hacking and the use of unlicensed software, continue to pose a real threat to the widespread development of safe electronic service delivery. Private work showed an increase from 5 per cent to 12 per cent of reported incidents.

16. The main consequences of the reported incidents of IT abuse can be categorised as:

- business disruption;
- reputational damage;
- financial loss; and
- the erosion of confidence in the use of IT to deliver services.

Business disruption

Virus infection

17. In May 2000 the 'Love Bug' computer virus was reported to have caused havoc in personal and business systems world-wide. The cost of restoring infected systems is not known but estimates run into hundreds of millions of pounds.

18. In the past the transmission of a complex virus was caused mainly by the exchange of infected disks. Today, the increased number of e-mail users and the trend towards networked rather than standalone PCs has meant that transmitting a virus has become much easier and quicker [CASE STUDY 1].

19. Two-thirds of respondents considered the receipt of a virus infection as medium or high risk. Two hundred incidents of viruses were reported but many added that they had suffered multiple infections although they were only reporting one incident for illustrative purposes.

CASE STUDY 1

An e-mail from a trusted source contained a virus. The sender of the e-mail was unaware of what they had done. The receiver of the e-mail had been experiencing problems while upgrading some software. The problems were attributed to an incompatibility with the anti-virus software installed on the machine and this was subsequently disabled while the upgrade took place. The e-mail was opened before the anti-virus software was re-enabled and many hours were lost in tracking down all occurrences and cleansing machines.

Joined-up working needs joined-up security.

20. Respondents also stated that low awareness of the risks, inadequate staff training and a lack of installed virus prevention and detection measures were the main reasons why infections occurred. Although the majority (77 per cent) stated that the overall impact on their organisation had been low, the average cost of dealing with incidents rose from £1,700 in 1997 to £7,285 in 2000.

21. As organisations share information with partners and develop common systems to work in a joined-up way, the risk of business disruptions increases. Joined-up working needs joined-up security.

Hacking

22. One of the major reasons for the introduction of the Computer Misuse Act 1990 was the increasing number of hacking incidents (Ref. 3). Over ten years later, the risk remains and for all organisations hacking can cause disruption and financial loss [CASE STUDY 2].

23. Most incidents of hacking were caused by poor controls over access to systems and passwords. The increasing availability of password-breaking programs and more powerful personal computers means that the risks of this form of IT abuse are increasing.

24. Whether hacking is undertaken as a prank or a challenge, or whether it is used as a means of committing further abuse such as sabotage – the costs can be high – almost £250,000 for those reported cases or an average of approximately £6,000 per incident. Such figures, however, do not include consequential costs such as the loss of business or customer loyalty.

25. Hacking offences are not always perpetrated by an ‘outsider’ – 40 per cent of hacking incidents were committed by the organisation’s own staff [CASE STUDY 3]. Organisations have used a variety of disciplinary measures such as written and oral warnings, downgrading, transfer to another position and dismissal to enforce the message that such behaviour is unacceptable.

CASE STUDY 2

A Health Authority was the victim of a sophisticated telephone fraud perpetrated by using the dial through feature included with voice mail. This is a practice known as ‘phreaking’. The authority was contacted by BT’s monitoring centre to warn of a dramatic increase in telephone traffic from the authority’s site over the weekend. Investigations were made at the authority which established that a hacker had successfully used the voice mail facility to set up a call forward facility, which was being used to call high-cost telephone services. By using the telephone management and monitoring system, it was established that the hacker was still making calls. The bill for the period has now been received, which includes £7,850 of international calls, some £7,780 of which relate to the fraud.

CASE STUDY 3

In one authority, sound network and access controls were lacking. This allowed a member of staff to access a word processing document that should have been held in another member of staff's personal area. No loss resulted but there was some sensitivity over the breach since the document related to a confidential staff matter.

*...it is
cyber-vandalism
that is a new
risk area.*

Sabotage

26. The term itself conveys an image of physical damage and most of the incidents reported to us in our early surveys in the 1980s were of this type. They are still a threat and can cause widespread disruption to the delivery of services. For example, the failure of some dot com companies and the subsequent staff redundancies have led to the employment of security experts in an attempt to reduce the risk of disgruntled employees sabotaging equipment.

27. Organisations should, therefore, ensure that basic physical and management controls – such as the screening of staff recruited – are not forgotten. But when they are with the dramatic growth of networking and use of the internet, it is cyber-vandalism that is a new risk area [CASE STUDY 4].

CASE STUDY 4

In January 2001 a large Internet company was brought to a standstill for almost a week by a hacker who flooded the company's system with millions of e-mail messages. As a result, the company was unable to distribute e-mails for millions of British users. This act of cyber-vandalism caused major disruption to the company and to its customers.

Reputational damage

Unsuitable material

28. In our last report we identified the downloading and distribution of pornography and other unsuitable material as a new and emerging risk. It continues to be a major cause for concern at all organisations. For many people, e-mail has become the chosen means of communication, and many of these have Internet access. Together, the Internet and e-mail provide widespread availability and ease of distribution of unsuitable material which can threaten an organisation's reputation.

29. Respondents told us about 193 incidents, representing almost one-third of all reported incidents – a significant increase in just three years [CASE STUDY 5].

30. Detecting this type of IT abuse can be difficult. However, there is encouraging evidence that improvements have been achieved. In 1997, almost two-thirds of incidents were discovered by accident. In 2000 that number has halved and proactive prevention measures, such as internal controls and internal audit reviews, detected 60 per cent of the reported cases of this form of IT abuse.

31. There is still room for improvement. More sophisticated monitoring, blocking and filtering software is now available and organisations should consider how best to use it.

32. There is also evidence that organisations are treating the threat of reputational damage seriously. Almost one-half of the perpetrators were dismissed or resigned with the remainder subject to some form of disciplinary procedure including demotion [CASE STUDY 6].

CASE STUDY 5

A routine audit was carried out at a Schools Services Department. This included an examination of PCs and servers to ensure that only licensed software was being used. While carrying out the audit, staff noticed that there were a large number of JPEG files held on a PC. The files were examined and were found to contain pornographic images.

The PC was used by an officer supplying IT support to schools. The local authority has an adequate firewall with associated logs and password security in place. The perpetrator, however, used an independent modem to circumvent the security and login procedures.

Disciplinary procedures were instigated during which the perpetrator resigned.

Organisations need to concentrate their effort on preventing the copying of software by users.

CASE STUDY 6

Ten employees of a major insurance company were dismissed for using e-mail to forward obscene material. The case highlights the growing trend of organisations taking robust action in such cases.

Unlicensed software

33. The theft of software, copying of licensed software without permission, continues to be a risk for all organisations. The ease with which software can be copied and made more widely available means that organisations run the risk of being publicly identified and embarrassed in allowing this form of IT abuse.

34. Respondents gave details of 35 such incidents (6 per cent of all those reported). Associated costs amounted to £70,000 – an average of £2,000 per incident. Organisations need to concentrate their effort on preventing the copying of software by users [CASE STUDY 7].

CASE STUDY 7

A hospital embarked on an IT update programme to replace older equipment and to introduce an information system and workstations to a new group of users.

Workstation licences had been bought in bulk, and at a discount, in the previous year. The workstation licence packs were not issued with machines – hard disks were copied from a reference unit, and licence-manager reports on the servers were ignored or neglected. Internal audit subsequently discovered that the number of workstations in use exceeded the number of licences purchased.

Breach of privacy

35. A feature of our previous surveys has been the impact of IT abuse upon individuals as well as upon organisations. This is particularly relevant in the use of personal information.

36. The implementation of new legislation that aims to increase protection for personal information, and new initiatives for electronic service delivery, which seek to improve information sharing, means that organisations will need to balance carefully these two, seemingly opposing, objectives.

37. While the number of incidents reported remains relatively small, the amount of legislation and regulation in this area is increasing to such an extent that the risk of an inadvertent breach has grown [CASE STUDY 8]

CASE STUDY 8

Healthcare information relating to a patient was unlawfully disclosed by a member of staff to a relative of the patient.

During the course of her authorised duties the member of staff, while accessing the system, noticed that a pathological investigation (with sinister consequences if found to be positive), had been requested on her mother-in-law.

Knowing how concerned her husband was about the condition of his mother, and because of a recent death in the family, she decided to tell her husband.

The following morning the husband rang the consultant and asked about the test and why it had been requested. As the consultant had not discussed the matter with the son or any other member of the family, he requested that the matter be formally investigated.

The investigation found that the security breach was not an act of malicious intent.

Financial loss

Fraud continues to be a major risk for organisations.

Fraud

38. Fraud continues to be a major risk for organisations. The Audit Commission's anti-fraud publications, *Protecting the Public Purse*, show that local government and NHS bodies need to remain vigilant to safeguard their resources (Ref. 4). Increasing automation also means that more frauds are likely to be IT-related.

39. This survey is not intended to define the scale of the problem but to raise awareness by highlighting examples of IT fraud and proposing ways to detect and prevent it.

40. IT fraud involves obtaining gain by:

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

41. Eight per cent of the incidents reported in this survey were frauds, a similar figure to that reported in our last report. The main reasons why the frauds occurred included:

- poor supervision and lack of proper division of duties;
- inadequate control over access to systems; and
- poor authorisation controls.

42. Most IT frauds are committed by employees. Clerical or administrative staff committed almost one-half of the reported incidents and those in managerial positions were responsible for one-third. A small number of perpetrators were temporary or agency staff, which is a reminder that screening procedures must apply to all staff [CASE STUDY 9].

CASE STUDY 9

A local authority officer took advantage of poor controls over computer access to set up, input and authorise fictitious invoices totalling over £15,000. Having built up the trust of his colleagues he would access their unattended terminals when they were out of the office to carry out the various stages of the process (system controls required different users). His actions were detected when routine budget monitoring highlighted significant expenditure against a particular ledger code. The police were notified and the officer was arrested, charged and convicted, receiving a six month custodial sentence. £11,000 was recovered from a police search and £4,000 via council insurance.

System time outs, together with revised instructions for staff to sign out before leaving their desks and increased supervision, were subsequently introduced.

Technology is changing traditional working patterns and practices.

43. Most frauds were detected as a result of information received from ‘whistle-blowers’. A key message from previous reports has been the need for organisations to create an anti-fraud culture, including the development of fraud response plans and whistle-blowing facilities. Many have responded by setting up telephone ‘hotlines’ where staff or members of the public can report suspected fraudulent activities. It is encouraging that the time and energy spent on facilitating whistle-blowing is beginning to pay off.

Private work

44. Technology is changing traditional working patterns and practices. The provision of laptop and hand-held PCs, dial-up facilities, mobile telephones and ‘hot-desk’ arrangements are creating a more flexible working environment for many people.

45. Private use of equipment should be considered as abuse where an employee uses IT facilities for personal commercial gain. Such instances are on the increase, with 72 cases reported in our latest survey [CASE STUDY 10].

46. Organisations must be clear about the level and type of private use that they consider acceptable. The policy should be communicated to all staff, but this is only the starting point. A more mobile workforce can mean that direct supervision of staff becomes more difficult. New ways of working may mean that organisations need to overhaul their monitoring mechanisms. The majority of incidents occurred because of poor supervision and inappropriate access to information systems.

Theft of information

47. While the theft of equipment continues to be a problem for all organisations, the theft of information is potentially more damaging. Fourteen incidents were reported and, while most respondents stated that the impact upon their business had been low, financial losses for these incidents amounted to over £5,500 per case [CASE STUDY 11].

CASE STUDY 10

Two faculty IT support technicians used university IT facilities during the summer when normal activity was minimal to download music from the Internet. They wrote the output onto CDs which were thought to have then been sold, although absolute proof of this was not obtained. The activity was discovered by routine monitoring of exceptional activity over the Internet.

CASE STUDY 11

There were indications that a marketing manager was trying to access information about existing and potential customers. His actions were monitored and it became clear that he was trying to sift business out of the company for his own benefit. He was dismissed. He had copied and stolen commercially sensitive information about actual and potential customers and suppliers. This information was critical to the success of the business and had taken some ten years and hundreds of thousands of pounds to develop.

Erosion of confidence in the use of new technology to deliver services

48. A major consequence of the incidents of IT fraud and abuse described in this report is the reduction of confidence in the facilities that are being used to deliver services. If not addressed, this could cause serious damage to an organisation's reputation.

49. In August 2000, a major retailer was forced to close its Internet service after a customer discovered that he was able to see other shoppers' credit card details on the company's website.

50. This was closely followed by a similar problem at one of the high street banks. Internet customers found that they could gain access to other peoples' accounts. One customer discovered that she could access her own account details even though she had logged off, simply by using the back key on her Internet browser. The latter incident presents real dangers where people share computers, for example, in Internet cafes.

51. Research last year by the National Consumer Council indicated that only 3 per cent of people in the UK regularly shop online because of worries about releasing their credit card details over the Internet. Widely reported security lapses like those outlined above can cause people to be extra cautious about using new technologies.

52. Even though security scares may hamper the speed at which electronic services develop, most projections about Internet-based services are for continuing growth. The findings of this and previous surveys and recent research by others suggests that, unless firm action is taken to address the risks identified, the expansion of electronic services will be matched by an increase in the levels of IT fraud and abuse [TABLE 2, overleaf].

TABLE 2

Key messages in recent reports

A consistent message has emerged from recent reports.

Information Risk Management

(Ref. 5)

New electronic risks are not being managed.

Security is not taken seriously.

Security breaches are increasing.

There has been little change in logical access controls.

There has been a modest improvement in traditional IT security.

Information Security Breaches

Survey 2000 (Ref. 6)

There is little understanding of what can be done to combat the significant risks arising from doing business electronically.

Over 30 per cent do not recognise that their business information is critical.

60 per cent of organisations have suffered a security breach in the last two years.

The most serious breaches, in terms of impact upon the business, were those caused by external unauthorised access.

Some good practices are implemented and adhered to.

yourbusiness@risk

New risks associated with the upsurge in the use of new technologies are not being sufficiently addressed.

Little use is made of risk analysis.

IT fraud and abuse continues to rise.

A failure in basic controls is still a problem.

Organisations have got better at establishing anti-fraud frameworks.

2

The Increasing Risk of IT Abuse

53. There are many textbooks about the controls and safeguards that IT requires. Auditors and security specialists continue to stress the need for proper control and security measures. Nevertheless, the majority of breaches of IT security are still caused by a lack of basic fundamental controls and safeguards.

54. In the past when computing was peripheral to the primary business activities this may have been understandable, but there are drivers for change that demand a radically different approach to IT risk management.

55. These drivers are:

- technology dependency;
- increasing IT literacy;
- the government's technology agenda;
- e-commerce;
- citizen expectations; and
- a rise in e-crime.

Technology dependency

56. Twenty years ago, when our first computer fraud survey was published, IT was in its infancy. Many organisations could function without a keyboard in sight and the use of technology was invariably limited to routine data processing of 'bulk' systems such as payroll and invoicing. The picture today is radically different. The corner shop uses a PC to manage its stock levels; the supermarket's carrier bag displays its web address; and the home-based shopper buys books and CDs from the other side of the world via the TV screen.

57. This change in approach is primarily due to one particular technology – the Internet – which allows individuals and organisations to communicate across local, national and international boundaries and to transmit orders, receive services and make payments as quickly as it takes them to type in instructions – or increasingly to use touch screens and voice input.

58. Respondents to our survey were asked which new technologies they would be using over the next two years and 78 per cent said digital TV and 89 per cent said smartcards. All this points to the rapid growth of technology and its increasing pervasiveness in our lives. We can only speculate on the technologies we shall be using in five years.

59. Despite these new technologies many still fail to recognise that there are risks associated with all developments. While, for example, 98 per cent of respondents now use email, only 51 per cent saw this as presenting a medium-level risk to their organisations, and yet as our survey shows that e-mail provides the means for introducing viruses and unsuitable material into IT systems.

60. Smartcard technology can also provide users with facilities for withdrawing cash, paying for services and receiving a range of benefits, yet only 15 per cent of respondents who will be using smartcards saw them as a high-risk development. As dependency on technology becomes more acute, organisations ignore the risks at their peril.

Increasing IT literacy

61. The national curriculum for schools emphasises the importance of educating children at all stages in the fundamentals of IT. The appreciation and understanding of technology is regarded as fundamental for children from an early age. This will increasingly put pressure on organisations who are failing to recognise that new recruits are arriving with a basic understanding of technology and an expectation that they will be using it to do their job.

The Government's technology agenda

62. IT is high on the government's agenda and there is a requirement for public service organisations to apply technology to improve customer services. Targets have been set for delivering services electronically by 2005 and organisations are being exhorted to use new technologies for the benefit of their customers and service users.

63. While the adoption of IT is to be encouraged, organisations must recognise that risk assessment is not an option: it is an integral part of the development process. UK Online provides a range of examples of innovation by both public and private sector organisations (Ref. 7).

E-commerce

*"It is vital that all of you ... get across the message that if your business doesn't see the Internet as an opportunity, it will be a threat."*¹

64. E-commerce is undoubtedly expanding. A Cabinet Office report argued that the contribution of e-commerce to the UK economy will become significant (Ref. 8). The Internet offers significant attractions and opportunities [BOX B].

¹ Tony Blair, Prime Minister interviewed by *Computer Weekly* 21 October 1999.

BOX B**Attractions of the Internet****Access to worldwide data**

- ever-growing wealth of readily-accessible data

Widespread availability

- web access through high-street Internet cafés
- home PCs
- WAP phones

Ease of use

- browsing the Internet
- buying on the Internet
- home-banking

Browse and search

- fast searching for business critical data

Availability of software

- shareware
- download upgrades of software from the Internet

Messaging

- easy creation of web addresses for e-mail

Accessing corporate systems

- Internet technologies used to create intranets & provide same 'look and feel'
- ability to access internal systems remotely via web technologies

Source: Audit Commission

65. UK Online says that 'ninety per cent of UK employees now work in businesses that are connected to the Internet – on a par with the US at ninety three per cent. Thirty three per cent work in UK businesses that engage in online financial transactions with customers or suppliers – a higher proportion than the USA, Sweden, Germany, France, Japan or Canada' (Ref. 7).

66. Retail organisations see their websites as a means of increasing business opportunities and others are beginning to recognise the financial benefits and efficiency gains that result from ordering goods and making payments electronically.

The key feature about the Internet is not that it necessarily presents new risks – rather it provides new and better opportunities for abuse.

67. Respondents were asked what business use they were and would be making of the Internet. The answers illustrate the shift to e-commerce but highlight, too, the perceptions of the risks presented by such a move [TABLE 3].

68. If e-commerce is to be a successful way of doing business then organisations will need to install processes that ensure the confidentiality, completeness and accuracy of all electronic transactions. Evidence from the last 20 years suggests that this is unlikely to happen. But while organisations may have managed to avoid installing effective security processes in the past, they cannot avoid such responsibilities in the future. The risk will no longer be restricted to the organisation: every Internet user worldwide becomes a potential hacker to the system, unless the organisation satisfies itself that it has measures in place to block unauthorised access.

69. The key feature about the Internet is not that it necessarily presents new risks – rather it provides new and better opportunities for abuse. The safeguards are fundamentally the same, but they need to be updated to counter these new opportunities. Box C highlights examples of the risks and the safeguards available [BOX C].

TABLE 3

e-commerce activity

The increasing use and higher risks of the Internet.

Activity	Use now	Use in future	Percentage of respondents		
			High risk	Medium risk	Low risk
Procure goods/services	36%	59%	28%	41%	23%
Make payments	17%	71%	43%	33%	18%
Receive income	11%	78%	41%	34%	18%

BOX C**Internet risks & safeguards**

The risks and the safeguards available

Risks	Safeguard
Creating the spoof organisation – setting up a dummy organisation on a web page & inviting orders for non-existent services/goods.	Apply business acumen to over-attractive offers.
Getting access to business critical data.	Control access to systems and information.
Viewing inappropriate material.	Use software to restrict access to nominated sites.
Distribution and/or receipt of inappropriate text, video and image files.	Use software to restrict size and type of files e-mailed in to and out from the organisation.
Download unauthorised software.	Use software to inhibit downloading of program and other specified files.
Introduction of viruses.	Use software to inhibit downloading of programs and other specified files and use virus-checking software.

Citizens' expectations

70. With more personal data now being held on computers, individuals have a right to expect that such data is secure. As more services are provided electronically and personal details are transmitted across the Internet, the risk of misuse, whether deliberate or accidental, increases.

71. People are being more vocal in demanding high-quality services, including the protection of personal data. Failure in this area attracts media attention and damages the reputations of organisations. Assurance is needed that:

- an individual's bank account details will not be disclosed to others, and, similarly, that they will be denied access to others' accounts; and
- sensitive personal data relating, for example, to the provision of and need for education, care services, and social conditions is only available on a need-to-know basis.

Rise in e-crime

72. Crime committed electronically, or cyber-crime, is increasing and is attracting the interest of governments. Research by the Foresight Crime Prevention Panel suggested that (Ref. 9):

‘new technology now and in the future might also create more opportunity for crime by:

- providing easier access to systems, premises, goods and information;
- removing geographical obstacles to crime;
- increasing the scale of potential rewards; and
- increasing anonymity in committing crime or consuming its proceeds.’

73. It went on to recommend that a national e-crime strategy be established for all levels of e-crime.

74. The global aspect of this problem has been highlighted, too, by the Council of Europe in its draft Convention on Cyber-crime, the first international treaty to address e-crime and IT abuse (Ref. 10). The draft provides for the co-ordinated criminalisation of a range of e-crimes, including computer hacking and hacking devices, illegal interception of data and interference with computer systems and computer-related fraud and forgery.

3

Prevention is Better than Cure

Why incidents happened

75. One of the main objectives of our survey has been to identify what lessons can be learned from the details of the reported incidents [TABLE 4].

TABLE 4

Why incidents are possible

The top ten reasons show a continued failure of basic controls and housekeeping procedures.

	Percentage of incidents reported
Poor supervision of staff	19
Inadequate controls over access to information systems	13
Inadequate or insufficient training	13
Few checks on data from other sources	11
Lack of Internet activity monitoring	11
Virus detection and prevention software not installed	9
Inadequate firewall	8
Transactions not traceable to individuals	7
Poor password control	6
Lack of clarity over security responsibilities	5

Source: Audit Commission

Most targeted systems

76. The number of staff disciplined for e-mail and Internet abuse has risen sharply over the last year according to reports by the Industrial Society (Ref. 11). Predictably, the information systems and facilities that were most affected by the abuse reported to us were PCs, e-mail systems and websites [BOX D].

Measures to prevent IT abuse

77. A conclusion common to all previous reports has been that IT abuse often happens because of a lack of basic internal controls – for example, inadequate division of duties or supervision by senior members of staff. Our survey shows little improvement in this area.

78. Poor management and personnel controls, as well as checks over information systems, were the most frequently mentioned reasons behind incidents. A lack of IT based controls, such as the installation of virus detection and activity monitoring software, were also regularly mentioned.

79. The predicted increase in electronic service delivery means that all organisations should give serious consideration to the effectiveness of their basic IT management controls. This is essential if the risks associated with IT abuse are to be minimised.

BOX D

The top ten systems and facilities most affected by IT abuse

PCs, e-mail systems and websites were most affected by the abuse reported.

1. e-mail
2. Desktop systems
3. Website
4. Administrative information system
5. Personal records
6. System software
7. Telephone system
8. Human Resources
9. Creditor payments
10. Accounting

Source: Audit Commission

80. There are tried and tested preventative measures that are common sense and are relatively easy to apply – if management has the will [TABLE 5]. At the other end of the spectrum there will be more complex and expensive measures that some organisations will need to apply to meet their particular business needs. Whatever the nature of the controls and safeguards, the driver for identifying the need for better security will be the nature of the risks that the organisation faces. Surprisingly – and disappointingly – our last two surveys show only one-third of organisations regard regular risk analysis reviews as a necessary contribution to the prevention of IT fraud and abuse.

81. Preventative measures fall into three main categories:

- security ethos;
- policies and protocols; and
- review processes.

TABLE 5

Preventative measures

There are well used preventative measures that are common sense and are relatively easy to apply.

Preventative measure	Percentage of respondents applying these measures
Security ethos	
Internal audit	86%
Computer audit skills	52%
Computer security awareness training	34%
Computer security staff	30%
Policies and protocols	
Up-to-date security policy	78%
Encouraging whistle-blowing	58%
Anti-fraud/corruption policy	47%
Ethics policy	32%
Review processes	
Regular reviews of computer security	66%
Logging and security breaches	65%
Regular personnel screening	11%

Security ethos

82. Top management should be seen to be taking IT security seriously and should create an awareness of security issues among staff. IT security is not a one-off exercise for the auditor or security officer: it has to involve management and staff at all levels. But few organisations apply this principle in practice – 66 per cent of respondents offer no computer security awareness training for their staff.

83. While it is encouraging that nearly 90 per cent of respondents employ internal auditors, only 52 per cent have staff with computer audit skills and only one-third have computer security staff. Given the technology dependency of organisations, and the need to identify and install effective security processes, it is critical that organisations have access to people with the necessary skills to address these concerns.

Policies and protocols

84. The national standard on information security – ISO/IEC 17799 (formerly known as BS7799) – provides a basis for assessing an organisation's IT security procedures (Ref. 12). The adoption of this standard has fallen since the last survey (only 15 per cent said that their organisation complied with the standard, against 19 per cent in 1997). Disappointingly, 70 per cent were not seeking BS7799 certification and the most frequently given reason was that it was not a business priority. Not enough attention is being given to IT security [BOX E].

85. If staff are to be made aware of the dos and don'ts then practical and easily readable IT security policies and protocols must be widely available, and around three-quarters of respondents said that they had an up-to-date security policy.

86. There is some evidence that organisations are beginning to pay more attention to the development of anti-fraud strategies and the implementation of appropriate arrangements to support them – for example, whistle-blowing facilities. About 20 per cent of incidents were discovered as a result of information received from whistle-blowers.

BOX E

Organisations not seeking ISO/IEC 17799 accreditation

The adoption of this standard has fallen since the last survey from 19 per cent to 15 per cent of organisations responding.

Reason for not seeking ISO/IEC 17799 accreditation

- not a business priority
- no knowledge of BS7799
- no knowledge of BS7799 certification
- no skills/resources in this area
- too expensive
- no top management support

Review of IT security procedures and processes

In too many cases, the first time an organisation becomes aware that it has been the target of IT abuse may be when an incident happens.

87. In too many cases, the first time an organisation becomes aware that it has been the target of IT abuse may be when an incident happens. For example, a virus infection may remain undetected until a particular process fails. Over one-third of the incidents reported to us were discovered either in this way or by accident.

88. About one-half of the incidents were detected as a result of internal controls and the activities of audit and security staff. All of these methods of detection are proportionally similar to our previous survey.

89. The regular review and updating of IT security procedures and processes and the application of these on a day-to-day basis does help to reduce the risk of IT abuse. Yet less than two-thirds of respondents have installed processes to regularly review their IT security arrangements and a similar number have failed to establish procedures to log and report breaches of security. Without such processes in place it is difficult to see how organisations can monitor the effectiveness of their IT security safeguards.

90. With the evidence showing that staff commit the largest number of cases of IT abuse it is disappointing that only 11 per cent of respondents undertake regular personnel screening. There have been examples of false CVs and professional certificates being produced to support job applications and desktop computing provides individuals with a quick and easy way of forging such material. If organisations fail to recognise that achieving a secure environment needs reliable and trustworthy staff then there is every likelihood that IT abuse will continue to thrive.

91. Given the high incidence in our survey of cases of accessing inappropriate material on the Internet, it is not surprising that preventative measures relating to Internet activity were poorly applied – around 25 per cent carried out no Internet activity monitoring and a little less than one-half of respondents failed to monitor e-mail activity. With an anticipated increase in e-commerce this bodes ill for the future. It suggests that organisations that are relaxed in controlling such Internet activity are unlikely to be concerned about Internet access more generally and so put their business activities at risk [TABLE 6, overleaf].

TABLE 6

Controlling Internet activity

Preventative measures relating to Internet activity were poorly applied.

Preventative measure for controlling Internet activity	Percentage of respondents applying these measures
Monitor Internet activity	76%
Monitor e-mail activity	53%
Bar access to specified sites	53%
Review out-of-hours web access	30%
None	7%

There must be a reliable and secure IT network underpinning Internet use.

92. As access to systems and use of services becomes more automated, so the identification and authentication processes will need to be integral elements of the new technology. Organisations will need to consider cryptography and other related techniques to ensure that users are properly identified and that their access rights and restrictions are effectively monitored and controlled.

93. There must be a reliable and secure IT network underpinning Internet use. If the network is not fully protected then the organisation will undoubtedly face major risks and may well find itself unable to survive. The network infrastructure must:

- be resilient,
 - capable of providing a 24 hours a day, seven days a week service;
 - capable of maintaining a service when power failures occur;
- identify users,
 - prevent unauthorised access attempts; and
- monitor activity;
 - report unusual occurrences.

94. The application of the IT security measures that are set out in this report will help all organisations to meet the risks and challenges that they face as the dependency upon IT increases.

References

1. Audit Commission, *Ghost in the Machine – An Analysis of IT Fraud and Abuse*, Audit Commission, February 1998.
2. Audit Commission, *Opportunity Makes a Thief – An Analysis of Computer Abuse*, HMSO, 1994.
3. *The Computer Misuse Act 1990*, HMSO 1990.
4. Audit Commission, *Protecting the Public Purse – Ensuring Financial Probity in Local Government*, Audit Commission, January 2001.
Audit Commission, *Protecting the Public Purse – Ensuring Probity in the NHS*, Audit Commission, December 1999.
5. National Consumer Council, *Information Risk Management – E-Commerce and Consumer Protection*, National Consumer Council, August 2000.
6. Department of Trade and Industry, *Information Security Breaches Survey 2000*, DTI, April 2000.
7. UKonline.gov.uk UK Online Annual Report, Ukonline.gov.uk, September 2000.
8. Performance and Innovation Unit, *e-commerce@its.best.uk*, Cabinet Office, September 1999.
9. Foresight Crime Prevention Panel, *Turning the Corner*, Foresight Crime Prevention Panel, December 2000.
10. Council of Europe, *Draft Convention on Cyber-crime*, Council of Europe, 2000.
11. The Industrial Society, Quote, *Daily Telegraph*, January 2001.
12. ISO, *ISO 17799: Code of Practice for Information Security Management*, ISO, November 2000.

yourbusiness@risk

Self assessment checklist

Please pull out and copy

In its update, *yourbusiness@risk*, the Audit Commission has identified the risks from IT fraud and abuse facing organisations.

These risks have been drawn together into a series of questions included in this pull-out checklist. Managers are invited to complete the checklist as an aid to assessing their organisation's current position.

Business disruption as a result of...	Yes	No
VIRUS INFECTION		
This organisation takes the threat of a virus infection very seriously.	<input type="checkbox"/>	<input type="checkbox"/>
Virus detection and prevention software is installed on all machines.	<input type="checkbox"/>	<input type="checkbox"/>
Virus detection and prevention software is regularly updated.	<input type="checkbox"/>	<input type="checkbox"/>
All staff have clear instructions about sweeping disks from external sources to check for viruses.	<input type="checkbox"/>	<input type="checkbox"/>
All staff have clear instructions about dealing with e-mailed files from external sources.	<input type="checkbox"/>	<input type="checkbox"/>
Security software has been installed that prevents externally e-mailed files containing program or suspect files from getting beyond the organisation's firewall.	<input type="checkbox"/>	<input type="checkbox"/>
Staff are alerted when new viruses are discovered and are provided with clear instructions as to what they must and must not do.	<input type="checkbox"/>	<input type="checkbox"/>
Guidance to staff on the risks from viruses is reviewed and updated on a regular basis.	<input type="checkbox"/>	<input type="checkbox"/>
This organisation makes it clear to all staff that use of unauthorised software is prohibited.	<input type="checkbox"/>	<input type="checkbox"/>
There are clear procedures in place for reporting a virus incident.	<input type="checkbox"/>	<input type="checkbox"/>
Procedures for recovering from a virus infection have been documented.	<input type="checkbox"/>	<input type="checkbox"/>
HACKING		
Proper user registration and sign-on procedures prevent unauthorised access to networks.	<input type="checkbox"/>	<input type="checkbox"/>
Proper password management is enforced by the system on all users.	<input type="checkbox"/>	<input type="checkbox"/>
Dial-up connections are secure.	<input type="checkbox"/>	<input type="checkbox"/>
Network management and security responsibilities are clear.	<input type="checkbox"/>	<input type="checkbox"/>
A detailed daily log of network activity is maintained and inspected regularly.	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive programs and information are given additional protection.	<input type="checkbox"/>	<input type="checkbox"/>
Any violations are reported immediately.	<input type="checkbox"/>	<input type="checkbox"/>

Business disruption as a result of (cont.)...	Yes	No
SABOTAGE		
Physical entry controls inhibit unauthorised access.	<input type="checkbox"/>	<input type="checkbox"/>
Equipment is sited securely and adequate protection is offered.	<input type="checkbox"/>	<input type="checkbox"/>
Positive action has been taken to minimise the opportunity for sabotage of IT systems by employees leaving the organisation.	<input type="checkbox"/>	<input type="checkbox"/>
Line managers are fully aware of the ways in which hardware, software and data can be damaged.	<input type="checkbox"/>	<input type="checkbox"/>
There are clear rules governing out-of-hours working to guard against unsupervised use or abuse of systems.	<input type="checkbox"/>	<input type="checkbox"/>
Unauthorised personnel are prevented from gaining access to any secure or sensitive area by physical entry controls.	<input type="checkbox"/>	<input type="checkbox"/>
Any amendment to a program or system must go through a rigorous change control process.	<input type="checkbox"/>	<input type="checkbox"/>
Backups of data and programs are taken frequently.	<input type="checkbox"/>	<input type="checkbox"/>
Backup arrangements are properly documented.	<input type="checkbox"/>	<input type="checkbox"/>
Remote monitoring of backup processes ensures that management is alerted when backups do not take place for whatever reason.	<input type="checkbox"/>	<input type="checkbox"/>
This organisation has set out a clear business continuity plan.	<input type="checkbox"/>	<input type="checkbox"/>
All staff involved in the operation of the business continuity plan know of its existence and their part in its delivery.	<input type="checkbox"/>	<input type="checkbox"/>
Reputational damage as a result of...	Yes	No
ACCESSING UNSUITABLE MATERIAL		
All Internet connections must be approved by the central IT unit.	<input type="checkbox"/>	<input type="checkbox"/>
There are effective security measures in place to ensure that outsiders cannot gain access to this organisation's networks via their Internet connection.	<input type="checkbox"/>	<input type="checkbox"/>
Records of Internet sites visited are reviewed regularly by managers.	<input type="checkbox"/>	<input type="checkbox"/>
Staff have been made aware of specific sites to which access is prohibited.	<input type="checkbox"/>	<input type="checkbox"/>
It has been made clear to all staff that the downloading of unsuitable material from the Internet is a disciplinary matter.	<input type="checkbox"/>	<input type="checkbox"/>
An effective firewall protects internal networks, systems and information from intrusion from outside.	<input type="checkbox"/>	<input type="checkbox"/>
Firewall software prevents prescribed data such as very large files; executable programs from reaching internal networks.	<input type="checkbox"/>	<input type="checkbox"/>
Protocols for e-mail use have been designed and circulated to all users.	<input type="checkbox"/>	<input type="checkbox"/>

Reputational damage as a result of (cont.)...	Yes	No
UNLICENSED SOFTWARE		
Staff have been made fully aware that it is an offence to use unlicensed software.	<input type="checkbox"/>	<input type="checkbox"/>
This organisation has installed security software that would prevent the loading of any unauthorised programs.	<input type="checkbox"/>	<input type="checkbox"/>
Internal Audit undertake thorough reviews of software on users' PCs.	<input type="checkbox"/>	<input type="checkbox"/>
Access to system utilities is controlled and restricted to system software staff.	<input type="checkbox"/>	<input type="checkbox"/>
Use of system utilities is logged and independently reported to management.	<input type="checkbox"/>	<input type="checkbox"/>
Unnecessary utilities are removed or disabled.	<input type="checkbox"/>	<input type="checkbox"/>
MISUSE OF PERSONAL DATA		
Sensitive information passing over the network is encrypted.	<input type="checkbox"/>	<input type="checkbox"/>
PCs are timed out and screen savers are password protected.	<input type="checkbox"/>	<input type="checkbox"/>
Enforced path for users prevents access to system facilities.	<input type="checkbox"/>	<input type="checkbox"/>
Staff understand fully their responsibilities under the Data Protection Act.	<input type="checkbox"/>	<input type="checkbox"/>
Systems which use personal data are registered with the Data Protection Commissioner.	<input type="checkbox"/>	<input type="checkbox"/>
Any misuse of personal data is treated as a disciplinary offence.	<input type="checkbox"/>	<input type="checkbox"/>
All users of IT facilities are required to sign a confidentiality (ie non-disclosure) undertaking as part of their conditions of employment.	<input type="checkbox"/>	<input type="checkbox"/>
This organisation has appointed a data protection officer.	<input type="checkbox"/>	<input type="checkbox"/>
BREACH OF THE LAW		
Staff have been briefed upon the implications of the:		
Data Protection Act.	<input type="checkbox"/>	<input type="checkbox"/>
Computer Misuse Act.	<input type="checkbox"/>	<input type="checkbox"/>
Freedom of Information Act.	<input type="checkbox"/>	<input type="checkbox"/>
Human Rights Act.	<input type="checkbox"/>	<input type="checkbox"/>
Public Interest Disclosure Act.	<input type="checkbox"/>	<input type="checkbox"/>
Financial loss as a result of...	Yes	No
FRAUD		
There is a clear anti-fraud strategy.	<input type="checkbox"/>	<input type="checkbox"/>
The systems that are most at risk from fraud have been identified.	<input type="checkbox"/>	<input type="checkbox"/>
Special priority is given to regularly testing those information systems considered to be at risk.	<input type="checkbox"/>	<input type="checkbox"/>
The risk of IT fraud has been significantly reduced by segregating duties within key systems areas.	<input type="checkbox"/>	<input type="checkbox"/>

Financial loss as a result of (cont.)...	Yes	No
The risk of IT fraud has been reduced by ensuring that IT development work and day-to-day systems operations are kept separate.	<input type="checkbox"/>	<input type="checkbox"/>
There is a clear and stringent access control policy which limits access to data and systems to those who need it.	<input type="checkbox"/>	<input type="checkbox"/>
PRIVATE WORK		
All staff have been told explicitly what is and what is not acceptable.	<input type="checkbox"/>	<input type="checkbox"/>
THEFT		
Unauthorised access to this organisation's premises is prevented by sound security measures.	<input type="checkbox"/>	<input type="checkbox"/>
There are program controls in place to limit access to information and software on a need-to-know basis.	<input type="checkbox"/>	<input type="checkbox"/>
Access controls are reviewed regularly.	<input type="checkbox"/>	<input type="checkbox"/>
There are tight controls to prevent the illicit copying or removal of software.	<input type="checkbox"/>	<input type="checkbox"/>
Hardware is clearly security-marked.	<input type="checkbox"/>	<input type="checkbox"/>
Loss of user confidence	Yes	No
There is an information security policy.	<input type="checkbox"/>	<input type="checkbox"/>
The policy is kept up-to-date.	<input type="checkbox"/>	<input type="checkbox"/>
Employees with responsibility for information security have a copy of the policy.	<input type="checkbox"/>	<input type="checkbox"/>
Staff are informed about the policy and what they must and must not do.	<input type="checkbox"/>	<input type="checkbox"/>
Top management is committed to the policy and its observance.	<input type="checkbox"/>	<input type="checkbox"/>
An effective security management framework has been established to manage the implementation of information security.	<input type="checkbox"/>	<input type="checkbox"/>
Information security responsibilities are clear and allocated to named individuals.	<input type="checkbox"/>	<input type="checkbox"/>
Owners of systems have been made responsible and accountable for security.	<input type="checkbox"/>	<input type="checkbox"/>
Regular independent reviews of information security are undertaken.	<input type="checkbox"/>	<input type="checkbox"/>
This organisation complies with international security standards.	<input type="checkbox"/>	<input type="checkbox"/>
There are clear written procedures for reporting and following up all security incidents.	<input type="checkbox"/>	<input type="checkbox"/>
Inventories of all IT assets are maintained.	<input type="checkbox"/>	<input type="checkbox"/>
Conditions of employment are clear about security dos and don'ts.	<input type="checkbox"/>	<input type="checkbox"/>
All users of secure web based services eg. web payments must go through an effective authentication and authorisation procedure.	<input type="checkbox"/>	<input type="checkbox"/>

Further copies are available from:

Audit Commission Publications

PO Box 99

Wetherby

LS23 7JA

Telephone: 0800 502030

STOCK CODE: LUP1834

£10.00 net

