Performance Summary Report

June 2007

audit commission

Your Business @ Risk

Lancaster City Council

Audit 2006/2007

External audit is an essential element in the process of accountability for public money and makes an important contribution to the stewardship of public resources and the corporate governance of public services.

Audit in the public sector is underpinned by three fundamental principles:

- auditors are appointed independently from the bodies being audited;
- the scope of auditors' work is extended to cover not only the audit of financial statements but also value for money and the conduct of public business; and
- auditors may report aspects of their work widely to the public and other key stakeholders.

The duties and powers of auditors appointed by the Audit Commission are set out in the Audit Commission Act 1998 and the Local Government Act 1999 and the Commission's statutory Code of Audit Practice. Under the Code of Audit Practice, appointed auditors are also required to comply with the current professional standards issued by the independent Auditing Practices Board.

Appointed auditors act quite separately from the Commission and in meeting their statutory responsibilities are required to exercise their professional judgement independently of both the Commission and the audited body.

Status of our reports to the Council

The Statement of Responsibilities of Auditors and Audited Bodies issued by the Audit Commission explains the respective responsibilities of auditors and of the audited body. Reports prepared by appointed auditors are addressed to members or officers. They are prepared for the sole use of the audited body. Auditors accept no responsibility to:

- any member or officer in their individual capacity; or
- any third party.

Copies of this report

If you require further copies of this report, or a copy in large print, in Braille, on tape, or in a language other than English, please call 0845 056 0566.

© Audit Commission 2007

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 Fax: 020 7976 6187 Textphone (minicom): 020 7630 0421
www.audit-commission.gov.uk

Contents

Introduction

1 The growth in the use of newer technologies to give greater public access has resulted in increased risks for public sector bodies. Computer viruses, IT fraud, hacking, invasion of privacy and downloading of unsuitable material from the internet remain real threats to many organisations. Confidence in technologies that are influencing the way we live and work is being eroded and organisations must address these issues if the increased use of new technology is not to be matched by a similar increase in IT abuse.

2 An Audit Commission report, published in 2005, concluded that although organisations have got better at establishing anti-fraud frameworks, cultures and strategies, failures in basic controls are still a problem and the upsurge in the use of newer technologies has not been matched by enhanced security measures.

3 The Audit Commission has developed an online survey, 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;
- highlight areas where risks are greatest; and
- take positive action to reduce risks.

4 As part of our audit of Lancaster City Council (the Council), we ran the above online survey in April 2007. This brief report summarises the responses by staff at the Council. The full survey results are reproduced in Appendix 1 and the report highlights positive messages and identifies any areas of significant weakness where further action is necessary. The results were compared with the Commission's national database which currently contains almost 15,000 responses from around 80 public sector organisations.

Main findings and conclusions

5 Our conclusions are based upon responses from 209 users and 11 ICT staff from a total of all council employees requested to take part in the survey.

6 Overall, the results are around the national average for users of IT and concerns are mostly around the lack of awareness of the fraud strategy and the lack of knowledge of the procedures for reporting security incidents.

7 The survey shows that the level of awareness of IT staff is also around the national average but that there are areas where improvements are needed, particularly in relation to change control procedures.

8 As the survey is based on the perceptions of respondents, the issues that arise often relate to the need to improve communication, provide more information and training. However, it may also point to areas where improved procedures are required. The main areas highlighted by the survey include the following.

- Lack of awareness of documented change control procedure among IT staff.
- Lack of knowledge for reporting security incidents.
- Lack of awareness of the Data protection officer.
- Knowledge of key areas of relevant legislation.

9 Key messages are drawn out in Table 1 and we have summarised the recommendations and will include management responses when discussed and agreed with officers. Appendix 1 and 2 provide a summary of the survey questions and the results for the Council.

Recommendations

Recommendations	
R1	*Ensure that Change Control procedures are documented, understood and used.*
R2	*Develop a programme to ensure all users understand how to deal with viruses.*
R3	*Ensure that systems which are most at risk from fraud are identified and protected accordingly.*
R4	*Improve awareness of staff of the Council's counter-fraud arrangements (including 'whistleblowing' under the Public Interest Disclosure Act).*
R5	*Take steps to prevent users from copying and installing software on their PCs.*
R6	*Raise awareness of the identity of the Data Protection Officer and the responsibilities of individuals under the Act.*
R7	*Ensure that all PCs are set to time out after a period of inactivity.*
R8	*Increase IT legislation awareness through improved induction and ongoing training programmes.*
R9	*Educate all staff, regarding the existence of the IT Security policy. Ensure users are aware of the mechanism for reporting a security incident.*

The way forward

10 The council may find it beneficial to carry out this survey again at a future date to measure any improvements that have been made.

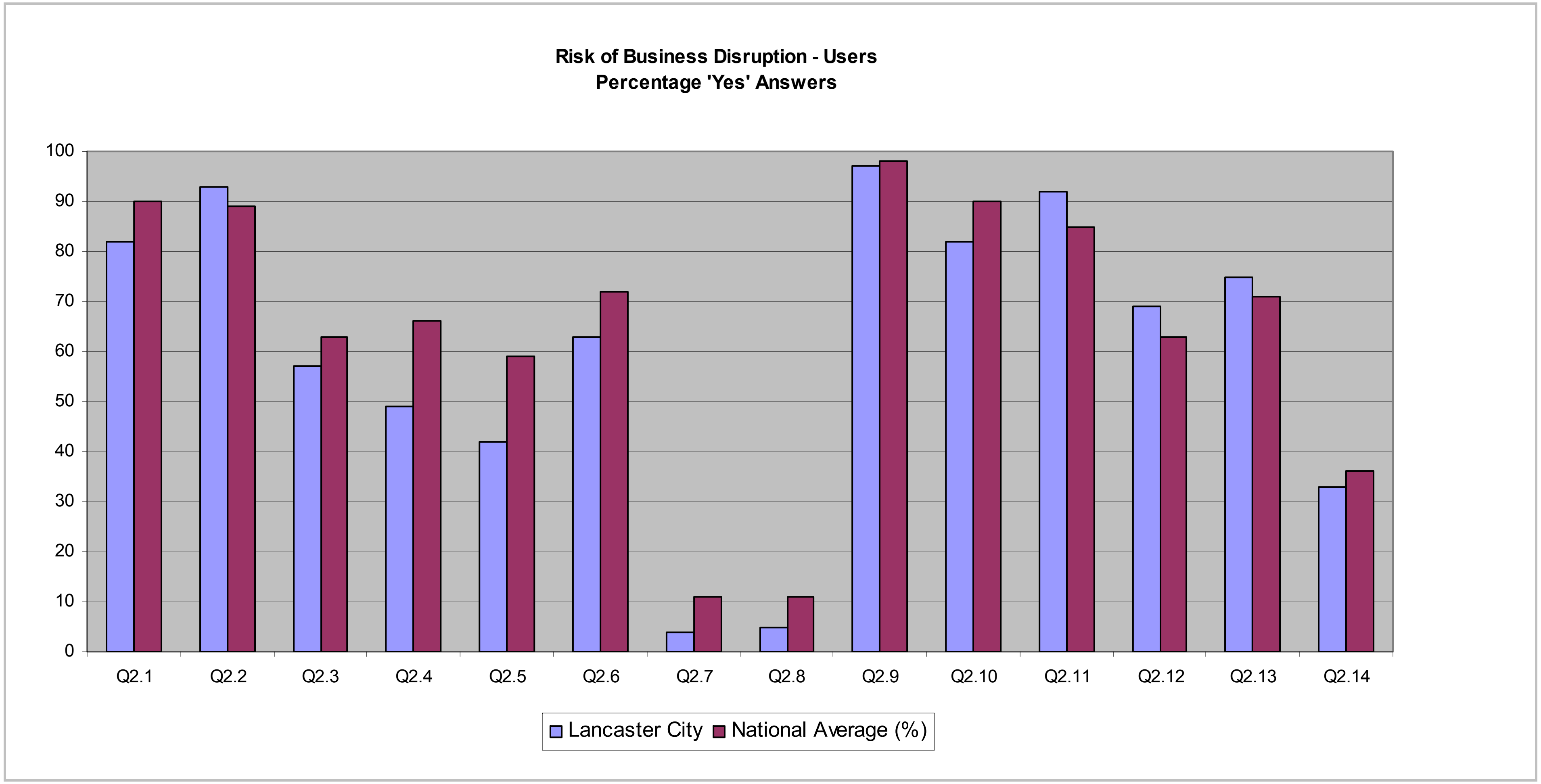
Table 1 Key messages

A brief summary of responses to our survey covering both dedicated ICT staff and departmental business systems users.

Business disruption risk		
Positive messages	**Areas requiring attention**	**Suggested action**
IT staff are confident about the processes in place to prevent virus attacks. 100 per cent of IT staff are aware that a firewall protects the network. 100 per cent of IT staff are confident that servers are sited securely and have restricted access.	IT staff did not consider that Change Control procedures were adequately documented or used. Users do not feel they have the information necessary to deal with virus infections.	Ensure that Change Control procedures are documented, understood and used. Develop a programme to ensure all users understand how to deal with viruses.

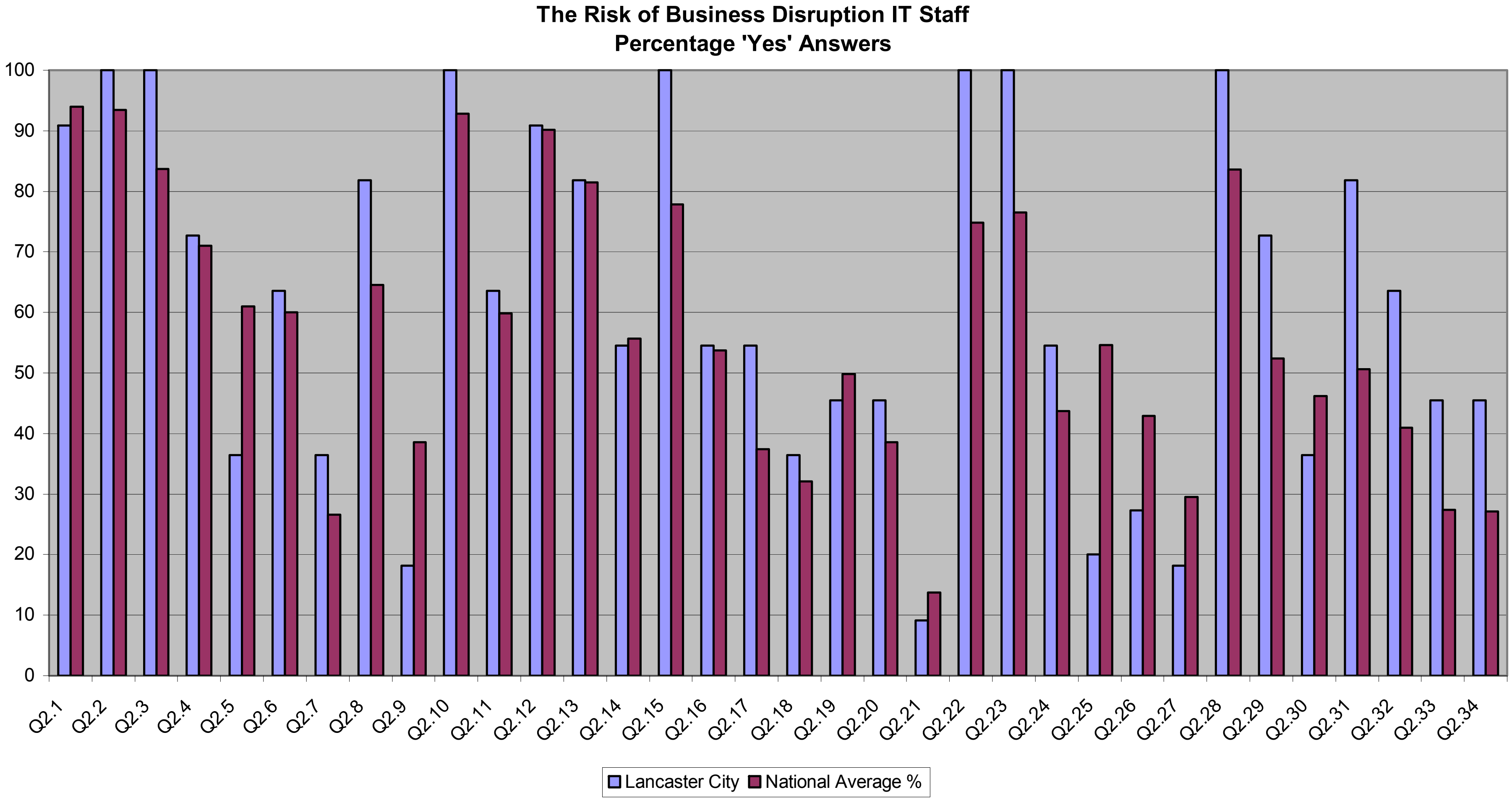
Figure 1 Risk of business disruption (users)

Results for council versus national results



Source: YB@R: Audit Commission
(Responses to Q2.7 and 2.8 on computer virus infection are better if lower than the national average).

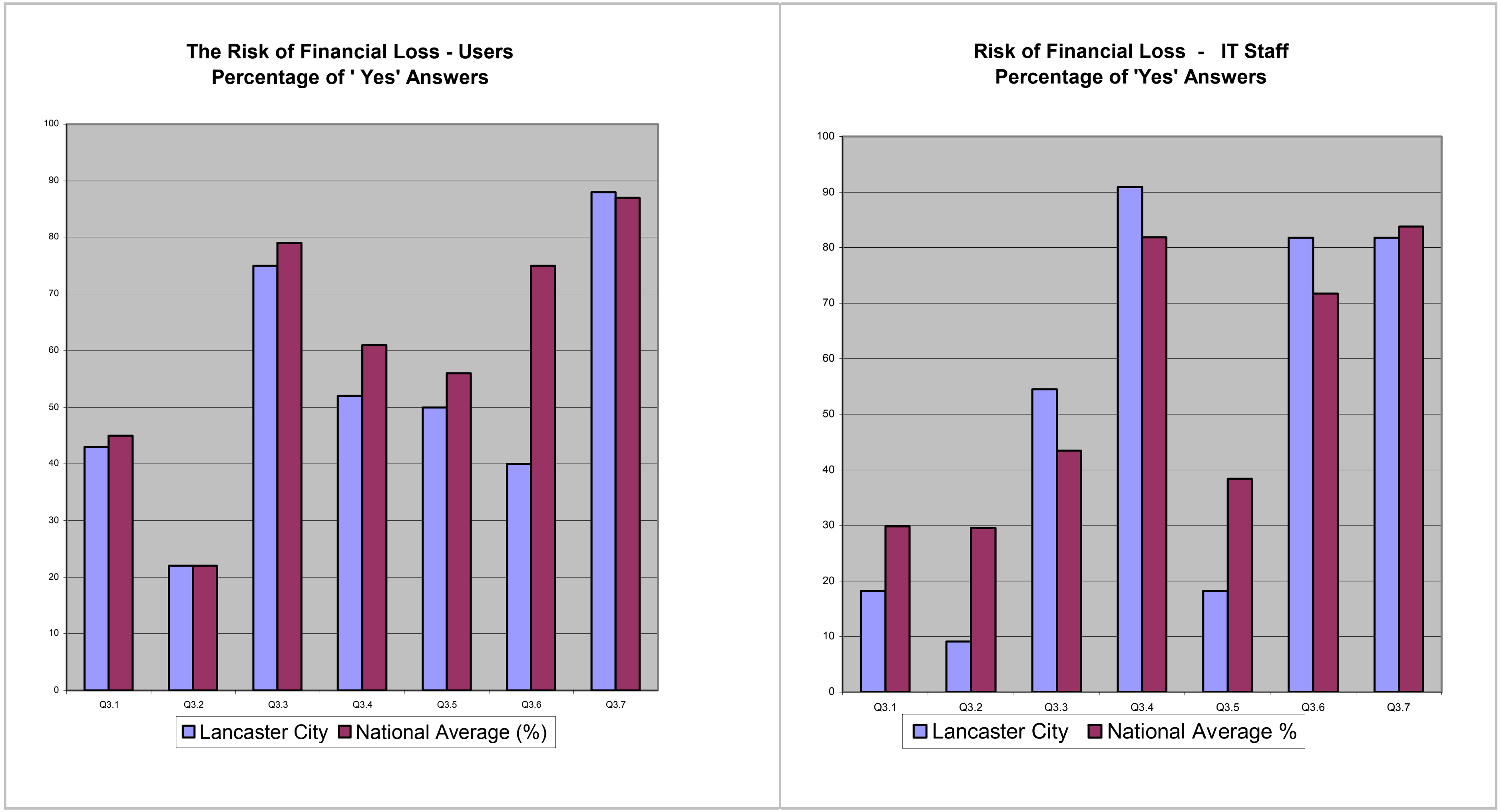
Figure 2 ICT staff results: risk of business disruption



Source: YB@R: Audit Commission

Financial loss risk		
Positive messages	**Areas requiring attention**	**Suggested action**
90.9 per cent of IT staff consider that access to systems is only granted to those who need it.	Only 18.2 per cent of IT staff consider that the systems most at risk from fraud have been identified.	Ensure that systems which are most at risk from fraud are identified and protected accordingly.
.	Only 43 per cent of users are aware of the anti-fraud policy and only 22 per cent are aware of the key elements.	Improve awareness of staff of the Council's counter-fraud arrangements (including 'whistleblowing' under the Public Interest Disclosure Act).
	Only 50 per cent of users and 18.2 per cent of IT staff consider there are controls in place to stop the copying and installation of software.	Take steps to prevent users from copying and installing software on their PCs.

Figure 3 Risk of financial loss Council versus national results



The Risk of Financial Loss - Users
Percentage of ' Yes' Answers

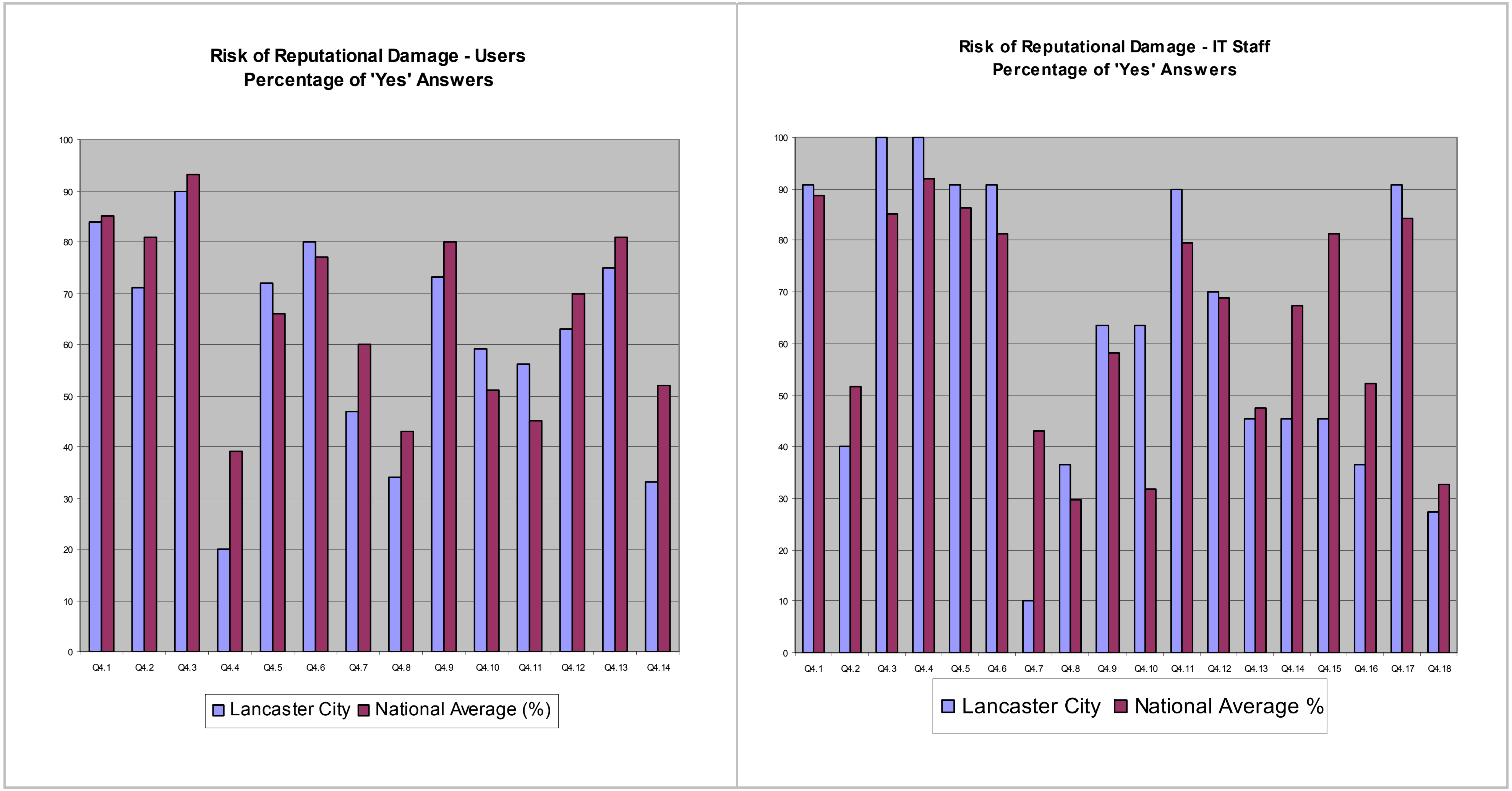
Risk of Financial Loss - IT Staff
Percentage of 'Yes' Answers

Source: YB@R: Audit Commission

Reputational damage risk		
Positive messages	**Areas requiring attention**	**Suggested action**
72 per cent of users have access to written protocols for email usage. 100 per cent of IT staff know downloading of unsuitable material from the internet is a disciplinary matter and that access to unsuitable sites is barred. Over 90 per cent of IT staff know their computer has a lockout facility for use when the computer is left unattended.	Only 59 per cent of users are aware that the Council has a data protection officer and only 45.5 per cent of IT staff feel their responsibilities under the Act have been explained to them. Only 33 per cent of users and 36.4 per cent of IT staff consider their PCs time out after a period of inactivity.	Raise awareness of the identity of the Data Protection Officer and the responsibilities of individuals under the Act. Ensure that all PCs are set to time out after a period of inactivity.

Figure 4 Risk of reputational damage

Council versus national results

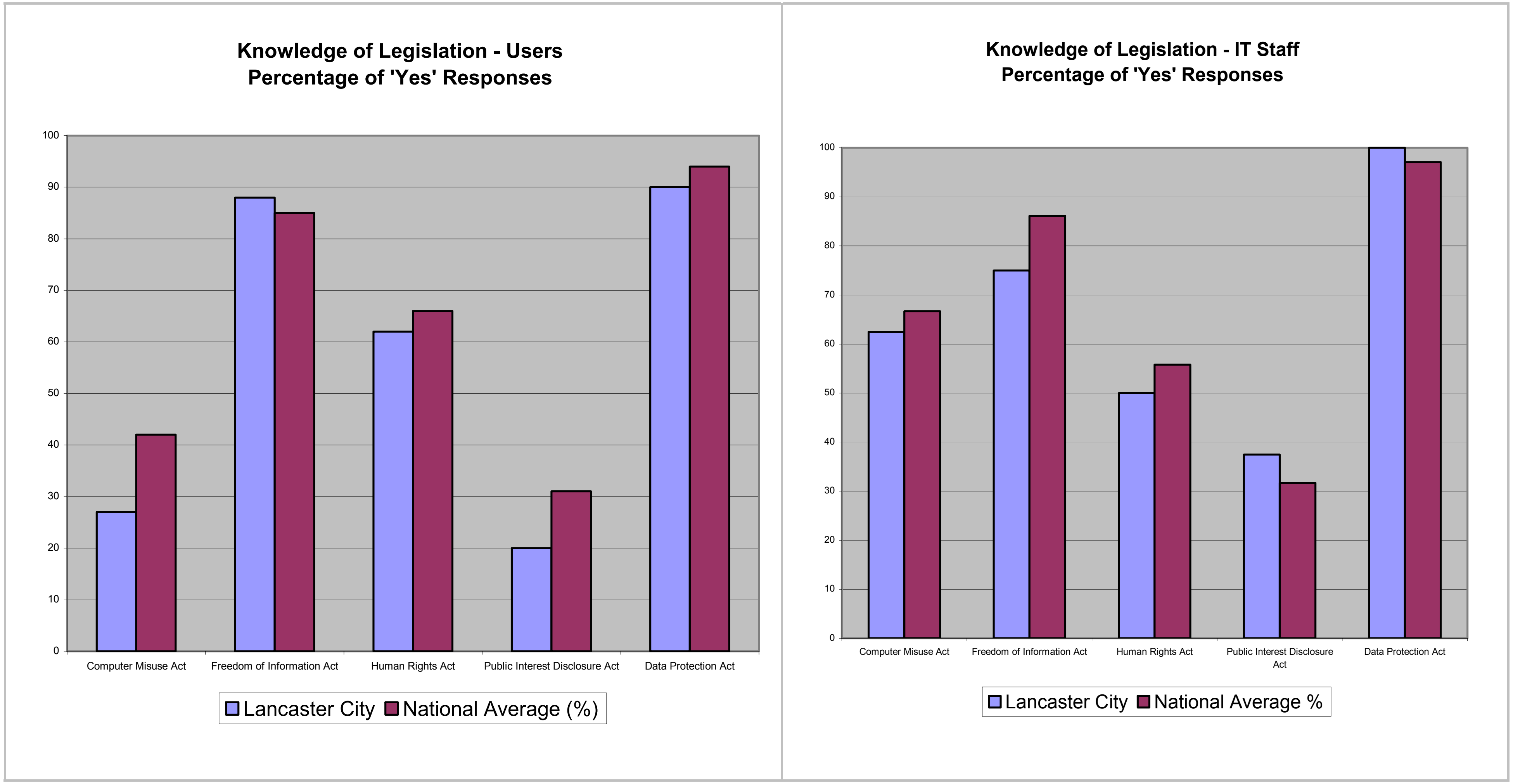


Source: YB@R: Audit Commission

Awareness of implications of legislation	Areas requiring attention	Suggested action
100 per cent of IT staff are aware of the main implications of the Data Protection Act. 88 per cent of users are aware of the main implications of the Freedom of Information Act.	Only 27 per cent of users are aware of the Computer Misuse Act and only 20 per cent are aware of the Public Interest Disclosure Act. Only 50 per cent of IT staff are aware of the Human Rights act and only 75 per cent are aware of the Freedom of Information Act.	Increase IT legislation awareness through improved induction and ongoing training programmes.

Figure 5 Awareness of implications of legislation

Council versus national results

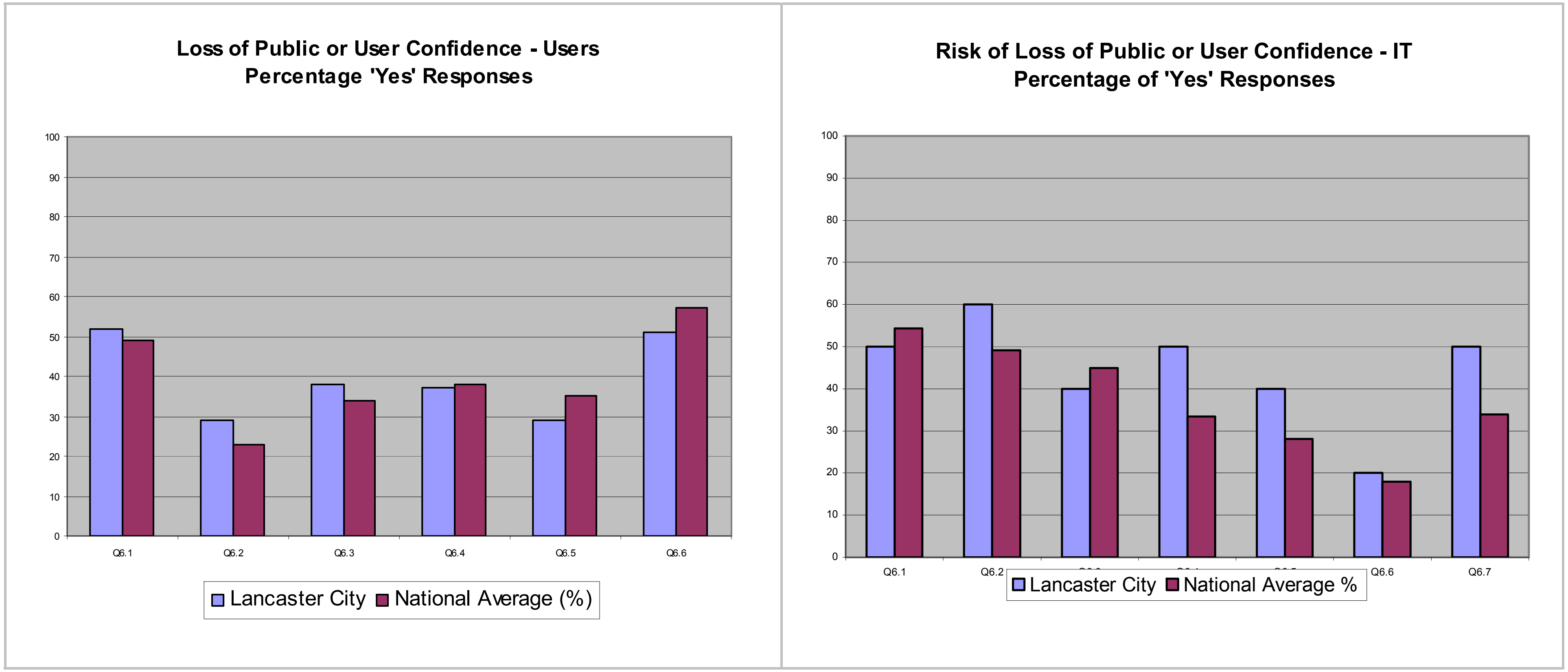


Source: YB@R: Audit Commission

Loss of user confidence risk		
Positive messages	**Areas requiring attention**	**Suggested action**
52 per cent of users are aware of the IT Security policy. 60 per cent of IT staff feel that users have been informed about the policy.	Only 29 per cent of users know where to find procedures for reporting a security incident.	Educate all staff, regarding the existence of the IT Security policy. Ensure users are aware of the mechanism for reporting a security incident.

Figure 6 Loss of user confidence

Council versus national results



Source: YB@R: Audit Commission

Appendix 1 – IT Staff

ICT Staff Survey

Q1	Which ICT Department do you work in?	
	Corporate ICT	70.0%
	Departmental ICT	30.0%

- 🟩 **At or above the national average**
- 🟨 **Below the national average**
- 🟥 **Cause for concern**

Q2	The risk of business disruption	Yes	No	Don't know	Not Applicable
	My organisation takes the threat of a virus infection very seriously	🟨 90.9%	9.1%	0.0%	0.0%
	Our policy is to install virus protection software on all our machines	🟩 100.0%	0.0%	0.0%	0.0%
	Staff are provided with regular updates to virus protection software	🟩 100.0%	0.0%	0.0%	0.0%
	Staff have been given clear instructions about dealing with emailed files from external sources	🟩 72.7%	18.2%	9.1%	0.0%
	Staff are alerted when new viruses are discovered and are advised as to what they must do	🟥 36.4%	45.5%	9.1%	9.1%
	We have clear procedures in place for reporting a virus incident	🟩 63.6%	18.2%	18.2%	0.0%
	Our procedures for recovering from a virus infection have been documented	🟩 36.4%	9.1%	54.5%	0.0%

	Yes	No	Don't know	Not Applicable
Our virus software is automatically updated by the software vendor	81.8%	9.1%	9.1%	0.0%
In the event of a virus outbreak measures are in place to restrict the impact of that virus eg. we make router changes to restrict virus infection	18.2%	27.3%	54.5%	0.0%
A firewall protects our networks, systems and information from intrusion from outside	100.0%	0.0%	0.0%	0.0%
Our firewall prevents large files and executable programs from reaching our networks	63.6%	18.2%	18.2%	0.0%
Our user registration and sign-on procedures prevent unauthorised access to our networks	90.9%	0.0%	9.1%	0.0%
Proper password management is enforced by the system on all users	81.8%	0.0%	18.2%	0.0%
Our dial-up connections are secure	54.5%	0.0%	36.4%	9.1%
Network management staff have been appointed	100.0%	0.0%	0.0%	0.0%
We have appointed an IT security officer	54.5%	9.1%	36.4%	0.0%
A detailed daily log of network activity is maintained	54.5%	9.1%	36.4%	0.0%
Network logs are inspected periodically by network staff	36.4%	9.1%	54.5%	0.0%
Sensitive programs and information are given additional protection	45.5%	18.2%	36.4%	0.0%

	Yes	No	Don't know	Not Applicable
Security violations are reported to IT security staff immediately by our security systems	45.5%	0.0%	54.5%	0.0%
Our web site vulnerability is checked every month	9.1%	27.3%	63.6%	0.0%
Physical entry controls prevent unauthorised access to our IT facilities	100.0%	0.0%	0.0%	0.0%
Our servers and network equipment are sited securely and adequate protection is offered	100.0%	0.0%	0.0%	0.0%
Our internal procedures minimise the risk of deliberate damage by employees leaving the organisation	54.5%	18.2%	27.3%	0.0%
Any amendment to a program or system must go through our change control process	20.0%	70.0%	10.0%	0.0%
Our change control processes are well documented	27.3%	63.6%	9.1%	0.0%
All IT staff are trained in our change control requirements	18.2%	54.5%	18.2%	9.1%
Backups of data on all servers are taken frequently	100.0%	0.0%	0.0%	0.0%
Backup arrangements are properly documented	72.7%	18.2%	9.1%	0.0%
User and IT staff have been trained in how to conduct backups of servers	36.4%	27.3%	36.4%	0.0%
Monitoring of backups ensures that management is alerted when backups of remote servers do not take place	81.8%	0.0%	18.2%	0.0%

	Yes	No	Don't know	Not Applicable
My organisation has a clear business continuity plan	63.6%	18.2%	18.2%	0.0%
All staff named in the business continuity plan know of its existence and their role in it	45.5%	9.1%	45.5%	0.0%
Our continuity plan is based upon a robust risk analysis process	45.5%	36.4%	18.2%	0.0%

Q3 The risk of financial loss

	Yes	No	Don't know	Not Applicable
The systems most at risk from fraud have been identified	18.2%	18.2%	63.6%	0.0%
The systems most at risk are afforded additional protection	9.1%	9.1%	72.7%	9.1%
We have a documented access control policy	54.5%	0.0%	45.5%	0.0%
Access to systems is only provided to those who need it	90.9%	0.0%	9.1%	0.0%
We have controls to prevent the copying or removal of software	18.2%	18.2%	63.6%	0.0%
Hardware is clearly security-marked	81.8%	18.2%	0.0%	0.0%
My organisation has clear rules covering private use of IT facilities and in particular what is and what isn't acceptable	81.8%	18.2%	0.0%	0.0%

Q4 The risk of reputational damage

	Yes	No	Don't know	Not Applicable
Staff are only allowed to access the Internet through our authorised ISP	90.9%	0.0%	9.1%	0.0%
Internet activity logs are reviewed by managers	40.0%	10.0%	50.0%	0.0%
We bar access to internet sites we deem to be unsuitable	100.0%	0.0%	0.0%	0.0%

	Yes	No	Don't know	Not Applicable
Our policies make it clear to all staff that the downloading or storage of unsuitable material is a disciplinary matter	100.0%	0.0%	0.0%	0.0%
Protocols for internet and email use have been developed and are available to all users	90.9%	9.1%	0.0%	0.0%
My organisation has made it clear to all staff that use of unlicensed software is prohibited	90.9%	0.0%	9.1%	0.0%
Security software that prevents the installation of any program except by authorised IT staff is installed on all PCs and laptops	10.0%	70.0%	10.0%	10.0%
Our Internal Auditors undertake reviews of software on users' PCs	36.4%	18.2%	45.5%	0.0%
Users in my organisation are prevented from gaining access to system utilities	63.6%	27.3%	9.1%	0.0%
Our asset register is up to date, as are all enterprise/site license numbers	63.6%	0.0%	36.4%	0.0%
My organisation has a documented Data Protection Policy	90.0%	0.0%	10.0%	0.0%
My organisation has appointed a data protection officer	70.0%	0.0%	30.0%	0.0%
All users are required to sign a confidentiality undertaking as part of their conditions of service	45.5%	27.3%	27.3%	0.0%
My responsibilities under the Data Protection Act have been explained to me	45.5%	45.5%	9.1%	0.0%
Misuse of personal data is treated as a disciplinary offence	45.5%	0.0%	54.5%	0.0%

	Yes	No	Don't know	Not Applicable
PC's are timed out after a period of inactivity	36.4%	54.5%	9.1%	0.0%
My computer has a lock out facility to be used when left unattended	90.9%	9.1%	0.0%	0.0%
Systems containing personal data are registered with the Information Commissioner	27.3%	0.0%	72.7%	0.0%

Q5 I am aware of the main implications of the following legislation:

□The Computer Misuse Act	62.5%
□The Freedom of Information Act	75.0%
□The Human Rights Act	50.0%
□The Public Interest Disclosure Act	37.5%
□The Data Protection Act	
	100.0%

Q6 The risk of loss of public or user confidence

	Yes	No	Don't know	Not Applicable
My organisation has an up to date Information Security policy	50.0%	10.0%	40.0%	0.0%
Staff are informed about the policy and what they must and must not do	60.0%	10.0%	30.0%	0.0%
Senior management is committed to the policy and its observance	40.0%	10.0%	50.0%	0.0%
An officer group manages the implementation of information security	50.0%	0.0%	50.0%	0.0%
Regular independent reviews of information security are undertaken	40.0%	0.0%	60.0%	0.0%
We comply with BS7799 standards	20.0%	30.0%	50.0%	0.0%
There are clear written procedures for reporting and following up all security incidents	50.0%	0.0%	50.0%	0.0%

Appendix 2 – Users

Your.Business@Risk

User Survey

Q1	Which Department do you work in? (only complete if agreed by your Authority/Trust)	
	Department 1	26%
	Department 2	10%
	Department 3	5%
	Department 4	6%
	Department 5	7%
	Department 6	6%
	Department 7	14%
	Department 8	10%
	Department 9	16%

Q2	The risk of business disruption				
		Yes	No	Don't know	Not Applicable
	My organisation takes the threat of a virus infection very seriously	82%	1%	16%	0%
		Yes	No	Don't know	Not Applicable
	Virus protection software is installed on my machine	93%	1%	6%	0%
		Yes	No	Don't know	Not Applicable
	Virus protection software is regularly updated on my machine	57%	3%	40%	0%
		Yes	No	Don't know	Not Applicable
	I have been given clear instructions about dealing with emailed files from external sources	49%	41%	9%	1%
		Yes	No	Don't know	Not Applicable
	I am sent an alert when new viruses are discovered and am told what to do and what not to do	42%	33%	24%	1%
		Yes	No	Don't know	Not Applicable
	I know how to report a virus infection if I suffer an infection on my machine	63%	25%	12%	0%
		Yes	No	Don't know	Not Applicable
	I have suffered a virus infection on my machine	4%	83%	12%	0%
		Yes	No	Don't know	Not Applicable
	Whenever I have suffered a virus infection, my machine was cleansed and restored quickly	5%	2%	15%	77%

	Yes	No	Don't know	Not Applicable
To log on to my machine I must enter a user name and password	97%	1%	0%	1%
To log on to my organisation's network I must enter a user name and password	82%	10%	5%	3%
I am forced to change my password by the system on a regular basis eg every month	92%	6%	1%	0%
To access the computers and systems I use to do my job I must remember more than two passwords	69%	31%	0%	0%
I have not written my password(s) down	75%	24%	0%	0%
I am not authorised to enter our computer rooms	33%	20%	38%	10%

Q3 The risk of financial loss

	Yes	No	Don't know	Not Applicable
My organisation has an anti-fraud strategy	43%	1%	56%	0%
I know what the key elements of the strategy are	22%	37%	36%	6%
I only have access to the information I need to do my job	75%	15%	10%	0%
I am prevented from installing any software on my machine	52%	21%	27%	0%
I am prevented from copying software from my machine	50%	11%	39%	0%
My computer is clearly security-marked	40%	15%	45%	0%
I know what are my organisation's rules are covering private use of IT facilities and in particular what is and what isn't acceptable	88%	6%	6%	0%

Q4 The risk of reputational damage

	Yes	No	Don't know	Not Applicable
I am allowed access to the internet only by connections provided by my organisation	84%	5%	11%	0%
I have been informed that my access to the internet will be monitored	71%	16%	12%	0%
It has been made clear to me that my organisation's policy is that accessing or storing unsuitable material is a disciplinary matter	90%	5%	5%	0%
Emails sent to me from outside my organisation that contain very large files or executable programs etc are prevented from reaching me	20%	16%	61%	3%
I have access to written protocols covering email usage and language	72%	6%	22%	0%
I have been informed by my organisation that the use of unlicensed software is prohibited	80%	6%	13%	0%
I am prevented from installing software on my machine.	47%	21%	31%	1%
Internal Auditors or IT staff in my organisation have checked the software on my machine	34%	8%	58%	0%
My organisation has a documented data protection policy	73%	1%	25%	0%
My organisation has appointed a data protection officer	59%	2%	39%	0%
I have been required to sign a confidentiality undertaking as part of my conditions of service	56%	22%	22%	0%

	Yes	No	Don't know	Not Applicable
My responsibilities under the Data Protection Act have been explained to me	63%	29%	8%	0%
I have been informed that the misuse of personal data will be treated as a disciplinary offence by my organisation	75%	13%	11%	0%
My PC is automatically timed out after a short period of inactivity and my password and user name must be entered to resume the session	33%	57%	10%	0%

Q5	I am aware of the main implications of the following legislation:	
	The Computer Misuse Act	27%
	The Freedom of Information Act	88%
	The Human Rights Act	62%
	The Public Interest Disclosure Act	20%
	The Data Protection Act	90%

Q6 Loss of public or user confidence

	Yes	No	Don't know	Not Applicable
My organisation has an Information Security policy	52%	0%	47%	0%
I have been provided with a copy of the policy	29%	36%	31%	3%
I have been informed about the policy and what I must and must not do	38%	30%	30%	2%
Senior management in my organisation is committed to the policy and its observance	37%	2%	60%	1%
I know where to find written procedures for reporting a security incident	29%	44%	26%	0%
Someone in my organisation is specifically responsible for IT security	51%	2%	47%	0%

Appendix 3 – Action Plan

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
5	R1 Ensure that Change Control procedures are documented, understood and used.	3	Help Desk Manager	yes	New Help Desk system - Footprints - will support this action.	July 2007
5	R2 Develop a programme to ensure all users understand how to deal with viruses.	2	Transformation Manager	yes	Via First brief item and update of information on ICS section of intranet. In conjunction with Communications Team.	September 2007
5	R3 Ensure that systems which are most at risk from fraud are identified and protected accordingly.	2	Internal Audit Manager	yes	Fraud issues will form part of our assessment when configuring the new Authority Financials.	December 2007
5	R4 Improve awareness of staff of the Council's counter-fraud arrangements (including ‘whistleblowing’ under the Public Interest Disclosure Act).	2	Internal Audit Manager	yes	Via First brief item and update of information on appropriate section of intranet. In conjunction with Communications Team.	September 2007
5	R5 Take steps to prevent users from copying and installing software on their PCs.	2	N/A	no	We use automatic tools to audit what is installed on each PC. If we find software which we believe to be unauthorised we contact the users for an explanation - referring to Internal Audit if necessary.	N/A

Page no.	Recommendation		Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
5	R6	Raise awareness of the identity of the Data Protection Officer and the responsibilities of individuals under the Act.	2	Transformation Manager	yes	Via First brief item and update of information on ICS section of intranet. In conjunction with Communications Team.	September 2007
5	R7	Ensure that all PCs are set to time out after a period of inactivity.	1	Help Desk Manager	yes	All PCs on the network can be set to need a password inputting after 15 minutes inactivity.	July 2007
5	R8	Increase IT legislation awareness through improved induction and ongoing training programmes.	2	Transformation Manager	yes	Via First brief item and update of information on ICS section of intranet. In conjunction with Communications Team and HR.	September 2007
5	R9	Educate all staff, regarding the existence of the IT Security policy. Ensure users are aware of the mechanism for reporting a security incident.	2	Transformation Manager	yes	Via First brief item and update of information on ICS section of intranet. In conjunction with Communications Team.	September 2007