

Public sector

Update

June 2005



ICT fraud and abuse 2004

An update to *yourbusiness@risk*

The Audit Commission is an independent body responsible for ensuring that public money is spent economically, efficiently and effectively, to achieve high-quality local and national services for the public. Our remit covers more than 12,000 bodies in England, which between them spend £100 billion of public money each year. Our work covers local government, housing, health, community safety and fire and rescue services.

As an independent watchdog, we provide important information on the quality of public services. As a driving force for improvement in those services, we provide practical recommendations and spread best practice. As an independent auditor, we monitor spending to ensure that public services are good value for money.

For further information on the work of the Commission please contact:

Audit Commission, 1st Floor, Millbank Tower, Millbank, London SW1P 4HQ Tel: 020 7828 1212

For additional copies of Audit Commission reports please contact:

Audit Commission Publications, PO Box 99, Wetherby LS23 75A Tel: 0800 502030

Summary	2
Introduction	4
Survey results and key conclusions	9
Preventing ICT abuse	26

© Audit Commission 2005

First published in June 2005 by the Audit Commission for local authorities and the National Health Service in England, 1st Floor, Millbank Tower, Millbank, London SW1P 4HQ

ISBN 186240 507 7

Photograph: Getty Images

Summary

The Audit Commission has reported on the incidence of information and communication technology (ICT) abuse in the UK regularly since its creation. Our reports are based on surveys of both the public and private sectors and provide a snapshot of the level of ICT abuse, the reasons why it occurs and the risks that organisations need to address.

Over the past 24 years, the trend in incidents suggests that ICT abuse continues to be a threat. While new types of incident have arisen over the lifetime of our surveys, frauds, viruses and accessing inappropriate material on the internet now present the greatest risks to organisations.

Organisations have improved their ICT governance arrangements:

- 96 per cent of organisations have developed ICT security policies;
- 82 per cent now employ email filtering; and
- 85 per cent now employ staff with specific ICT security responsibilities.

But there is less evidence of commitment to providing users with robust guidance and unambiguous statements about their responsibilities:

- only half of the organisations surveyed have initiated ICT security awareness training;
- only one-fifth of staff have been provided with a copy of their organisation's ICT security policy;
- only one-third of staff have been informed about the policy and what they must and must not do; and
- only one-third of staff know where to find written procedures for reporting a security incident.

ICT security is only as effective as the staff within the organisation and failure to communicate to users their responsibilities has led to:

- a significant increase in inappropriate use of the internet and email (despite around three-quarters of respondents scoring the accessing of the web and email as medium to low risks);
- virus infections continuing to represent a major risk; and

- ICT fraud still being committed across all organisations.

Organisations still appear to be complacent about the risks of newer technologies:

- two-thirds regard wireless technology as being a medium to low risk; and
- three-quarters regard PDAs as only medium to low risk.

Organisations must emphasise to their staff the need for secure use of ICT. Given the continuing expansion of ICT throughout public services, management must do more to make staff aware of their responsibilities and ensure that their organisation provides an environment in which ICT security is recognised as essential to effective business processing.

There is no doubt that despite the best endeavours of organisations and their security staff, auditors and managers, ICT abuse will continue to thrive. As this report shows, fraud, virus attacks and inappropriate use of ICT are the most common forms of abuse across public services. Many organisations have responded to the range of risks they face by deploying more preventative measures, but there is still an alarming minority that fails to protect its information assets, whether through complacency or ignorance of risks.

Despite the increased sophistication of preventative measures, though, there is no evidence to suggest that ICT abuse will diminish before our next review is due. More must be done to help avoid an increase in risks by protecting public service information that relies upon technology for its safekeeping and security.

Good governance relies upon sound internal processes to protect corporate data. To help in focusing attention on ICT governance we have included some key questions that we believe all chief executives should ask of their organisations.

For our part, we shall pursue an ongoing review of organisations' responses to this report. We will help to highlight weaknesses and emphasise the need for constant attention to the reduction of ICT abuse in public services.

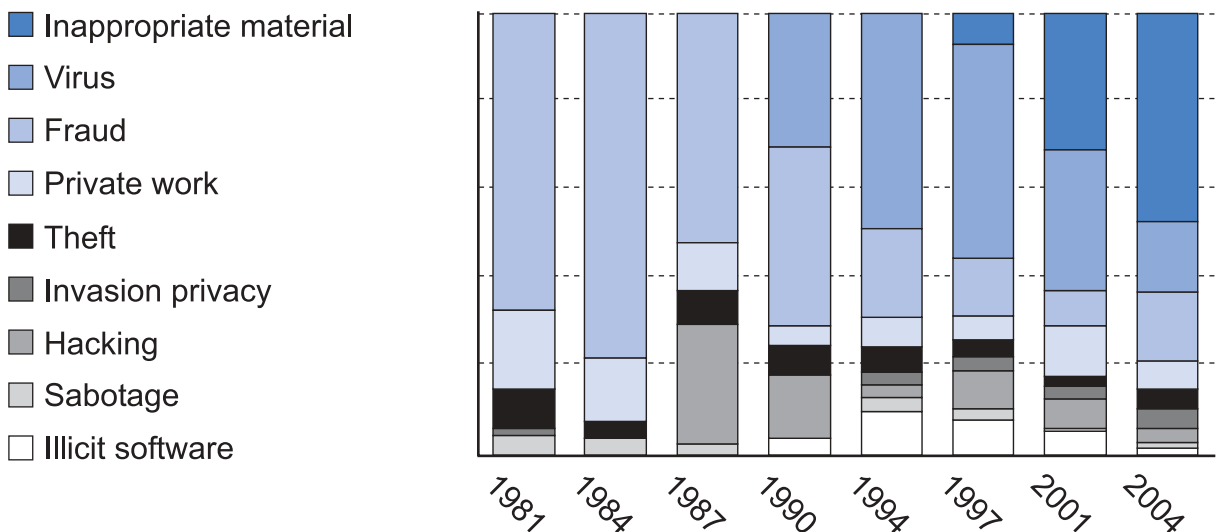
Introduction

- 1 While the benefits of technology are widely accepted, the risks are often less well appreciated. Publicity around the failures of high-profile ICT developments provide ample evidence of what can go wrong when ICT systems are poorly defined, badly managed or ineffectively developed. Deliberate acts of ICT abuse, as with all white-collar crime, are less apparent. The risks remain significant (**Figure 1**).

Figure 1

Incidents of ICT abuse

ICT abuse continues to be a threat.



Source: Audit Commission

- 2 In 1981, the Local Government Audit Inspectorate published the first UK report on computer fraud and abuse and it created widespread interest both in the UK public and private sectors 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 and the last report, *yourbusiness@risk*, published in September 2001, concluded that:

- organisations had got better at establishing anti-fraud frameworks, cultures and strategies but failures in basic controls were still a problem;
 - new risks associated with the upsurge in the use of new technologies had not been sufficiently addressed, ICT abuse continued to rise and respondents to the survey generally felt more vulnerable in their use of ICT;
 - business disruptions had grown and reputational damage was emerging as a significant threat;
 - financial losses and associated costs remained high; and
 - confidence in the technologies that were influencing the way we lived and worked was being eroded.
- 4 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 those public services that are audited and inspected by the Commission. The surveys provide valuable information, comparative data and practical advice, which managers in other sectors will find helpful.
- 5 We have also updated the self-assessment tool provided with the last report.
- 6 To inform this latest report, an online survey was made available to: local authorities, police and fire authorities, housing associations, NHS bodies, universities, central government departments, non-departmental public bodies (NDPBs) and agencies.
- 7 This report is based on responses from 407 organisations from which there were 200 reported cases of ICT fraud and abuse. All of these occurred during the last three years – that is, 2001 to 2004. Although the response rate was lower than our last survey in 2001, it still represents some 18 per cent of the public service bodies invited to participate, with 46 per cent of those responding reporting one or more incidents.
- 8 As media attention and evidence from the wider business community has identified new forms of ICT misuse so we have extended the scope of our surveys. For example, when we undertook our first survey in 1981, viruses and hacking were unheard of. We have had to extend the areas that our surveys cover to include new forms of abuse, such as invasion of privacy, use of unlicensed software and the accessing of inappropriate material. For the latest survey we extended our definition of 'virus infections' to include 'denial of service' (**Box A**).

Box A

ICT abuse: definition of incidents

Virus/denial of service

Distributing a program with the intention of corrupting a computer process or of denying access to ICT facilities that overcomes controls to infect an organisation's systems.

Accessing pornographic/inappropriate material

Introducing pornographic, racist or other inappropriate material via ICT facilities, for example, through email or internet access.

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 an ICT process by causing deliberate damage to a processing cycle or to equipment.

Source: Audit Commission

Continuous assessment since *yourbusiness@risk* survey

- 9 The Audit Commission's 2001 report concluded that though organisations have got better at establishing anti-fraud frameworks, cultures and strategies, failures in basic controls were still a problem and the upsurge in the use of new technology had not been sufficiently addressed.
- 10 Following that report, the Audit Commission developed an online self-assessment tool (YBAR) that was designed to help organisations to:
 - raise awareness of the risks associated with their increasing use of technology;
 - gauge the level of knowledge within their organisations of such risks;
 - measure improvement;
 - highlight areas where risks are greatest; and
 - facilitate positive action to reduce risks.
- 11 The audience for the assessment tool was executive directors, members of management teams, senior managers, heads of service and frontline or ICT members of staff.
- 12 Over 20 local authorities and NHS bodies in England and Wales and over 3,700 individuals have used this tool over the past three years. Their responses, together with the results of the Audit Commission's latest survey, have been brought together and analysed for this report to highlight the key messages for management in public service organisations. Throughout this report we refer to these responses in boxes titled 'YBAR online survey'.

Other research

- 13 We have also taken account of other research and fraud investigation work undertaken in the public and private sectors: HM Treasury's published Fraud Reports provide an analysis of reported fraud in government departments and NDPBs. The NHS Counter Fraud and Security Management website provides details of cases investigated throughout the NHS.
- 14 Our previous surveys have included responses from private sector organisations. For this survey, the primary target audience was the wider public sector. We have, however, drawn on the results of other national surveys conducted throughout the private sector at

around the same time. These included the Information Security Breaches Survey 2004, carried out by PricewaterhouseCoopers for the DTI, and the Survey of Information Security Policy and Practice 2004, published by the National Computing Centre.

- 15 The Financial Services Authority report, *Countering Financial Crime Risk in Information Security* (November 2004), was also reviewed.
- 16 The Audit Commission is grateful to HM Treasury and Audit Scotland for their help in bringing the initiative to the attention of the public bodies in their respective areas. The table below shows the number of organisations and types of public sector body that responded to our survey, together with their percentage share of reported incidents (**Table 1**).

Table 1
Survey responses

We received a good spread of responses from across the public sector.

	Number of organisations	% of reported incidents 2004
Local government, fire and police	119	39%
Health	86	16%
Housing	49	4%
Higher education	30	3%
Central government departments and agencies	61	20%
NDPBs	62	18%
Total	407	100%

Source: Audit Commission

2

Survey results and key conclusions

- 17 Deliberate acts of abuse continue across the breadth of public services. ICT-related fraud and other forms of ICT abuse are still in evidence in the results of our latest survey but as with other recent national surveys, the overriding message is that ICT-related fraud occurs less often than other forms of reported abuse. By far the two most common forms of abuse that affect organisations across the public and private sectors are virus infections and inappropriate use of ICT facilities by staff.
- 18 Following the pattern set by the *yourbusiness@risk* report, we have categorised incidents under three main headings (**Table 2**).

Table 2

We categorised incidents under three main headings

The form of abuse reported most often is accessing inappropriate material.

	% of incidents 2004	% of incidents 2001
Business disruption		
Virus infections/denial of service	16	32
Hacking	3	6
Sabotage	1	1
Reputational damage		
Inappropriate material	47	31
Invasion of privacy	4	3
Using unlicensed software	1	5
Financial loss		
ICT-related fraud	16	8
Using ICT facilities for private work	7	12
Theft of information or software	5	2
Total	100	100

Source: Audit Commission

- 19 We have included some key questions for each type of incident that chief executives should ask in order to satisfy themselves that their organisations are mitigating the risk from these forms of abuse.

Business disruption

Virus infections/denial of service

- 20 Virus infections remain a major form of abuse that can lead to the disruption of day-to-day business activities. While the proportion of reported incidents is lower than in previous years, it remains in the top three at 16 per cent. This is consistent with the results of other national UK surveys.
- 21 This form of abuse is, largely, self-inflicted – not because employees deliberately create malicious software to cause disruption but rather because organisations fail to prevent such software being introduced. Our previous reports have highlighted why such incidents occurred – that is, low awareness of the risks and inadequate staff training together with a lack of installed virus prevention and detection measures. In the past, transmission of a virus was helped to a large extent by the exchange of infected disks. New and more invasive viruses continue to be developed and distributed on a worldwide basis. The majority are introduced by internet access and email systems. Current experience suggests that organised crime commonly uses viruses to cause denial of an ICT service.
- 22 When asked how respondents rated the disruption to their day-to-day activities caused by virus infections, 42 per cent gave a medium to high score, suggesting that the work involved in recovering from such incidents is not trivial.
- 23 Respondents were asked in the survey what preventative measures their organisations employed to minimise the risk of virus infection. All replied that they used virus prevention software and yet the primary reason for virus infections was seen to be ineffective virus protection facilities, followed by a failure to communicate the need for more vigilance by staff.
- 24 As more data is distributed electronically and on easy to use media, such as CD/DVDs, USB drives and PDAs, the opportunity to spread viruses increases.

YBAR online survey

The evidence of the YBAR online surveys highlighted that:

- 20 per cent of users said that their organisation had suffered a virus infection;
- 93 per cent said that their organisation took the threat of a virus infection seriously; and
- 94 per cent had virus protection software installed on their PCs.

However, one-third had no clear instructions for dealing with emailed files from external sources and over a quarter were not sent alerts when new viruses were discovered or told what to do and what not to do.

Source: Audit Commission

- 25 The YBAR results emphasise that more needs to be done to minimise the risk of virus infections. A virus attack may not be trivial nor easily resolved – particularly where the objective is malicious and the infection widespread. As the YBAR results highlight, users need to be told what to do when facing a real or potential virus incident. Guidance needs to be readily and clearly available in order to minimise the risk of staff trying to resolve a problem without assistance and thereby creating greater risks or real damage to an organisation’s data or facilities.
- 26 The reduction in percentage of incidents of virus infections reflects the increased effectiveness of anti-virus counter measures and their increased automation. The survey reveals that despite these efforts, viruses are still getting through and disrupting organisations. In an increasingly interconnected world, the speed of infection is amazing and even the smallest organisation can find that it is hit by a new virus within hours of its release.

- 27 All organisations can substantially reduce the risk of virus infections by selecting and installing virus prevention software on their networks and PCs to inhibit such intrusions. But this is not enough. Organisations should also ensure that security software is kept up-to-date and staff must be aware that they have a responsibility to ensure that they receive and, where necessary, install such updates regularly.

Case study 1

A university reported that their main problem was virus attacks, with some 1,600 occurring in the past year. Although their network servers were protected, the key problem was with their PCs. They are now tackling this issue as a major new security project.

Source: Audit Commission

Questions for chief executives

Are our PCs and servers protected by anti-virus software?

How do we ensure that they are all regularly updated?

Hacking

- 28 The proportion of hacking incidents has fallen significantly since the 2001 survey and this is consistent with other national surveys. Improvements in the quality and sophistication of access control software, and more widespread adoption of such software as more organisations rely on internet access, may well have helped contribute to this reduction.
- 29 Of those responding to our latest survey, 85 per cent said that their organisation installed access control software and 98 per cent used firewalls to help minimise unauthorised access.

YBAR online survey

The evidence of the YBAR online surveys highlighted that:

- 97 per cent must enter a user name and password to logon to their PC;
- 93 per cent must enter a user name and password to logon to their network;
- 72 per cent are forced to change their password on a regular basis;
- 75 per cent said that they don't write down their passwords; and
- 84 per cent were allowed access to the internet only by connections provided by the organisation.

Source: Audit Commission

- 30 The YBAR results suggest that organisations have gone some way to improving staff access to their networks. This is a positive result, but such measures must be updated continually to ensure that they meet the increasing sophistication of cybercrime. The high incidence of virus attacks and the ability to access inappropriate material illustrates how inadequate precautions leave networks open to misuse.
- 31 Hacking was initially perceived as a threat from pranksters anxious to demonstrate their skills at breaching low-quality security safeguards. As criminals seek to exploit technology and find more sophisticated means of perpetrating abuse, so hacking has taken on a more sinister aspect.

Questions for chief executives

How are our networks and PCs protected from hackers?

Have our network controls been tested?

How do we monitor the effectiveness of our safeguards?

Sabotage

- 32 Sabotage may take the form of physical attack and damage or, as was reported in our previous survey, it may involve cyber-vandalism. This includes the mass distribution of spam emails with the intention of causing massive disruption. Variations of this mass distribution, described under phishing below (paragraph 60), may well be the next generation of this form of abuse.

YBAR online survey

The evidence of the YBAR online surveys highlighted that:

- only 36 per cent of respondents knew that they were not authorised to enter their computer rooms; and
- only 42 per cent of users' PCs automatically timed out after a period of inactivity requiring users to re-enter their password and user name to resume their sessions.

Source: Audit Commission

- 33 The YBAR results suggest that access to ICT areas is potentially weak and that PCs left unattended pose a risk of unauthorised access. Poor access controls inevitably increase the risk of accidental damage and deliberate abuse. The fact that over half the YBAR respondents' PCs are not protected when they are left unattended suggests a low level of ICT abuse awareness within organisations. The ability to process data on a colleague's PC without their knowledge – perhaps during a lunch break – may prove to be an irritating prank or, at worst, malicious exposure of business or personal data.
- 34 Ineffective management of disgruntled workers – such as a failure to escort them from the building and remove all ICT access facilities – may well result in such staff having the time and opportunity to vent their discomfort on the organisation's ICT systems, thereby causing major disruption. While the proportion of reported sabotage incidents was low, the organisations affected said that the disruption and reputational damage to their organisations was significant.

Questions for chief executives

Do we site our servers in a safe, protected environment?

What do we do to protect our ICT facilities from damage by disgruntled staff?

How do we monitor the effectiveness of our safeguards?

Reputational damage

Accessing inappropriate material

- 35 A 16 per cent increase since the 2001 survey in the proportion of incidents involving accessing pornographic and other inappropriate material on the internet puts this form of abuse at the top of the list of reported incidents in the current survey.
- 36 The ready and necessary availability of internet access for genuine business purposes, coupled with the fast-growing range and availability of inappropriate sites make it difficult for organisations to control access successfully.

YBAR online survey

The evidence of the YBAR online surveys highlighted that:

- 76 per cent of users had been informed that all access to the internet was being monitored; and
- 92 per cent were informed that accessing or storing unsuitable material was a disciplinary matter.

However, only 62 per cent had access to written protocols covering email usage and language.

Source: *Audit Commission*

- 37 While software exists to identify and inhibit access to inappropriate websites, the quality and successful application of such software is only as good as its most recent update. New sites appear on a daily basis and users, if so inclined, can find and retrieve material relatively easily making management's task quite challenging.
- 38 Evidence from the survey suggests that six primary deficiencies in controls led to this high incidence of abuse (**Table 3**).

Table 3
Control deficiencies

Deficiency	Result
a failure to communicate to staff their personal responsibilities	staff were unaware of what the organisation deemed acceptable internet activity
a failure to communicate the organisation's policies	staff were unaware of what they should or should not be accessing
ineffective supervision of staff	management did not take seriously inappropriate use of the internet
poor security awareness	the organisation failed to recognise the need for software protocols to inhibit access to inappropriate sites
ineffective policies	policies did not reflect current internet activity
poor monitoring software and controls	the risks were not taken seriously so monitoring was ineffective

Source: Audit Commission

- 39 Where such incidents were discovered, this was generally due to successful internal controls, such as the use of monitoring software, or to information being received and/or whistleblowing and, as with other forms of abuse, through accidental means.
- 40 Research carried out in 2004 by Queen's University, Belfast for a leading software security company revealed that British employees are more likely to download and send sexually explicit material while at work than those in the USA.

- 41 The business impact of such activity may well be perceived as quite low. Respondents from organisations that suffered such abuse reported little or no disruption to their day-to-day activities and reputational damage was generally judged to be of little significance.
- 42 Clearly if the effect of such activity is not seen as significant then management may well not treat this abuse seriously. At one level, such abuse may be reflected in significant time-wasting but at another may well involve serious criminal activity and management should not dismiss such threats. Management needs to be unambiguous in what it regards as acceptable behaviour and ensure that the relevant policies and standards are clearly communicated to all staff.
- 43 The YBAR results show that only two-thirds of staff had access to written protocols covering email usage and language. Without clear statements to show what is acceptable, organisations are likely to find it more difficult to pursue investigations of inappropriate activity.
- 44 Of those cases reported in our survey, there was evidence of positive action being taken against perpetrators. This ranged from formal warnings to dismissal. In one well-publicised case, over 200 staff in a public body were disciplined with 16 being dismissed for downloading pornographic material on to their work computers.

Case study 2

An employee who was a home worker with internet access provided a member of her family with her username and password. That individual accessed pornographic websites. The perpetrator also had access to confidential emails and files held on the PC.

Source: Audit Commission

Case study 3

An agency worker employed by an organisation's outsourced ICT service provider sent inappropriate emails to female members of staff. The individual was traced by internal audit matching the email headers to internet activity logs.

Source: Audit Commission

Questions for chief executives

Have we defined clearly what we regard as unacceptable behaviour?

How have we communicated this to our staff?

Does our software prevent access to inappropriate sites?

How are these defined?

How do we deal with reported violations?

How do we monitor internet activity?

How frequently do we examine internet activity logs?

Using unlicensed software

- 45 The incidence of the use of unlicensed software has been consistently reducing over the Commission's past three surveys. There are clear financial consequences where there has been a failure to meet licence costs, but this matter is generally perceived to pose a greater reputational threat where organisations are publicly exposed as having avoided software licence fees.
- 46 The Federation Against Software Theft (FAST) was established in 1984 as the first software copyright organisation. It argues that the management of software licences is a complex area, which if not managed properly can have significant implications for any organisation, regardless of size or sector. A survey conducted by FAST in 2002 found that while senior management are becoming more aware of software licensing issues, 54 per cent of organisations would find it difficult to prove that they are fully compliant.

YBAR online survey

The evidence of the YBAR online surveys highlighted that:

- 74 per cent of respondents were advised by their organisations that the use of unlicensed software was prohibited.

However, only:

- 43 per cent had their PCs checked for non-standard software by internal audit or ICT staff;
- 54 per cent were prevented from installing software on their PCs; and
- 50 per cent were prevented from copying software from their PCs.

Source: Audit Commission

- 47 The YBAR results illustrate clearly that more needs to be done to reduce the opportunity for unlicensed software to be installed on PCs. The incidence of this form of abuse could be significantly reduced if staff were prevented from downloading software onto and from their PCs through the use of specialised software. Responses suggest that around half of public sector bodies do little to minimise the risk of unlicensed software being installed on PCs. Condoning such software theft sends the wrong signals to staff and weakens any determination to demonstrate sound governance.

Questions for chief executives

How do we ensure that we have no unlicensed software on our computers?

Do we undertake software audits?

When was the last audit and what was the outcome?

Invasion of privacy

- 48 Breaches of data protection legislation have remained at a consistent, albeit low, level for the past three surveys. Respondents did not judge these incidents to cause any significant impact on their day-to-day activities, nor did they result in any reputational damage to the organisation.

YBAR online survey

The evidence of the YBAR online surveys highlighted that:

- 56 per cent had been required to sign a confidentiality undertaking as part of their conditions of service;
- 71 per cent had had their data protection responsibilities explained to them; and
- 82 per cent had been informed that misuse of personal data would be treated as a disciplinary offence by their organisations.

However, only 49 per cent knew whether their organisation had appointed a data protection officer.

Source: Audit Commission

- 49 The key reasons for breaches of data protection were ineffective policies and a failure to communicate to staff their responsibilities and the existence of policies and procedures.
- 50 As more and more information is shared across organisational boundaries, the risk of accidental and deliberate disclosure of personal data increases. Freedom of Information legislation encourages more transparency in information provision. While personal data is not covered by this legislation there may well be a risk for public sector bodies in accidental disclosure under the mistaken belief of a requirement for more general increased openness.
- 51 The 2004 Annual Report from the Office of the Information Commissioner highlights ‘an organised and systematic industry whose lifeblood is the unlawful obtaining of personal information through deception, bribery and other underhand tactics. This is known as ‘blagging’. The Commissioner investigated the activities of employees of various organisations who were abusing their position of trust by corruptly obtaining and unlawfully disclosing personal information, usually for payment. This has proved to be a particular problem for some public sector organisations holding a wealth of personal data. As a result of the investigations a number of employees in public bodies have been suspended pending prosecution.

- 52 Although on the statute books for 20 years, knowledge of the compliance requirements of data protection legislation is still patchy. YBAR highlights that around half the respondents were not required to sign any confidentiality undertaking nor did they have any knowledge of responsibility for data protection within their organisation.

Questions for chief executives

How have we communicated the key elements of the data protection legislation to our staff?

How do we monitor compliance?

Financial loss

ICT-related fraud

- 53 With the majority of business systems using technology for processing it is becoming increasingly difficult to differentiate between those frauds involving an ICT process and those that do not. We have traditionally adopted a wide definition of fraud in our surveys to include as many different types of fraud incidents as possible and so our definition includes any fraudulent activity that involves obtaining gain by:
- unauthorised alteration of input;
 - destroying, suppressing, or stealing output;
 - making unapproved changes to stored information; or
 - amending or misusing programs (excluding virus infections).
- 54 Around 16 per cent of reported incidents were attributed to ICT-related fraud – an increase in the proportion of reported incidents when compared with the 2001 survey.
- 55 The perceived increase in reported frauds needs to be viewed against a background of increasing monitoring and investigative work in different sectors. The HM Treasury's Assurance, Control and Risk Team collects information on frauds across government departments and the NHS Counter Fraud and Security Management Service actively investigates fraud across the health service. More information is, therefore, more readily available from these sectors.

- 56 Payments systems proved to be the most prone to fraud with operational staff the most usual perpetrators. Detection was usually the result of information having been received. As with previous surveys, the most common reasons for the occurrence of frauds were poor staff supervision and inadequate division of duties.

YBAR online survey

The evidence of the YBAR online surveys highlighted that:

- only 41 per cent knew whether their organisation had an anti-fraud policy; and
- only 21 per cent knew the key elements of the policy.

Source: Audit Commission

- 57 Fraud remains a risk to all organisations and while the results of this survey, as with previous years, focus on direct acts of fraud and abuse perpetrated primarily by employees against the organisation, evidence from other initiatives shows a far greater incidence of fraud perpetrated by the general public.
- 58 The Audit Commission's well-established National Fraud Initiative has ample evidence of substantial and ongoing fraud. Its latest report *National Fraud Initiative 2002/03* (May 2004) reported a 66 per cent increase of detected frauds and overpayments in the previous two years, with an overall total of £83 million. While this exercise is much wider than ICT-related frauds, it does illustrate that fraud within public services generally shows no sign of diminishing.
- 59 A recent survey by the Financial Services Authority, *Countering Financial Crime Risk in Information Security* (November 2004) highlighted 'phishing' as a new threat aimed at impersonation and identity theft and increasing the risk, initially at least, to the financial community.

- 60 Phishing occurs where criminals send spoof emails misrepresenting the identity of organisations – often banks – to trick individuals into divulging personal data. Mass distribution of spam emails provides the means and opportunity to encourage the unsuspecting to disclose personal details and this version of hacking is proving attractive to organised crime for money laundering. It remains to be seen whether this form of abuse will become a key risk for public service bodies over the next few years if perpetrators seek to use such techniques to gather critical data and use it for fraud.

Case study 4

A manager used business account credit cards and the organisation's ordering system, to spend £2,800 on items for personal use. Eventually, this was brought to the attention of internal audit by a junior member of staff questioning the appropriateness of certain purchases and the whereabouts of certain items. Internal audit enquiries, and interviewing the manager established that various purchases could not be demonstrated to be for official use. This led to disciplinary procedures being actioned and the manager resigning.

Source: Audit Commission

Case study 5

An employee manipulated the creditor payments system to pass a bogus invoice for payment for £20,280. The employee exploited known weaknesses in processes and controls and managed to get hold of the cheque and cash it. Police were unable to trace the individual, who it was presumed went abroad, and the funds were never recovered.

Source: Audit Commission

Case study 6

The perpetrator was responsible for using a spreadsheet to record income collections and bankings. The employee misappropriated £22,826 over three years by manipulating the spreadsheets by temporarily amending formulae to show a reduced income collection figure, recording receipts that had been issued by cashiers as voided or at a lower amount, and not recording some receipts. The fraud was perpetrated because of a lack of separation of duties between receipting, checking and banking. The employee was prosecuted.

Source: Audit Commission

Case study 7

An employee had forged supplier invoices and obtained passwords for the creditor payments system. The individual raised overpayments to those suppliers and arranged for refunds to be sent to himself by cheque with the payee name left blank! The total fraud was £166,000 of which £141,000 was recoverable from insurers and the employee was prosecuted.

Source: Audit Commission

Questions for chief executives

Have we identified which of our systems are most at risk?

What additional protection do we provide for them?

When did we last review our anti-fraud policies and procedures?

How have we communicated the essential elements of our policy to our staff?

How do we monitor compliance?

Using ICT facilities for private work

- 61 When survey respondents were asked how they rated the risk of various forms of ICT abuse occurring, the use of an organisation's ICT facilities for private work was judged to present the greatest risk. The evidence of such activity does not support the perception, however, with the proportion of such incidents having fallen back to 1997 levels – accounting for 7 per cent of incidents.

YBAR online survey

The evidence of the YBAR online surveys highlighted that:

- 85 per cent of respondents knew what their organisation's rules were covering private use of ICT facilities and in particular, what was and was not acceptable.

Source: Audit Commission

- 62 Providing portable computing to a mobile workforce can provide significant opportunities for individuals to use facilities for private use. Organisations need to be clear about what they deem to be the limits of acceptability for private use and then communicate those parameters unambiguously to their staff. The borderline of acceptability may well be where use is for private commercial gain and/or where it represents a disproportionate element of the overall usage of the organisation's ICT facilities. The YBAR results demonstrate that the majority of staff did know what their employing organisation regarded as acceptable.
- 63 Poor supervision was judged to be the primary cause of the abuse but with managers being the primary perpetrators, it may not be entirely surprising that they were able to take advantage of their positions. Action against such staff seemed to have been positive – around half were reprimanded and a third were dismissed.

Questions for chief executives

- Have we defined what we regard as acceptable private use of ICT facilities?
- How have we communicated this to our staff?
- How do we monitor compliance?

Theft of information

- 64 The number of reported incidents of theft of information or software is relatively low compared with other forms of abuse. It has remained at a similar level when compared with previous years.
- 65 The survey has not sought to include the incidence of theft of equipment – not because this is not deemed to be a significant loss but rather because it is relatively easily replaced and insurable. Data, however, is not necessarily as easy to replace and its loss may well cause embarrassment, loss of confidence and potentially business disruption or even failure. It may also lead to breach of data protection legislation if personal data is involved.

Questions for chief executives

- How do we protect information stored on PCs, servers and PDAs?
- What are our procedures for deleting any data held on ICT equipment prior to its disposal?

3

Preventing ICT abuse

- 66 While prevention is better than cure, new technology continues to present an ever-increasing range of risks that users must be aware of.
- 67 Respondents were invited to rank a selection of newer technologies. They were asked to indicate whether they intended to take advantage of them and how they rated any risks they presented. Three of the topics were included in *yourbusiness@risk* and while the results from this survey were broadly consistent with the earlier survey, attitudes have clearly changed, with each item now being perceived as presenting a lower risk. E-procurement, e-payment and smart cards are now all seen as low risk by over half of the respondents. Perhaps this is due to experience in using the systems or a perception that the technology has now matured or that controls and procedures are sufficiently robust to address any risks. Web-enabled processes still present a significant risk and while products and protocols do exist to help to minimise such risks, the obligation to ensure that those control mechanisms do indeed work needs to be fully grasped.
- 68 It is a salutary lesson that in *yourbusiness@risk*, around three-quarters of respondents scored accessing websites and the use of email as medium to low risks – yet the greatest number of reported incidents for this survey was internet-related – accessing inappropriate material and virus infections.
- 69 Respondents were invited to say whether they currently used, or were intending to use, some particular newer technologies. Each presents different risks and the objective was to assess how far risks were perceived.
- 70 Large proportions of respondents judged the risks as medium to low (**Table 4**) and yet each of these technologies present not insignificant challenges to controls and safeguards as shown in **Table 5 overleaf**.

Table 4

PDA's are used by two-thirds of organisations but are perceived as a medium/low risk by the majority of them

	Risks				
	Use now	Plan to use	High	Medium	Low
PDA	63%	12%	12%	35%	41%
wireless networking	41%	27%	22%	34%	30%
SMS text messaging	20%	22%	8%	21%	53%

Source: Audit Commission

Preventative measures

- 71 Overall there has been an across-the-board increase in the adoption of a range of governance measures to help manage and minimise ICT-related risks when comparing the 2004 results with the previous survey. There has been an increase in take-up in all of the preventative measures identified in the summary and for many of the measures there has been a significant step change. This improvement is welcome and supports the increased professionalism required and increased sophistication in the area of ICT to meet the wide range of threats that exist (**Table 6, overleaf**).

Table 5

Technologies can provide obvious benefits, but they need effective safeguards to minimise risks

Technology	Benefits	Risks	Safeguards
SMS text messaging	<ul style="list-style-type: none"> easy to use intuitive and requires no training avoids demands upon ICT service engages younger people 	<ul style="list-style-type: none"> avoids organisation's security firewalls allows transfer of inappropriate material and avoids monitoring processes 	<ul style="list-style-type: none"> usage policy apply encryption apply specific monitoring software
PDA's	<ul style="list-style-type: none"> easy to use very mobile increasing range of standard applications available may allow constant communication with peripatetic staff 	<ul style="list-style-type: none"> cannot support full range of access control software very susceptible to theft and consequential loss of business data may allow transfer of inappropriate material and avoids monitoring processes 	<ul style="list-style-type: none"> usage policy secure backup away from the device password enforcement anti-virus controls restrict access to corporate networks regular synchronisation with network
Wireless technology	<ul style="list-style-type: none"> quicker and lower cost implementation easier connectivity to organisation/internet 	<ul style="list-style-type: none"> increased risk of hacking and sabotage 	<ul style="list-style-type: none"> secure data across the network use an encryption key limit/control wireless range

Source: Audit Commission

Table 6**There has been a real improvement in the adoption of preventative measures**

	2004 (%)	2001 (%)
Up-to-date computer security policy	96	78
Anti-fraud/corruption strategy	57	47
Ethics policies	46	32
Logging and reporting breaches	83	65
Email filtering	82	
Regular reviews of computer security	82	66
Regular risk analysis reviews	71	32
Internal audit	91	86
Computer security staff	85	31
Encouraging whistleblowing	66	58
Computer audit skills	61	52
Computer security awareness training	53	34
Regular personnel screening	28	11

Source: *Audit Commission*

- 72 While respondents said that their organisation had a current security policy, the success of such a policy depends upon it being communicated to and understood by staff. The YBAR online survey results paint a less satisfactory picture with a low recognition by staff of the availability of and commitment to such protocols.

YBAR online survey

The evidence of the YBAR online surveys highlighted that only:

- 22 per cent had been provided with a copy of the ICT security policy;
- 31 per cent had been informed about the policy and what they must and must not do;
- 32 per cent knew where to find written procedures for reporting a security incident; and
- 35 per cent felt that senior management was committed to the policy and its observance.

Source: Audit Commission

73 Respondents were asked, too, about a range of technical measures that they might be employing and the results were equally satisfying. Hopefully this all points to a greater awareness of the need for better governance and a willingness by management to invest in such control mechanisms (**Table 7**).

Table 7

Take-up of software controls to minimise risks has increased

Type of software	% take up
Anti-virus software	100%
Firewalls	98%
Access control software	85%
Deny access to specific internet sites	76%
Remote access control through smart cards/strong authentication	48%

Source: Audit Commission

74 Ensuring that effective safeguards are in place presents a different challenge. It is worth reviewing the reasons why cases of ICT-related fraud and abuse occurred. For example, while all respondents said that they installed anti-virus software, one of the most common forms of ICT abuse was virus infections so one could question the adequacy of the installation and effectiveness of this level of protection.

Causes and detection of incidents

- 75 Respondents were asked to indicate which particular control weaknesses most contributed to each of the reported incident's occurrence. A range of possible reasons was suggested, based upon experience from previous surveys (**Table 8**).

Table 8

Poor communications to staff is a key contributor to ICT abuse

Reason for incident	% respondents
communicating personal responsibilities to staff	41%
supervision of staff	32%
communicating existing policies to staff	27%
security awareness	22%
adequacy of strategy/policies	22%
monitoring processes	20%

Source: Audit Commission

- 76 All of these reasons point to a failure to exercise adequate managerial control over staff use of ICT facilities. An example of a reported fraud highlights the consequences of failures in basic controls such as releasing passwords to colleagues (**Case study 8**).

Case study 8

A temporary employee had worked in the organisation's central accounting section and had access to high-level passwords. The individual was then transferred to the payments department and asked a former colleague for their high-level password. It was then used to reactivate a closed supplier's account. A bogus payment for £7,600 was created and processed via BACS but an incorrect address was entered on the remittance advice. When it was returned to the organisation suspicions were aroused. The perpetrator was investigated and a subsequent payment stopped. The payment was recovered and the individual was prosecuted.

Source: Audit Commission

- 77 The incidents reported in this and previous surveys were not technology-related failures – they reflected poor supervision and management of staff and point to 'control myopia' by management. Security is only as good as the people who design it and apply it. If

management fails to design adequate protocols, and/or neglects to ensure that standards and codes of practice are made known to staff then management puts its organisation at risk.

Detection of incidents

- 78 Respondents were asked to indicate how incidents were detected. The most common responses were the application of internal controls; information received through whistleblowing and claimant/customer enquiries; accidental means; and the work of internal audit and security staff. Often the incidents were detected through a combination of these mechanisms and the table below shows how each of the incident types were most usually detected. The most common of all was through internal controls, and this represents an improvement on the last survey, where over half of all incidents were uncovered through accidental means (**Table 9**).

Table 9

The detection of ICT fraud and abuse

Most ICT abuse is detected through a combination of mechanisms, with internal controls most common.

	Total no. of incidents	Internal controls	Information received	Accidental means	Internal audit
All types	200	48%	33%	13%	12%
Fraud	31	52%	36%	10%	7%
Theft	9	33%	11%	22%	22%
Unlicensed software	3	33%		33%	
Private work	13	39%	54%		23%
Invasion privacy	9		56%	11%	33%
Hacking	6	83%		33%	
Sabotage	3	67%			33%
Virus	32	63%			3%
Inappropriate material	94	47%	44%	17%	13%

Source: Audit Commission

Perpetrators

- 79 The majority of incidents were perpetrated by the organisation's own staff – operational staff accounting for 37 per cent, administrative/clerical staff 31 per cent and managers around 15 per cent.
- 80 The table below provides an analysis of action taken against the perpetrators of ICT fraud and abuse. 151 respondents answered this question, and the figures show that in some cases more than one specific action was taken. It is encouraging that positive action was generally taken against the perpetrator where they were identified (**Table 10**).

Table 10
Responses to incidents

Of 151 responses to this question, action was taken in the majority of cases

		No action taken	Warning/reprimand	Reported to police	Dismissed/contract terminated	Resigned after discovery	Legal action	Downgraded/pay reduction	Transferred/downgraded/reduction in pay	Resigned before discovery
	151	17%	31%	23%	21%	16%	14%	5%	1%	1%
Fraud	29	3%	7%	66%	14%	21%	66%			
Theft	4			50%	25%	25%	25%			
Unlicensed software	1	100%								
Private work	13	15%	46%		31%	15%				
Invasion privacy	7	29%	71%		29%					
Hacking	3	67%		33%						
Sabotage	1	100%								
Virus	21	76%	19%	5%				5%		
Inappropriate material	72	1%	42%	15%	28%	21%	1%	10%	1%	3%

Source: Audit Commission

- 81 But taking action against perpetrators – both inside and outside the organisation – will often depend upon whether the perpetrator has had the organisation's definition of acceptable behaviour made clear to them. A failure to determine what is acceptable and a failure to communicate those rules and procedures will open the organisation to unnecessary risks.

Questions for chief executives

When did we last update our ICT security policies?

Do they address all the issues raised in this report?

How effectively have we communicated these policies to all our staff?

Trends in ICT abuse

- 82** There is no doubt that despite the best endeavours of organisations and their security staff, auditors and managers, ICT abuse will continue to thrive. As this report has shown, fraud, virus attacks and inappropriate use of ICT are the most common forms of abuse across public services. There is no evidence to suggest that these will diminish over the next three years.
- 83** Evidence from our survey, and from other surveys, suggests that misuse of the internet will continue to present the greatest risks both to individuals and organisations over the next few years. Poor controls over internet facilities may well lead to the accessing and/or distributing of inappropriate material; embarrassment to, or legal action being taken against, the organisation and individual; and unauthorised disclosure of personal and/or business-critical data. Organisations will continue to face all of these risks.
- 84** Identity theft is now increasingly common. Utilising email and the intranet, users can be tricked into divulging key information about themselves and particularly their financial circumstances. Public services hold much personal information about citizens and the risk of criminal attention being focused upon these personal data stores is becoming acute. The next few years may well see an increase in blanket identity theft across public bodies.
- 85** Wholesale reliance by organisations upon technology presents the obvious risk of the consequences of that service being deliberately disrupted. Denial of service attacks perpetrated by the sending of mass emails are a real possibility and can bring down an organisation's ICT service quickly and completely. The threat and the reality of such attacks may well become a very real issue for public sector bodies either through disgruntled citizens or criminal threats.

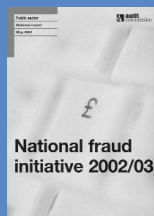
Actions

- 86 Good governance relies upon sound internal processes to protect corporate data. To help to focus attention on ICT governance we have included some key questions that we believe all chief executives should ask of their organisations.
- 87 We shall pursue an ongoing review of organisations' responses to this survey report to help to highlight weaknesses and emphasise the need for constant vigilance in the reduction of ICT abuse – and of the consequential waste in public services of time, effort and resources in pursuing such abuse.
- 88 In continuing to promote good governance in the application of technology to the delivery of public services we shall continue to offer our YBAR online survey service and encourage our audited bodies to use this facility to better understand perceptions of ICT governance within their organisations.



Matchwinner – Report on National Fraud Initiative 2000 *More than 600 councils and other public bodies contributed to the detection of over £500 million of fraud and overpayment in the Audit Commission’s National Fraud Initiative (NFI) 2000.*

GUP2743, ISBN 186240 362 7, £12



National Fraud Initiative 2002/03 *The National Fraud Initiative (NFI) brings together data from NHS bodies, local authorities, government departments and other agencies to detect a wide range of frauds against the public sector. This report looks at the value and types of fraud detected.*

GAR3219, ISBN 186240 493 3, £10



Your Business@Risk – An Update on IT Abuse 2001 *The explosion of new technologies in the public sector is giving rise to new risks, which are not being sufficiently addressed. Consequently, IT abuse continues to rise, business disruptions have grown and reputations are being damaged. Your Business@risk aims to help all organisations meet the risks and challenges they face. It considers lessons from the past, and conclusions from other similar work, to provide guidance and recommendations for detecting and preventing IT abuse.*

LUP1834, ISBN 186240289 2, £10

To order further copies of this report, priced £15, please contact **Audit Commission Publications, PO Box 99, Wetherby, LS23 7JA, 0800 502030.**

This report is available on our website at **www.audit-commission.gov.uk**. Our website also contains a searchable version of this report.

Audit Commission
1st Floor, Millbank Tower,
Millbank, London SW1P 4HQ
Tel: 020 7828 1212 Fax: 020 7976 6187
Textphone (minicom): 020 7630 0421
www.audit-commission.gov.uk

Price £15
Stock code: GUP3268