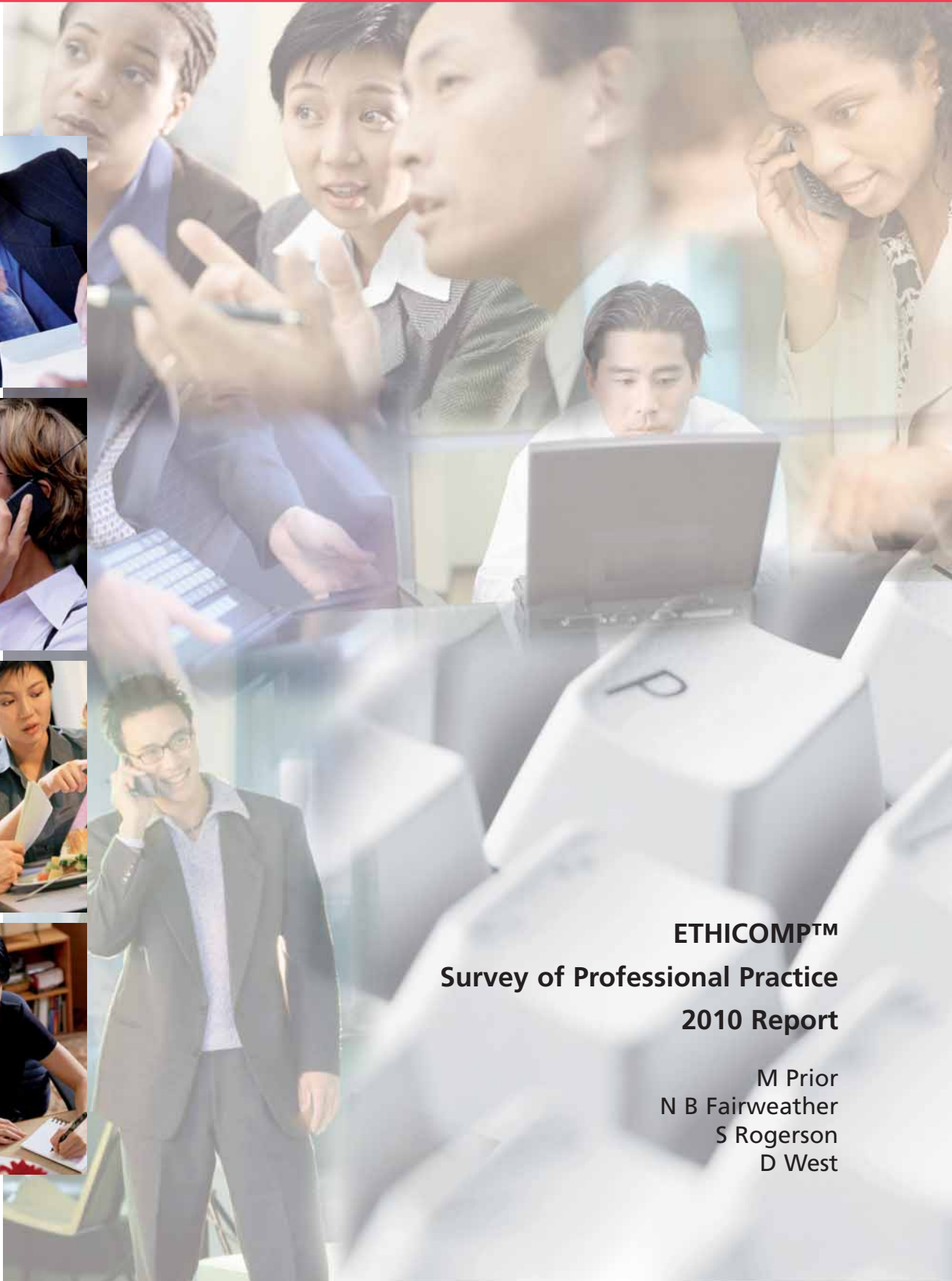


IS IT Ethical?



ETHICOMP™
Survey of Professional Practice
2010 Report

M Prior
N B Fairweather
S Rogerson
D West



The Institute for the Management of Information Systems



Is IT Ethical?

ETHICOMP™ Survey of Professional Practice
2010 Report



M Prior
N B Fairweather
S Rogerson
D West



Centre for Computing and Social Responsibility
De Montfort University

ETHICOMP® is a registered trademark of De Montfort University



The Institute for the Management of Information Systems



C o n t e n t s

1. INTRODUCTION

2. METHODOLOGY

3. PROFILE OF RESPONDENTS

4. FINDINGS

4.1 Importance of ethical considerations to organizations

4.2 Importance of ethical considerations to self

4.3 Intellectual property

4.4 Use of employer's computing facilities

4.5 Privacy and data protection

4.6 Security

4.7 Electronic surveillance of employees

4.8 Responsibility to users/clients

4.9 Licensing of IS professionals

4.10 Globalization

4.11 Responsibility for loss of personal data

5. RECOMMENDATIONS

APPENDIX

Survey of IS Professionals' Ethical Attitudes

1. INTRODUCTION

This report presents an analysis of the responses to the sixth ETHICOMP™ survey devised to ascertain the attitudes of Information Systems (IS) professionals to a variety of ethical issues. The survey was conducted during 2009 and is referred to throughout this report as ‘the 2009 survey’. Analysis of, and reflection upon, the survey results is presented in this 2010 report.



As explained in sections 2 and 3 of this report, the method of distribution of the survey altered in 2006, and again in 2009, resulting in some changes to the profile of respondents as compared with the earlier surveys. In retrospect, it appears that the 2006 survey results reflected a unique set of respondents; the responses to the 2009 one are in many respects more in line with those of the earlier surveys. This has enabled apparent trends noted in previous survey reports to be further examined.



The 2009 survey has seen an increase in the overall number of respondents, representing a range of age, experience, type of employing organization and country of employment. For some issues, these factors appear to have some influence on respondents' attitudes. In particular, the tendency perceived in earlier surveys for younger, less experienced respondents to show less ethical awareness in some areas than their more experienced colleagues, is confirmed. The differences in response between respondents working for some types of employing organizations and in certain geographical areas raise intriguing questions.



This report follows the format of previous reports in the series, presenting the responses to each issue addressed by the survey and providing comment and analysis on the findings. After discussion of the methodology adopted, a profile of the respondents to the survey is provided. The findings are then presented in detail, issue by issue, including comparisons with the previous surveys. Finally, a series of recommendations are made for organizations, for professional societies and for educators, intended to promote more socially responsible practices within the IS community.



The intended readership of this report is both those professionals practising in industry and commerce, and those responsible for the education of the next generation of IS professionals.

The work was carried out by the Centre for Computing and Social Responsibility at De Montfort University Leicester, on behalf of the IMIS.





2. METHODOLOGY

2.1 SURVEY CONTENT

Following a study of attitude survey methods and of previous attempts to determine ethical views, it was decided for the first survey in 1998 to formulate a series of statements and ask respondents to indicate the extent to which they agreed or disagreed with each statement.

In order to facilitate comparison, twenty of the original twenty-one statements were used as a basis for the second survey. Thirteen additional statements were introduced, some for the purpose of clarification where there may have been some ambiguity in the original statements, others to seek more detail (for example, with respect to electronic surveillance at work) or to introduce new issues (for example, globalization).

A core of twenty-seven statements has now been used in each survey from the second in 2000 through to the sixth in 2009. These have been supplemented in each survey with statements that incorporate issues of current concern and that support ongoing research. In 2009, these supplementary statements were used to address the question of responsibility for security breaches that lead to loss of personal data.

For the majority of ethical issues, more than one statement was provided, tackling the issue from different angles and in some cases distributed randomly among the statements to test the respondents' consistency of response. The issues covered are listed below, together with the number of statements devoted to the issue in each of the surveys:

Core statements:	1998	From 2000
<i>The importance of ethical considerations to organizations</i>	3	3
<i>The importance of ethical considerations to self</i>	2	2
<i>Intellectual property</i>	4	4
<i>Use of employer's computing facilities</i>	2	2
<i>Privacy</i>	2	3
<i>Security</i>	2	2
<i>Electronic surveillance of employees</i>	1	2
<i>Involvement of users and clients</i>	2	3
<i>Affect of computer system on work environment</i>	1	1
<i>Honesty to the client</i>	1	1
<i>Amount of testing effort</i>	1	1
<i>Licensing of professionals</i>	N/A	1
<i>Globalization</i>	N/A	2
<i>Ability to refuse to work on a project</i>	N/A	1
<i>Policies for facilities use</i>	N/A	1
Supplementary statements:		
<i>Use of codes of conduct</i>		2000: 4, 2006: 3
<i>Privacy and Data Protection</i>		2002: 3, 2004, 2006 & 2009: 1
<i>Trust and responsibility</i>		2002: 4
<i>Intranet use</i>		2004: 8
<i>Security breaches</i>		2009: 2

The same eight questions have been used across all five surveys to gather demographic data such as the respondents' gender, age and employment profile.

A copy of the survey will be found in the Appendix.

2.2 SURVEY DISTRIBUTION

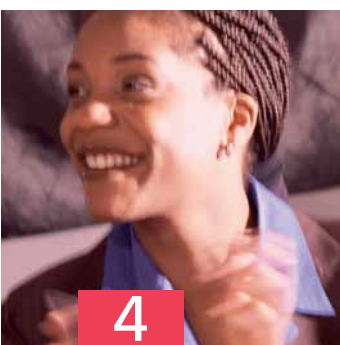
The response to the survey by IMIS members has fluctuated over the years and in 2006 it was particularly low, after a change to the means of distribution. The first four surveys were distributed to members in hard copy using the postal service; but since IMIS has changed to mainly electronic communication with its members, this ceased to be a viable option. The fifth survey in 2006 was made available via a link on the IMIS website and as an attachment to a copy of the e-bulletin. So few responses were received through that route that alternative means of distribution to a wider range of respondents was sought that year, resulting in the changed profile of respondents.

Since a return to postal distribution was not practical, for the 2009 survey, another change in survey distribution was utilised: it was deployed as an online survey. In addition to IMIS members, the link to the survey was sent to distribution lists of IS Professionals available to the Centre for Computing and Social Responsibility at De Montfort University. The result was a large increase in the number of respondents as compared with previous surveys:

1998	2000	2002	2004	2006	2009
170	90	188	136	188	324

Number of responses received

A number of comments were received from respondents to the effect that the survey was too long. The printed format, at four A4 pages, was identical to previous surveys and contained a comparable number of questions. However, the move to an online survey required the re-numbering of question parts and the resulting on-screen presentation gave the impression of a much longer survey. Consequently, it should be noted that although the number of responses received was nearly double that of the previous survey, it represented only 20% of those who attempted it: more than 1600 people attempted the online survey, of which over 1300 abandoned it. It is evident that while the use of an online survey may make it easier to reach a wider audience and could encourage high response rates, care must be taken in its design in order to maximise completion rates. In addition, respondents could be advised at the start of the survey of the approximate amount of time it should take to complete.

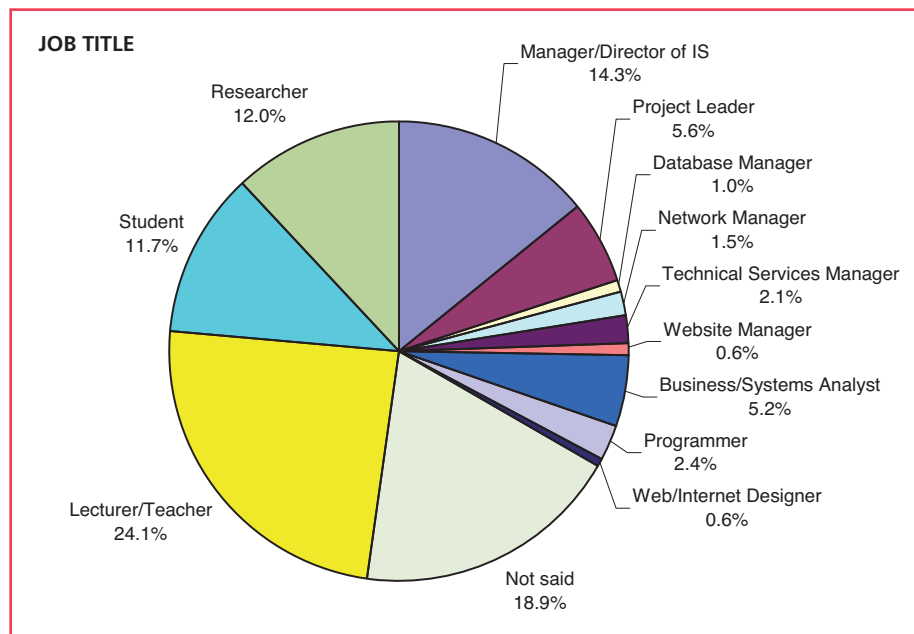




3. PROFILE OF RESPONDENTS

There has been a change in the profile of respondents throughout the period during which this survey has been administered. The majority of respondents to the first two surveys (1998 and 2000) were based in the UK, were over the age of 40 years and were professionals with a considerable amount of experience. In the following two surveys (2002 and 2004) the proportion of UK respondents dropped to below 40% and Africa was better represented (over 50% of respondents), in particular Zambia and Kenya where IMIS has many student members. The proportion of student respondents rose from around 10% in the earlier surveys to 30%, and there was a corresponding increase in the proportion of younger and less experienced respondents.

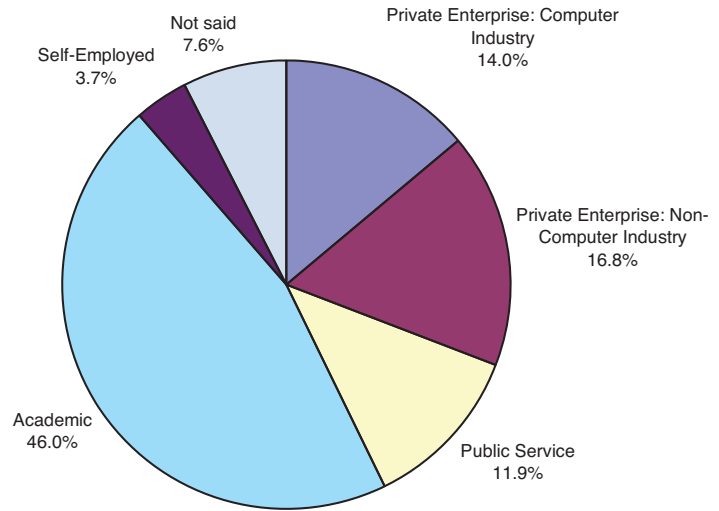
The change of distribution method for the 2006 survey brought another change in the profile of respondents. The majority (81%) were students and a majority of all respondents (70%) were based in the UK. For the only time, the respondents included a substantial minority of Chinese students (14%). Over 70% of all respondents were under 25 years of age. There were few practitioners from industry who responded to the survey.



The change to an online survey and the use of distribution lists to encourage as wide a group of respondents as possible has brought about another change. The largest group of respondents by job title are 'lecturers/teachers' (24.1%), with another 12% 'researchers' and 11.7% 'students'. Thus 47.8% work within an academic organisation; this probably accounts for there being 43.6% who work for an organization with over 1000 employees. It should be noted that nearly 20% of respondents did not answer the question about job title.

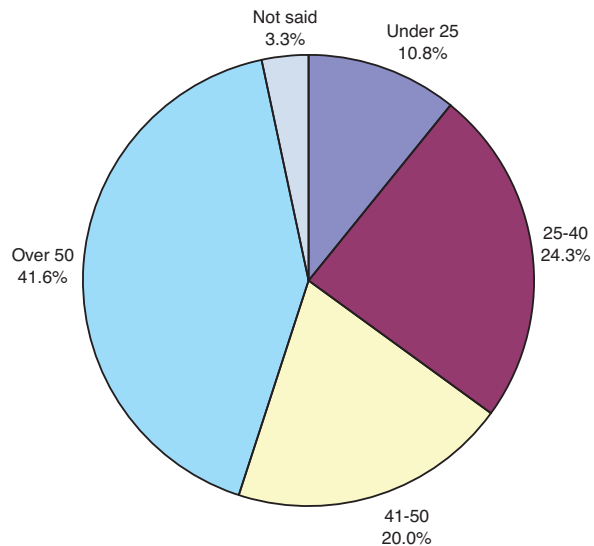


CONTRY EMPLOYED IN



Among the non-academic respondents, the largest group by job title are 'managers/directors of IS'. There is an overall movement back to a more experienced set of respondents; 49.1% have worked as an IS Professional for 15 or more years, with 41.6% aged over 50.

AGE



Just under 48% of respondents work in the UK. For the first time, there are respondents from the US (8.3%) and Australia (3.4%). Some 6.5% of respondents are from Zambia, with a total of 11.1% from African countries. Altogether, there are respondents from 28 nations across all 5 continents.



In common with previous surveys, the majority of respondents are male (71%). This time, though, the greater total number of respondents allowed some observations to be made about the relationship between gender and responses for the first time, although a different profile, in other respects, between male and female respondents confounds clear conclusions based on gender differences (for example 36% of female respondents are 'lecturers/teachers', with another 14% 'researchers' and 14% 'students', all three being higher than the proportion of males giving that occupational category).

Overall, only 16.4% of respondents this time have completed a previous IMIS survey. Some 40.4%, however, are members of IMIS and a variety of other professional bodies are represented including the British Computer Society (19.8%) and the ACM (10.2%).

The profile of respondents to this survey has presented the opportunity to examine the views of experienced practitioners and academics alongside those of less experienced practitioners and students. The large proportion of academic respondents enables comparisons between them and respondents working for other types of employer. Finally, the range of countries in which respondents are employed enables some interesting geographical differences to be observed.

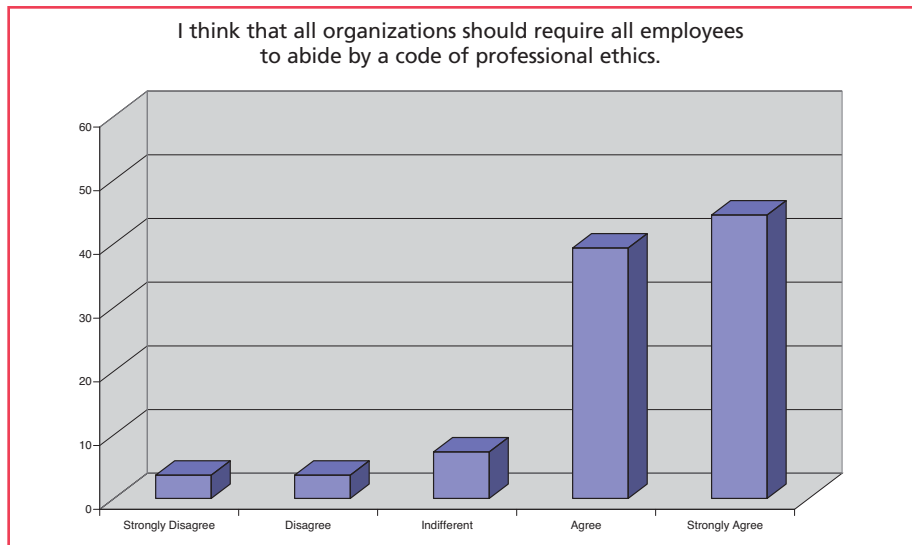
4. FINDINGS

This section presents an analysis of the responses to the survey, each issue being considered in turn.

4.1 Importance of Ethical Considerations to Organizations

For the last five surveys respondents have been asked both the extent to which they agree that all organizations should require all employees to abide by a code of professional ethics and whether organizations should require IS/IT employees to abide by a code of professional ethics. These two statements were separated by seventeen others covering various other issues.

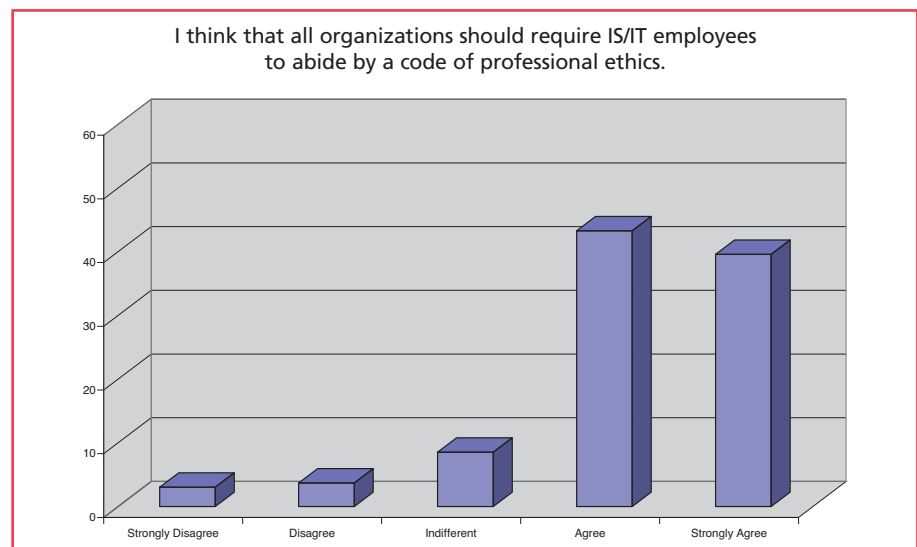
The responses from the first four surveys were remarkably similar, with over 90% agreeing or strongly agreeing both that all employees, and that IS/IT employees, should abide by a code of professional ethics. In the fifth survey, the total proportion in agreement was lower (70+, rather than 90+ percent) and the strength of agreement was less marked. There was also an increase in the proportion of 'indifferent', from a negligible percent in earlier surveys to 16% and 14% respectively for the two statements in the fifth one.



A similar pattern was found in the responses to the idea of organizations developing and administering an ethics awareness programme for their employees. While there was an increasing level of support for this in the first four surveys, culminating in 93% agreement in 2004, both the overall level (74%) and strength of agreement had dropped in the fifth survey and there were more 'indifferent' responses.

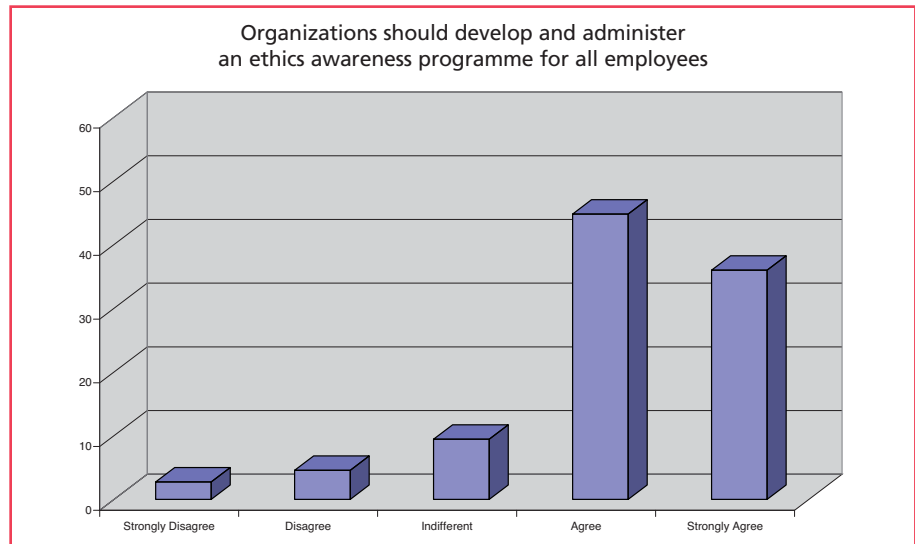


We commented in the report on the last survey that students appeared to be less strong in their support for the implementation of ethical policies at an institutional level than IS/IT practitioners. The current survey appears to partly support this notion, but also to suggest something else. Nearly 85% of respondents agree or strongly agree that organizations should require all employees to abide by a code of professional ethics, and 83.3% that IS/IT employees should be required to do so. The minority who disagree or strongly disagree with these statements are more likely to work in an academic institution. Interestingly, it is not just students, however, but also academic staff and researchers who appear in this group. Of the 24 respondents (7.4%) who disagree or strongly disagree with the statement about all employees, 7 describe their role as 'lecturer/teacher', 6 as 'student' and 3 as 'researcher'. Similarly, of the 20 (6.2%) who disagree or strongly disagree with the statement about IS/IT employees, 3 describe their role as 'lecturer/teacher', 7 as 'student' and 4 as 'researcher'. Of the 22 respondents (6.8%) who are indifferent about the 'all employees' statement, and the 28 (8.6%) who are indifferent about the 'IS/IT employees' statement, 14 and 16 respectively are either academic staff, students or researchers.



It is also younger respondents who are more likely to disagree or strongly disagree: with, for example, 5.5% of those over 40 disagreeing with the statement about all employees, 8.9% of those between 25-40 and 14.3% of those under 25.

The same trend is discovered in the responses to the statement *'Organizations should develop and administer an ethics awareness programme for all employees'*. Those respondents who disagree or strongly disagree are more likely to work in an academic institution. The proportion of the under 25s who disagree, strongly disagree or who are indifferent (25.7%) is double the proportion of the over 50s who give these responses (13.3%).



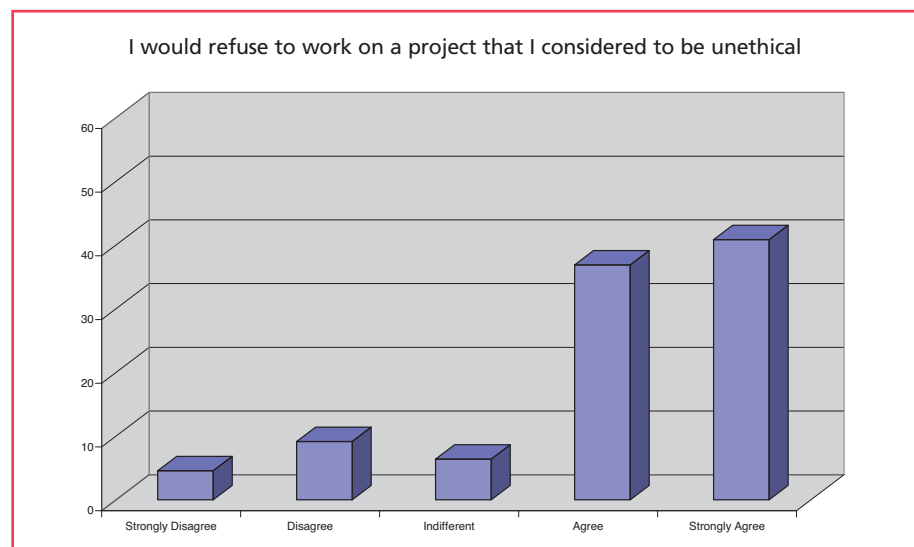
These findings appear to confirm that younger respondents may be less strong in their support for the implementation of ethical policies at an institutional level, as suggested in the previous survey. But they also suggest that academic staff and researchers may also be less strong in their support than IS/IT practitioners working for private enterprise or public service organizations. It is possible that they do not perceive such initiatives to be necessary. Or perhaps staff in academic institutions expect a degree of autonomy in their work which causes them to regard institutional initiatives with a degree of scepticism. This is an area worthy of further investigation.



4.2 Importance of Ethical Considerations to Self

Over the years that the survey has been conducted there has been a clear majority who agree or strongly agree that they would refuse to work on a project they considered to be unethical. The proportion agreeing varied between 75% and 83% over the first four surveys and as reported after the 2004 survey, the variation was consistent with the theory that a smaller cohort of responses could represent more 'ethically committed' practitioners.

In the fifth survey the proportion agreeing that they would refuse to work on a project they considered to be unethical dropped to just under 56%. The level of disagreement went up, as did the level of indifference, to some 20% each.



The results of the 2009 survey are closer to those of the earlier four, than to the previous (2006) one, with 79.3% of respondents agreeing or strongly agreeing that they would refuse to work on a project they considered to be unethical. Examining possible factors affecting the responses, we found that as many as a third of under-25s disagree or strongly disagree with this statement, while only between 10-12% of other age groups did so. It seems as though age has a stronger affect than any other factor, including occupation. For it was not just 26.3% of students who were among those to disagree/strongly disagree that they would refuse to work on a project they considered to be unethical, but also 33.3% of project leaders and 35.3% of business/systems analysts. Among other occupations represented by more than a handful of respondents, for whom any statistical analysis would be misleading, just 4.3% of managers/directors of IS and 6.8% of lecturers/teachers and researchers, disagreed or strongly disagreed.

These results need to be considered alongside the extent to which respondents are able to refuse to work on a project. Overall 34.3% of respondents have a free choice of projects to work on; 40.7% can sometimes choose and 21% have no choice. However, as might be expected, there is considerable variation according to occupation. While 36.2% of managers/directors of IS have a free choice, only 11.1% of project leaders do, with 33.3% of the latter having no choice. Among business/systems analysts, 29.4% say they have no choice. By way of contrast, 47.4% of lecturers/teachers have a free choice and only 3.8% have no choice. Thus, it is among the occupational groups with no, or limited, choice about the projects they work on that we find the highest levels of unwillingness to refuse to work on a project. The age of these respondents appears to confirm surmises made in earlier survey analyses about the limited degrees of freedom open to young professionals embarking on or building their careers.



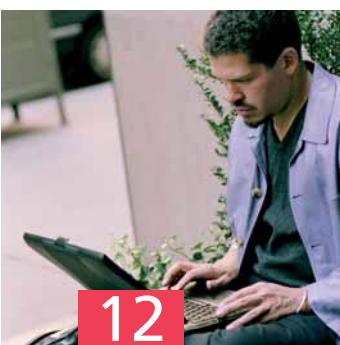
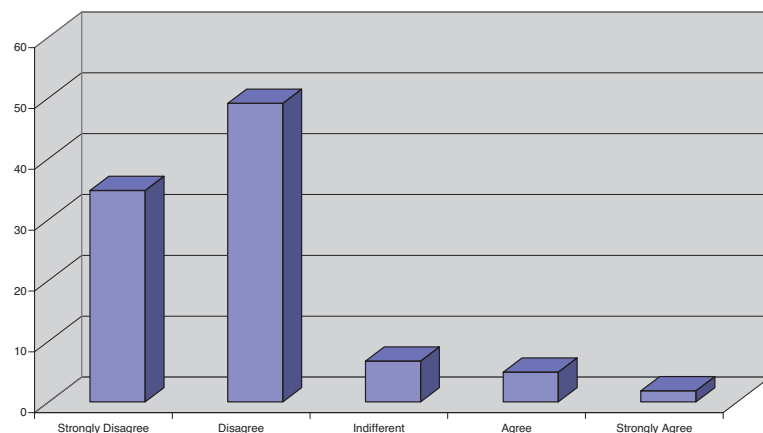
Although some younger respondents may not be able or willing to refuse to work on a project that they consider to be unethical, this does not mean that they do not care about its overall aim. When it comes to the statement, *'Providing a systems development project provides me with an interesting challenge, I do not care about its overall objectives or purpose'*, there was an increase in 2006 in the proportion of the respondents agreeing and those indifferent, with a reduction in the proportion who disagreed. The 2009 responses are more in line with the earlier surveys:



	1998	2000	2002	2004	2006	2009
Strongly Disagree	28	24	24	35	15	35
Disagree	56	63	54	43	49	50
Indifferent	9	6	11	5	19	7
Agree	3	2	6	7	9	5
Strongly Agree	3	1	1	2	3	2



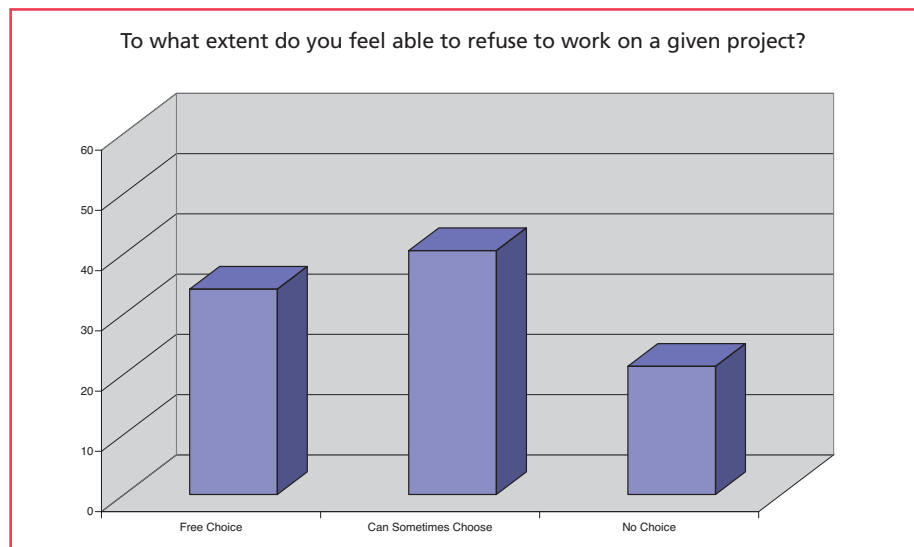
Providing a systems development project provides me with an interesting challenge, I do not care about its overall objectives or purpose





For this statement, age appears to have only a small effect, with 8.6% of under-25s agreeing/strongly agreeing that providing a project provides them with an interesting challenge, they do not care about its overall objectives; 2.5% and 6.2% for those aged 25-40 and 41-50 respectively and 4.4% of those over 50. Neither does occupation appear to have much of an influence; while 13.2% of students agree or strongly agree with the statement, so did 11.1% of project leaders and 11.8% of business systems analysts. It would seem that the responses of the student respondents in 2006 were out of line with student respondents in both the previous and the latest surveys.

From the responses to the 2009 survey, a picture emerges of young professionals who care about the overall objectives or purpose of the projects they work on, but who may not have the freedom to refuse to work on any that they consider to be unethical. The more mature professional in senior management posts, on the other hand, is more able to be more discriminating about his or her work. If this is the case, we re-iterate the calls made in earlier survey reports for organizations and professional societies to support younger professionals, enabling them to take an ethical stance regarding their work.



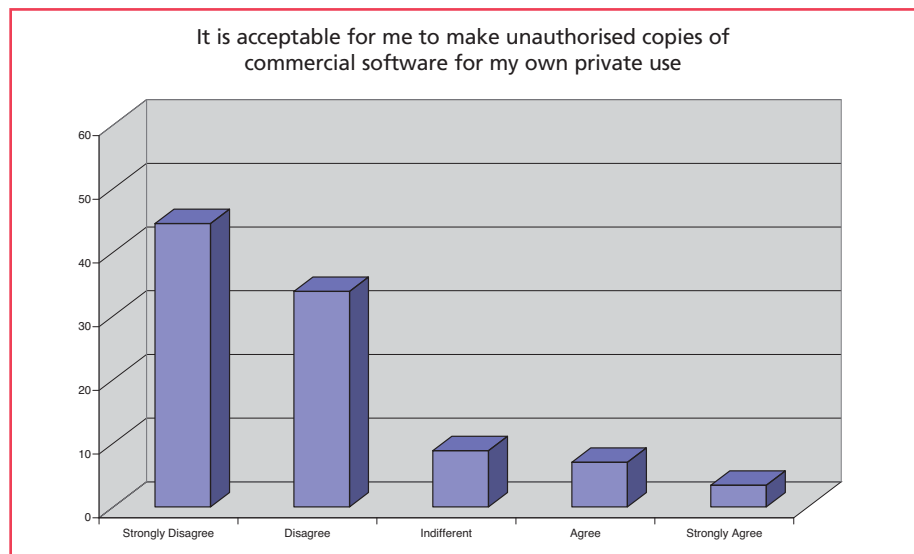
4.3 Intellectual Property

In each of the surveys there has been a majority of respondents who say that they find the unauthorised copying of software to be unacceptable. However, in 2006 there were some marked variations from the previous surveys, with a large drop in the size of the majority. The results of the 2009 survey are more in line with the earlier ones; however the large proportion of respondents with an academic background gives rise to some interesting findings.

In response to the statement, *'It is acceptable for me to make unauthorised copies of commercial software for my own private use'*, a total of 79.3% disagree or strongly disagree; this compares to 85% in 2005 and only 56% in 2006. However, it is the respondents working for an academic organization who account for the majority of those who agree, strongly agree or who are indifferent to this statement:

	Agree	Strongly agree	Indifferent
Lecturer/Teacher	12.8% (10)	1.3% (1)	6.4% (5)
Researcher	10.3% (4)	10.3% (4)	17.9% (7)
Student	2.6% (1)	7.9% (3)	10.5% (4)
All other occupations	4.4% (5)	1.7% (2)	6.1% (7)

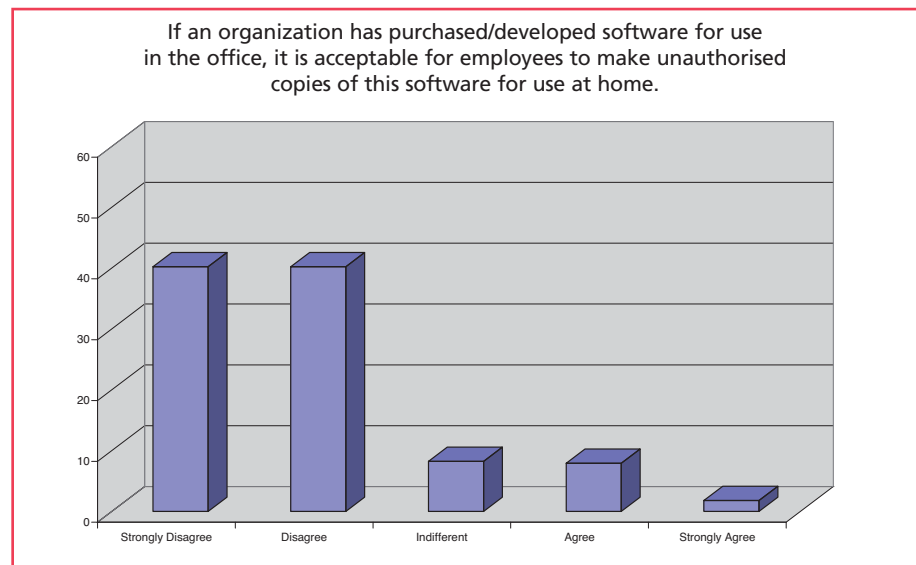
Similarly, in response to the statement, *'If an organization has purchased/developed software for use in the office, it is acceptable for employees to make unauthorised copies of this software for use at home'*, a total of 81.5% respondents disagree or strongly disagree (compared to 92% in 2004 but only 68% in 2006). It is once again the respondents working for an academic organization who account for almost all of the minority who agree or who are indifferent.





It is striking that it is a minority of academic staff and researchers, as well as students, who find the use of unauthorised copies of software to be acceptable, or who do not hold an opinion about this issue. As noted in the report of the 2006 survey, which found this tendency among academics attending an ETHICOMP conference, these may be responses from those who champion Open Source software. It may also be that for academics, students and researchers 'the workplace' extends into the home (in the case of students if they are thinking of their place of study as the 'workplace' applicable to their answers); thus some feel that software licensed for the one should cover use at the other.

It is worth noting that while the split of opinion between males and females is similar for most questions, for this question there was a discernable difference. Female respondents, like the male respondents, had a large majority disagreeing or strongly disagreeing, but noticeably fewer females 'strongly disagree' (37% vs 43% of males) and noticeably more agreed or strongly agreed (12% vs 8% of males). However, this could be because a significant majority of female respondents either work in academia or are students. On our sample size we cannot assess the two influences independently.



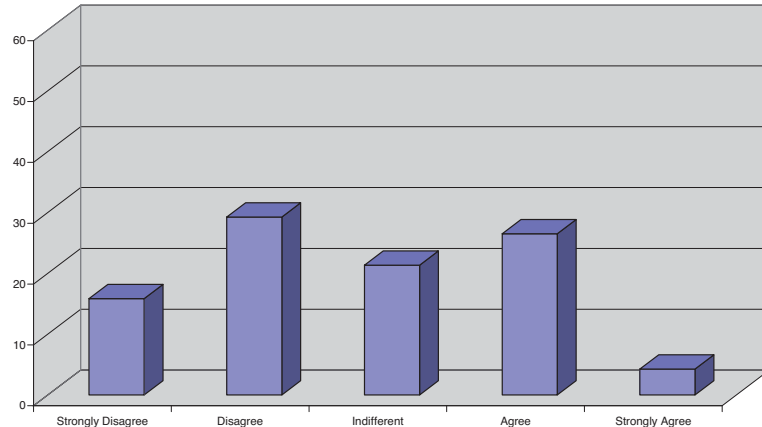
There is a difference of opinion among respondents as to whether *'Employees should be allowed to recreate a product/program/design for another organization if they change jobs and are no longer employed by the organization who paid them to create it'*. The level of disagreement (45.7%) is in line with the level of disagreement in previous surveys which has varied from 42-50%. The level of agreement (30.9%) is also similar; previously it has fluctuated between a low of 28% to a high of 48%, with the level of indifferent varying from 13% when agreement was at its highest to 22% when agreement was at its lowest.

One factor that appears to affect the responses to the 2009 survey is the type of employing organization. Those who are self-employed or who work in public service are most likely to disagree about employees being able to re-create intellectual property for an employer other than the one who originally paid for it; 75% and 64.1% respectively. There is still a majority of respondents from private enterprise who disagree, but the figures are smaller: 54.3% of those working in the computer industry and 47.3% of those in non-computer industries. When it comes to respondents working for academic organizations, responses are evenly split with 39% disagreeing, but 41% agreeing with the statement. The response of those working in public service is in line with previous surveys, but there have not previously been sufficient respondents from all types of organization to be able to perceive these differences.

It appears that there is less support among respondents working in academic settings for organizational intellectual property rights. Among staff working in private enterprise as many as 22.2% of those working in the computer industry and 30.9% in non-computer industries say that employees should be allowed to re-create a product/program/design for another employer. Employers need to be aware of this if they wish to secure intellectual property rights to work created by their employees.



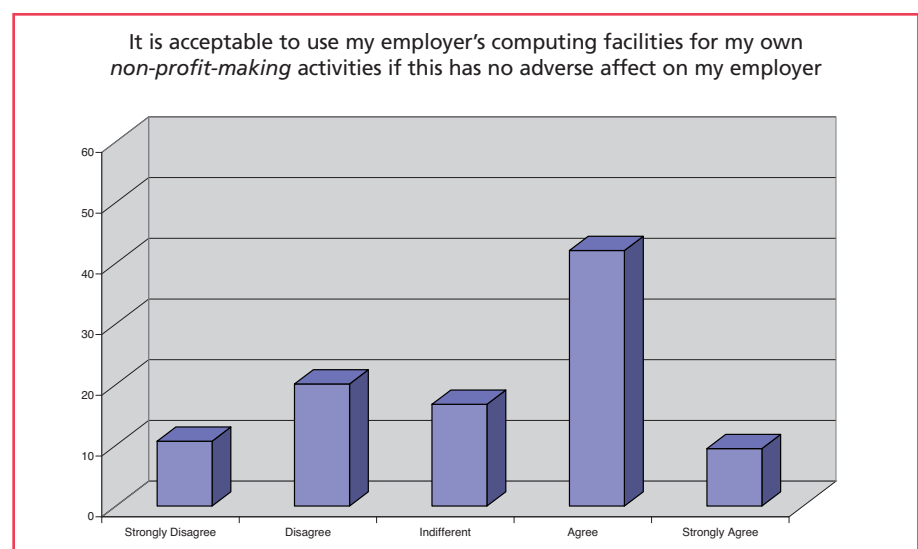
Employees should be allowed to recreate a product/program/design for another organization if they change jobs and are no longer employed by the organization who paid them to create it.





4.4 Use of Employer's Computing Facilities

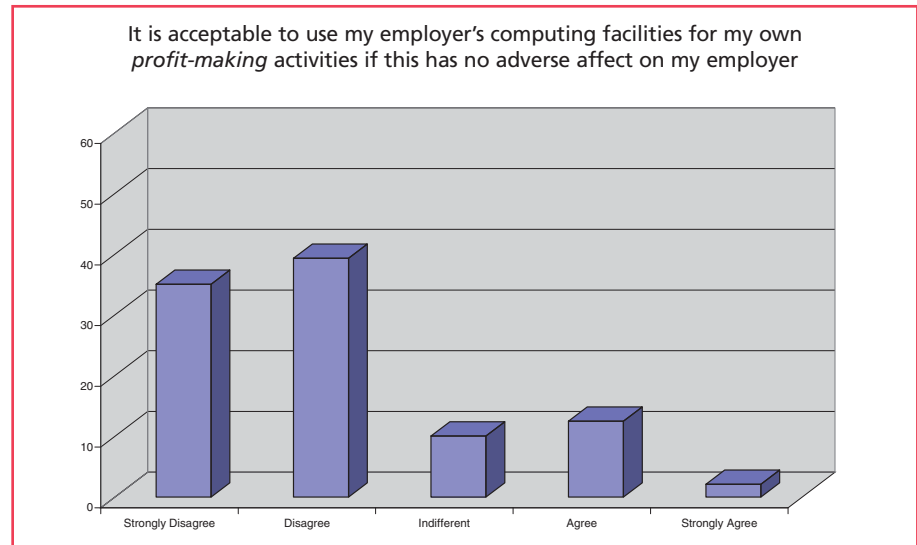
In all of the surveys, respondents draw a distinction between whether their employer's computing facilities are used for the employees' own *profit-making* or *non-profit-making* activities. In the first four surveys we found the attitudes of respondents across the age range, working in a range of IT roles, and for a variety of types of employer situated in several different countries, to be similar. In 2006 we found that delegates to an ETHICOMP conference, most of whom worked in academic institutions, were more likely than other groups to find *non-profit* use acceptable. The 2009 survey, with a larger number of respondents from each type of employing organization, sheds further light upon this issue.



Respondents working for private enterprise of all types, and in public service, are fairly evenly split on the acceptability of using their employer's computing facilities for *non-profit* use. The proportion of those agreeing that it is acceptable varies between 34.5% (private enterprise, non-computer industry) to 46.2% (public service). However, among those working for academic institutions the level of agreement is much higher: 65.1%. Among all three job titles in academic institutions (lecturer/teacher, student and researcher) there is majority agreement that it is acceptable to use their employer's computing facilities for *non-profit* use.

In academic settings, there is often a blurring of boundaries between 'workplace' and 'home', with work being undertaken in both environments, frequently outside the confines of 'office hours'. This may foster an attitude whereby use of the employer's facilities for non-profit activities may therefore be seen as legitimate, particularly in the evenings, and not to be interfering with commercial activity. Perhaps it is perceived as legitimate recompense for use of personal computing facilities for work use at home.

When it comes to *profit-making* use, there is much less agreement that this is acceptable. A minority of around 15% of respondents from each type of employing organization agrees that this type of use is acceptable. The proportion is higher for those working in academic institutions: 18.8%. However, this figure is accounted for by the student respondents. Both academic staff and researchers are in line with respondents from other types of employer, with just 15% agreeing that profit-making use of computing facilities is acceptable. But as many as 31.6% of student respondents agree that it is acceptable to use their employer's computing facilities for their own profit-making activities.



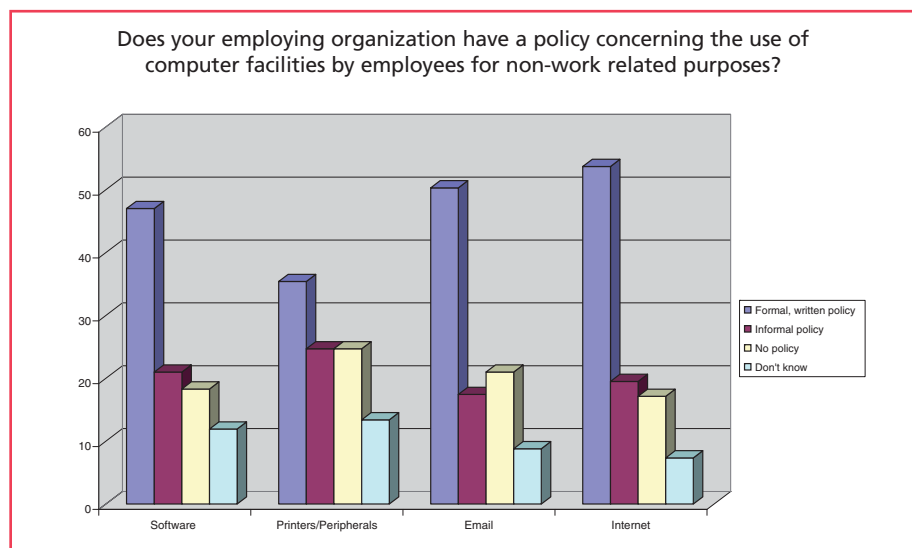
We noted a similar trend among student respondents in the 2006 survey. We commented then that full-time students have the freedom to use University computer laboratories throughout weekdays and evenings without an undue amount of monitoring of the work they are undertaking. The only obvious restrictions and monitoring relate to use of the internet; even so, there is a greater degree of freedom to use this than in most workplaces. The move to the workplace, therefore, involves a considerable change of culture with respect to the use of computer facilities. Employers may wish to consider giving student or recent graduate employees clear guidelines about facility use and informing them about the different norms that apply in the workplace as opposed to those in the more liberal academic environment they have come from.

As in all surveys since 2000, we included a question concerning the existence of organizational policies for the use of the computer facilities. The response rate to the question was higher this time, with 98% of respondents answering this question as compared to about three-quarters of all respondents in previous surveys. The overall responses are similar to those of previous surveys. The 2006 survey showed a drop in the number of respondents reporting policies for internet and email use; however, this was largely accounted for by the group of Chinese respondents to that survey.



Those working for non-computer private enterprises reported a higher level of formal or informal policies in existence; 82.1% as compared to 64.0% in public service and academic institutions and 71.7% in the computer industry. Large organizations with more than 5,000 staff were more likely to have policies; 79% of respondents working for these organizations reported the existence of a formal or informal policy as compared to between 66-70% for smaller ones.

Each of our surveys indicates that a large proportion of employees find it acceptable to use their employer's computing facilities for their own non-profit making activities providing this has 'no adverse affect' on their employer. This is the case despite the existence of organizational policies covering facilities' use. Organizations may wish to ensure that employees are not only informed about policies but that they understand their relevance; for example what are the possible 'adverse effects' of unauthorized use. A regular review of policies and frequent reminders to employees may also be required. In particular, this survey has highlighted the need to communicate policies to student and new graduate employees, who may assume that the relative freedom of use offered to them in academic institutions will apply in other workplaces.



One recommendation that we made as an outcome of the previous surveys was that organizations not only introduce a clear policy concerning the use of computing resources by employees for their own activities, but consider allowing the use for selected non-profit-making activities as a contribution to the local community or as a legitimate perk for employees. In the light of the findings from the 2009 survey, we believe this recommendation to remain valid.

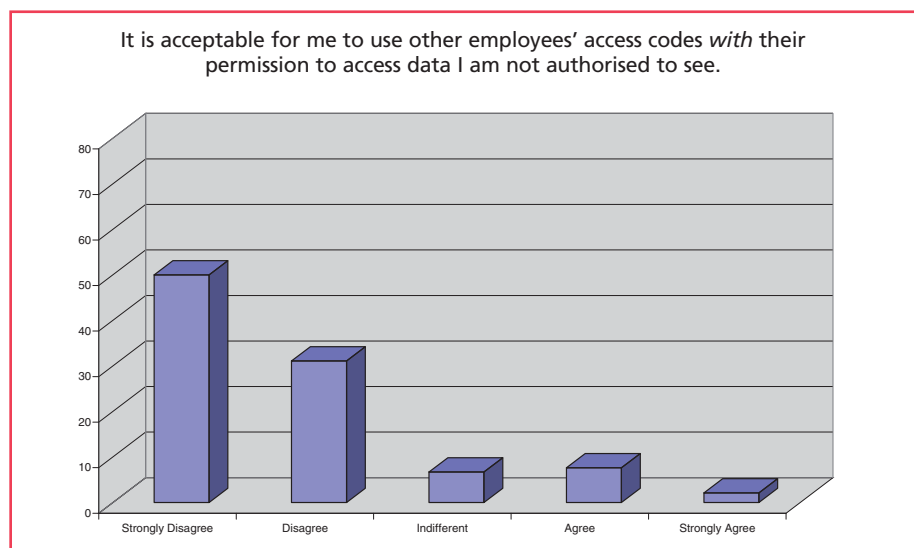
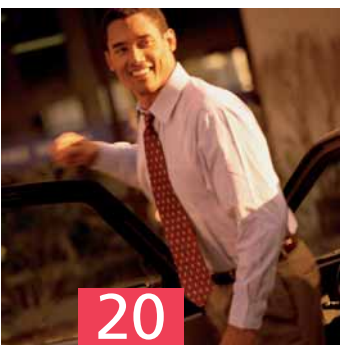
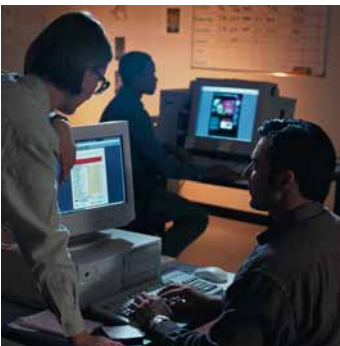
4.5 Privacy and Data Protection

Two statements concerning unauthorised access to data, as used in each survey since 2000, were included again in this one. In the three surveys between 2000 and 2004 there was an overwhelming and consistent majority of more than 95% who said that it was *not* acceptable to access data they were not authorised to see by using other employees' access codes *without* their permission. The figure dropped to 80% finding it unacceptable to access such data *with* the other employee's permission.

In 2006 there was a reduction to 85% of those finding it *not* acceptable to access data *without* the permission of the employees whose access codes they were using. There was an even larger reduction to 61% of those finding it not acceptable *with* permission; some 21% agreed that it *was* acceptable to access data they were not authorised to see if they had the permission of the employee whose access code they were using. The difference from the previous surveys was, again, largely accounted for by the group of Chinese respondents to the 2006 survey. The group of UK student respondents were also more likely to find it acceptable to access data they were not authorised to see both with or without permission of the employee whose access code they were using.

Once again the responses to the 2009 survey are more in line with those from the earlier surveys than the 2006 one. At the same time, it is possible to see a variation in response according to the age of the respondent.

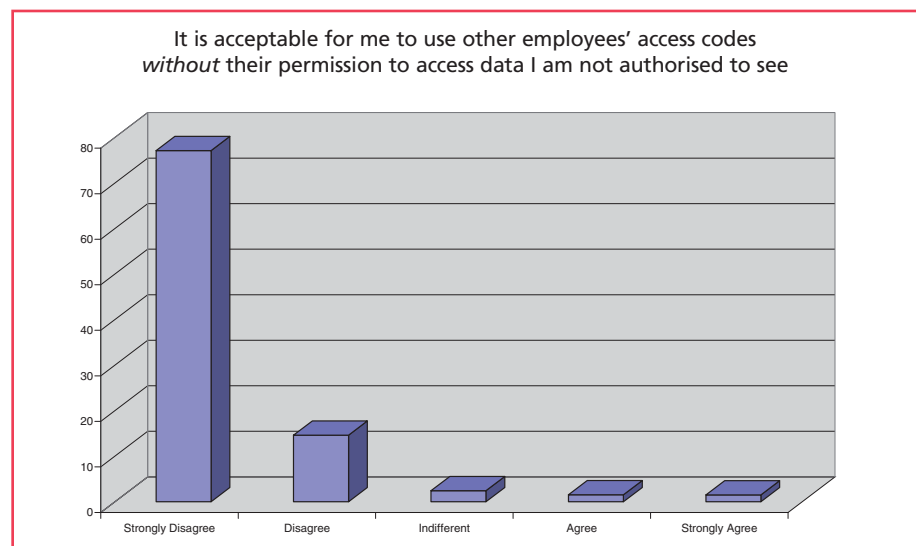
With respect to the statement, '*It is acceptable for me to use other employees' access codes without their permission to access data I am not authorised to see*', over 90% disagree, with over 80% of those aged 25 or more *strongly* disagreeing. In the under-25 age group, there is less strength of disagreement; nearly 69% strongly disagree with more than 20% disagreeing.





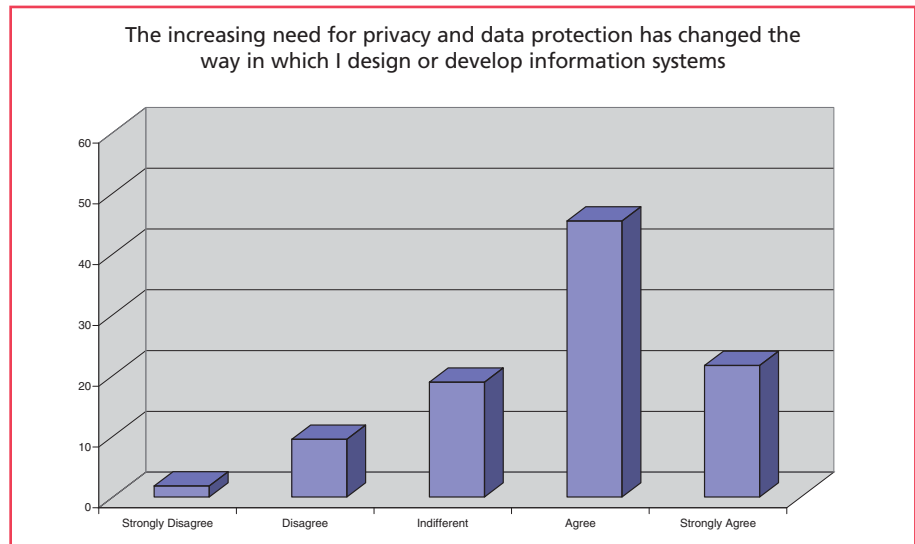
There is a greater discrepancy between the youngest age group and the older ones with respect to the statement, *'It is acceptable for me to use other employees' access codes **with** their permission to access data I am not authorised to see'*. While more than 80% of those aged 25 or over disagree with this statement, just 65.7% of the under-25s did so. Some 9-10% of the over 25s agree with the statement, but 20% of the under-25s.

Job title appears to have no effect on the responses; it is not just the student respondents who are represented in the under-25 age group. As with the importance of ethical issues to respondents, discussed in Section 4.2, it is age, rather than occupation, that appears to affect the responses.



There is a clear warning for organizations that they need to ensure that their privacy and security policies are clear, communicated to all employees, and that employees' awareness and deployment of them are continually reviewed. Younger employees, in particular, may need to be the target of privacy awareness campaigns.

For the 2006 survey a new statement was used to the effect that, *'The increasing need for privacy and data protection has changed the way in which I design or develop information systems'*. This statement was retained in the 2009 survey. A total of 67.9% of respondents agree with the statement, comparable to the 65% who did in 2006, despite the difference in the profile of the respondents between the surveys being the likely explanation for variations in responses to other questions. Responses are similar across different job titles, with the exception of students where the level of agreement is less; 57.9% compared with over 70% for most of the other occupations. One interpretation of this result might be that student respondents have been involved in systems design/development for too short a time to be able to say they have 'changed the way' they work. There is a small difference between the genders, females more likely to disagree or strongly disagree (16% total, vs 10% of males), and less likely to agree or strongly agree. This gap could, to some extent, be accounted for in part by a higher proportion of the female respondents than the males being students.



Overall, further work is required to determine the extent to which privacy compliant design is becoming common practice amongst those designing and developing information systems.



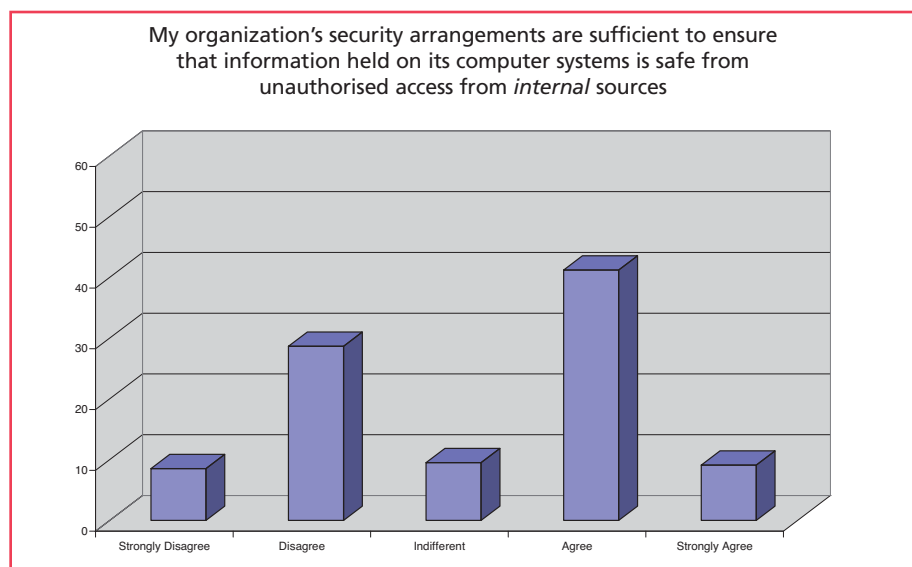
4.6 Security

Over the first four surveys, the proportion of respondents who agreed or strongly agreed that their organization's computer-held data was secure from unauthorised access from *external* sources fluctuated from a high of 81% in 1998 to a low of 62% in 2002. There was a consistently lower level of confidence in the security of organizational data from *internal* sources; agreement that data was secure varied between 51% and 59%.

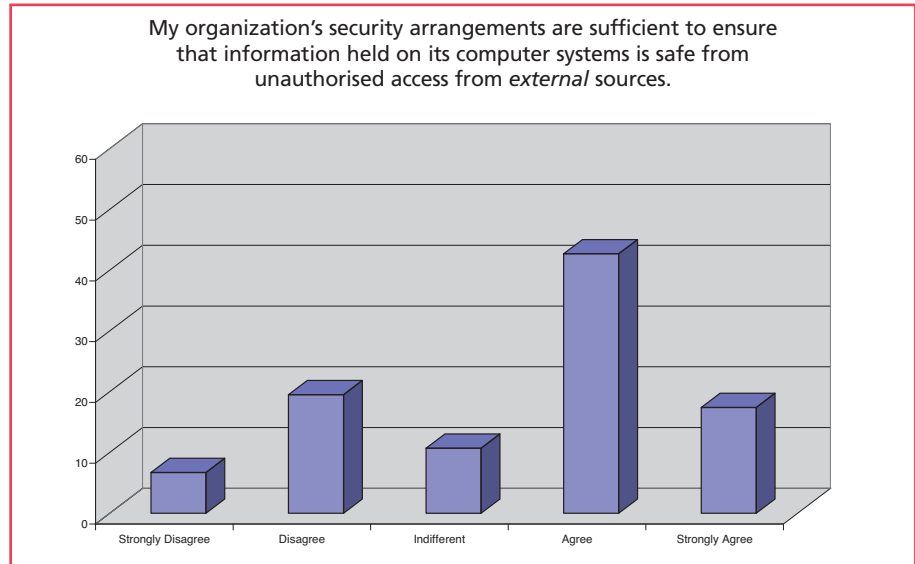
Once again, there was a different pattern of responses in 2006, which appears to have been due to the variation in the profile of respondents to that survey (see Section 3), as the 2009 responses are more in line with those of the earlier surveys.

With respect to *external* sources, 60.2% of respondents agree or strongly agree that their organization's data is secure from unauthorised access. The figure is 50.3% for *internal* sources. These overall percentages hide some variation according to type of organization.

The most confidence in the security of their organization's data is shown by respondents working in the computer industry. Of these, 82.6% agree that their organization's security arrangements are sufficient to ensure that information held on its computer systems is safe from unauthorised access from *external*, and 71.7% from *internal* sources. For those working in non-computer industries, the figures drop to 72.7% and 61.8% respectively. For those working in public service the figures are lower still; 61.5% for *external* and 59% for *internal* sources. But it is respondents working for academic employers who display the lowest level of confidence in the security of their organization's information: just 49.7% agree that it is safe from unauthorised access from *external* and 38.9% from *internal* sources. This confirms the findings of earlier surveys, that it is those working in academic institutions who perceive their employers as having less data security than respondents working in other types of organization.



These questions about security arrangements showed a difference of opinion between male and female respondents. Access from *external* sources was seen as a problem by 33% of females (vs 25% of males) across all sectors (adding 'disagree' and 'strongly disagree'). But the contrast was even more notable for *internal* threats.



More females felt that their organization's security arrangements were insufficient to ensure that information was safe from internal sources (49%) than felt they were sufficient (41%). By contrast, 34% of males overall felt security was insufficient, and 55% agreed or strongly agreed it was sufficient. This is the one instance we have spotted of a clear disagreement in direction of opinion between the genders. As with other questions where we have a noticeable difference of opinion between the genders among our respondents, we cannot tell whether gender is behind the lower level of confidence among those in academic institutions, whether industry sector is behind the apparent difference of opinion between the genders (due to our distorted sample), or whether both have effects that reinforce each other.

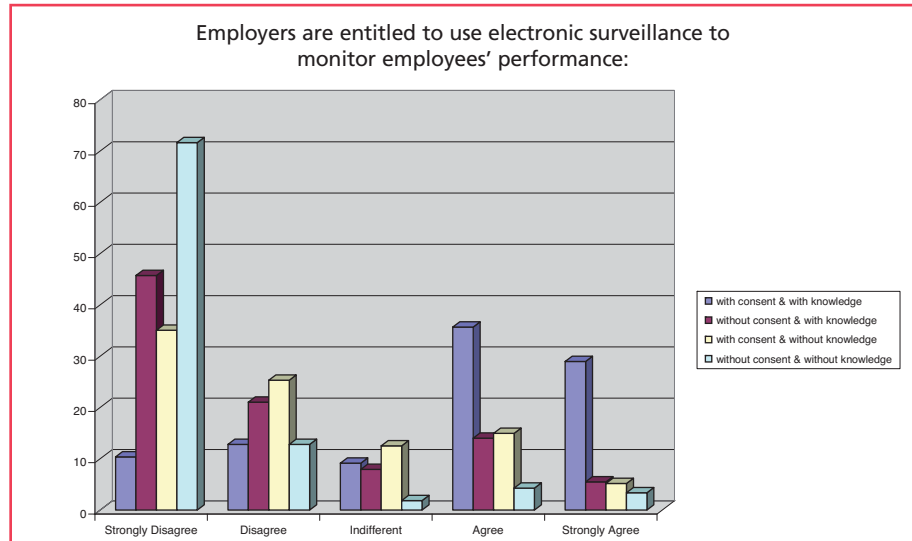
We re-iterate the comment made in the previous survey report that taken together with the findings on privacy (see section 4.5) there is a clear warning to organizations in general, but perhaps to academic institutions in particular, to review both the technical aspects of the security of their systems and also the human resource management issues. Policies and practice relating to data security need to be carefully scrutinised and their effective communication to and deployment by employees continually reviewed.



4.7 Electronic Surveillance of Employees

A statement detailing the entitlement of employers to monitor their employees' performance with various combinations of their knowledge and consent has been used since the 2000 survey. In the 2000, 2002 and 2004 surveys we found 74%-80% agreement that employers are entitled to monitor with both their employee's consent and knowledge. The proportion agreeing with the entitlement to monitor with neither consent nor knowledge had increased slightly each year, to reach 20% in 2004. Responses to the other combinations presented suggested that respondents considered employees' consent to be slightly more important to obtain than their knowledge before carrying out performance monitoring.

The 2006 survey responses differed from those of the earlier surveys; there was a drop in the proportion of respondents agreeing that employers are entitled to monitor both with and without the consent and knowledge of their employees. The 2009 survey results show a similar trend; the majority who agree that employers are entitled to use electronic surveillance with employees' knowledge and consent is 65.7%, much the same as 2006 but less than in the previous surveys. This time only 7.7% agree to use without either employees' knowledge or consent; down from 11% in 2006 and the highest level of 20% in 2004. The finding of earlier studies, that respondents consider employees' consent to be slightly more important to obtain than their knowledge, is confirmed by the results.



We speculated in previous reports that in an apparent trend towards the greater acceptance of the electronic monitoring of employees, we were seeing an effect of the increasing level of surveillance at all levels of contemporary society. It may have been the case that there was such a trend among the respondents to our surveys; however it now appears to have been reversed. It may be that a difference in the profile of the respondents from those who responded to the earlier postal surveys accounts for this. An alternative explanation is that there has been more awareness raised about the extent of surveillance in all areas of life and the potential dangers to civil liberties that accompany it. This could perhaps be the result of an expansion of surveillance capacity that was initially accepted but some respondents now feel has 'gone too far'. Further research would be needed to reveal which explanation is the more likely.



As it is IS professionals who are likely to be involved in the development, installation and maintenance of some types of electronic surveillance software and equipment, that they should be sensitised to potential ethical issues in the use of these technologies is important. In addition, they need to be aware of any legal requirements that may exist in their country of employment, such as the Data Protection and Human Rights Acts in the UK.



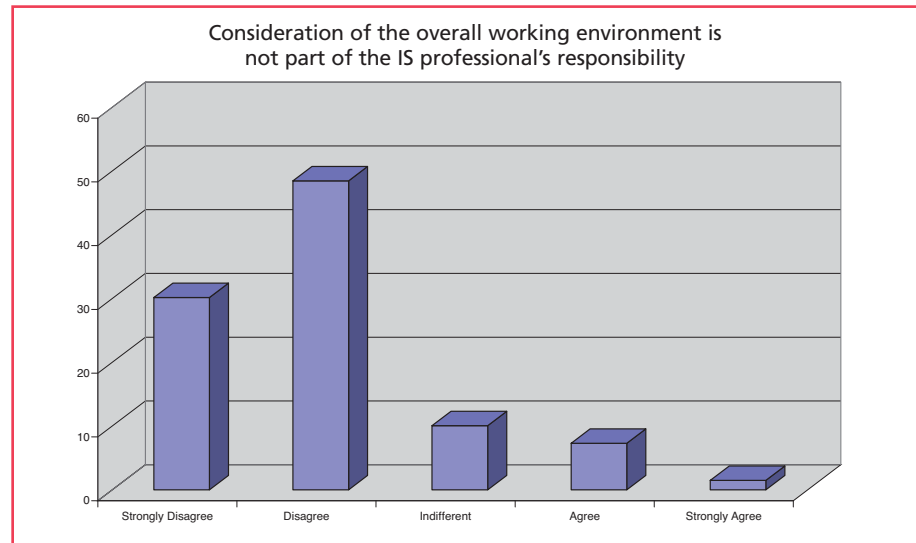
With electronic surveillance becoming a more ubiquitous part of life, there continues to be a need for a debate about its deployment in the workplace. Educators of the next generation of IS professionals have the responsibility to raise their students' awareness about the ethical, legal and people-management issues surrounding the use of electronic surveillance technology. More research is required to examine its effect on employees and to produce guidelines about whether and in what circumstances such surveillance techniques are acceptable and what policies should be in place to protect the interests of all those involved.



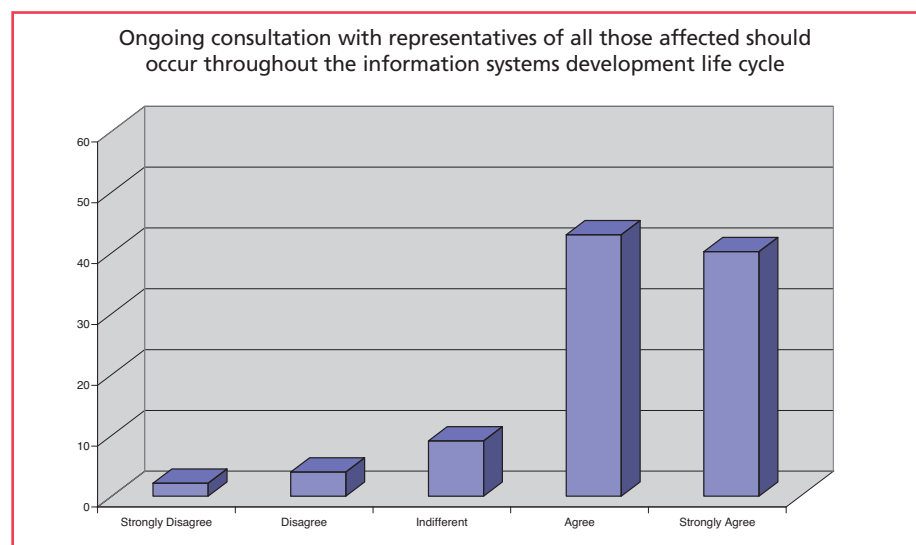


4.8 Responsibility to users/clients

Several statements, worded in slightly different ways, were designed to find out respondents' views of their responsibility to clients and to users. Again, for some of these statements, the responses to the current survey are more in line with those of the first four surveys than those of the 2006 survey with its unique cohorts of respondents. For other statements there are some interesting trends, and for all of them the responses appear to be influenced by the respondents' age and experience.



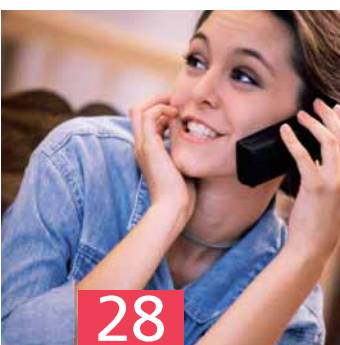
In response to the statement, '*Consideration of the overall working environment is not part of the IS professional's responsibility*', nearly 80% of respondents either disagree or strongly disagree. This is similar to the first four surveys where between 75%-90% of respondents expressed disagreement. The responses are similar across all job titles and age groups.



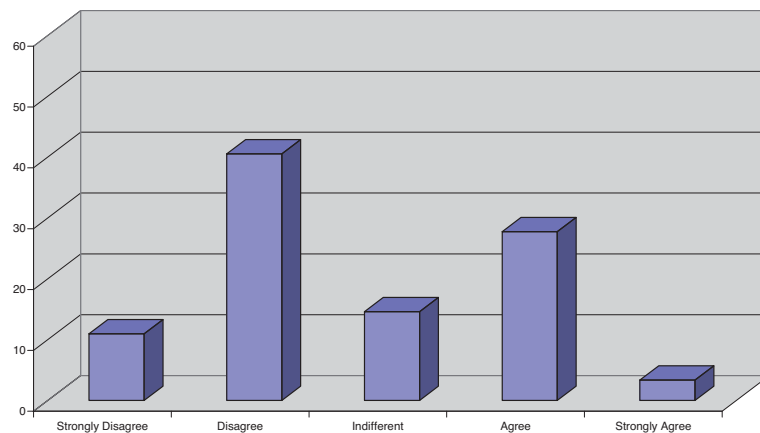
With respect to the statement, *'Ongoing consultation with representatives of all those affected should occur throughout the information systems development lifecycle'*, there is agreement from 83.95% of respondents. Agreement is particularly high among the managers/directors of IS at 93.6%, compared to between 70%-80% of other occupations.



More variation in responses is seen to the statement, *'When disagreements arise between development personnel and those affected by the system, it is the project manager who should have the final say'*. Overall, 52.2% of respondents either disagree or strongly disagree, with 31.5% agreeing or strongly agreeing. Managers/directors of IS show the highest levels of disagreement, at 63.8%, with students the lowest (36.8%). Both age and experience affect responses. It is only among the under 25s that more respondents agree (48.6%) than disagree (40%) that the project manager should have the final say. In the over 40s, nearly 60% disagree with less than half that proportion agreeing. Age and experience are linked, consequently among respondents with 10 or more years of experience, over 60% disagree. Earlier surveys found respondents to be fairly evenly split in their response to this statement; there has been a shift towards the view that the project manager should not have the final say when there are disagreements.



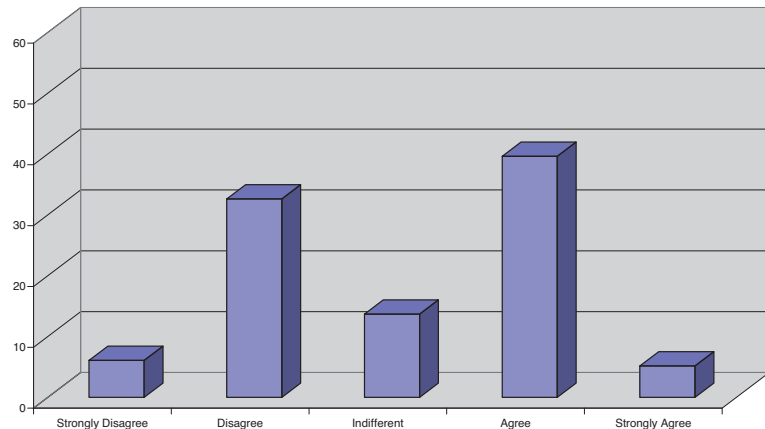
When disagreements arise between development personnel and those affected by the system, it is the project manager who should have the final say



As we noted in 1998 that the way in which the concepts of 'consultation' and 'responsibility' were interpreted by respondents were open to question, from the 2000 survey we included an additional statement, *'Consultation with all stakeholders in an information systems development project is not always possible; to keep stakeholders informed is sufficient'*.



Consultation with all stakeholders in an information systems development project is not always possible; to keep stakeholders informed is sufficient



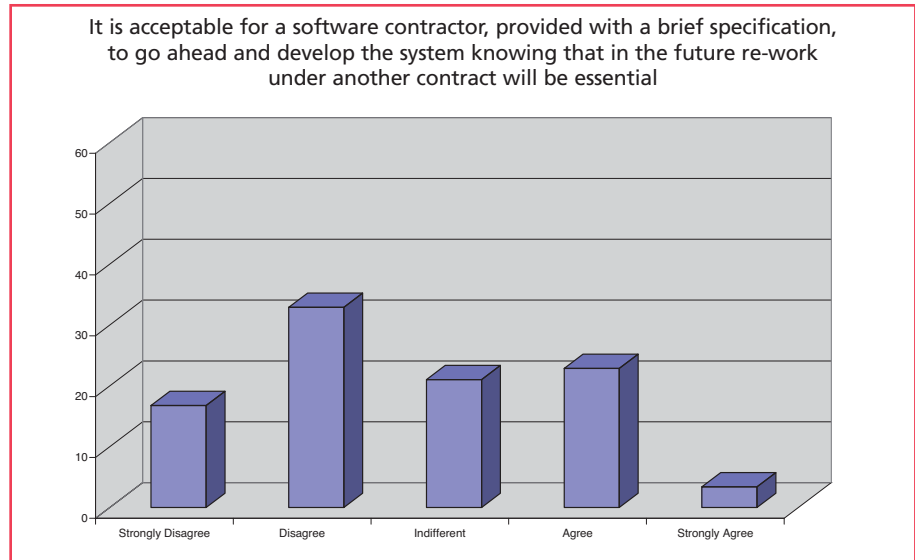
In each survey up to and including 2006, there was a reduction in the level of disagreement with this statement; however the 2009 survey has reversed this trend:

	Agree/ Strongly Agree	Indifferent	Disagree/ Strongly Disagree
2009	45	13	39
2006	53	17	21
2004	54	13	28
2002	47	15	31
2000	46	11	44

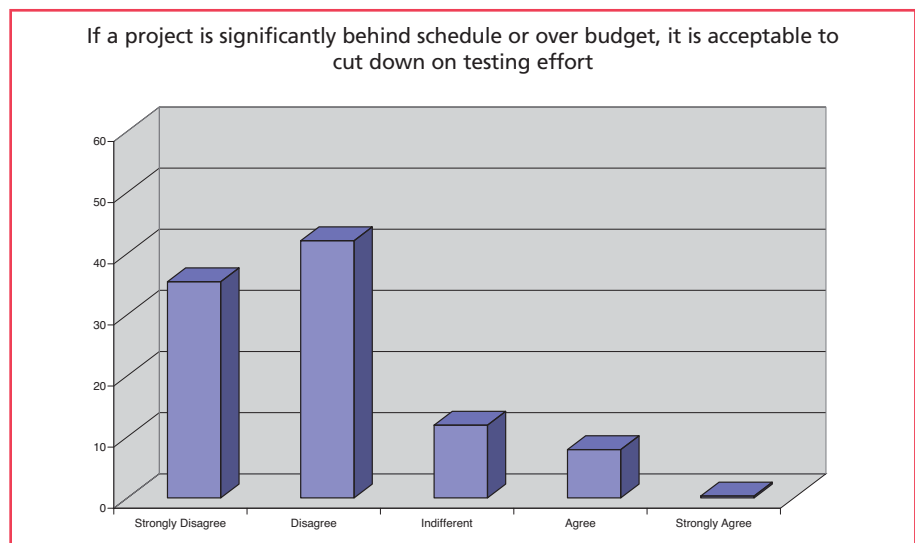
Once again there is a marked difference of response according to job title and age. Among managers/directors of IS and project managers just over 51% disagree that 'to keep stakeholders informed is sufficient', with around 38% agreeing. However, only 23.7% of students disagree, with 63.2% agreeing. The effect of experience is even more stark; among those with less than 1 year's experience, 52.8% agree that 'to keep stakeholders informed is sufficient', with only 27.8% disagreeing. Those aged 25-40 are more evenly split with just over 40% in each of the 'agree' and 'disagree' camps. Only among the over 50 group do more disagree (48.9%) than agree (38.5%) with the statement.

In reporting the results of previous surveys we noted that an ethically acceptable approach to systems development requires consultation that embraces meaningful involvement of representatives of those affected. Employees should have some input into any redesign of their working environment brought about by the introduction of new information systems. Practitioners with more experience appear to appreciate the importance of meaningful involvement of stakeholders beyond the project team. There is work to be done to persuade younger practitioners and students that all stakeholders in an information systems development project need to be a part of the decision-making process beyond a 'consultation' which may subsequently be ignored. Those in education and the professional societies have a role to play in encouraging young IS professionals to adopt a more participative approach.

The statement, 'It is acceptable for a software contractor, provided with a brief specification, to go ahead and develop the system knowing that in the future re-work under another contract will be essential' implies a level of deceit to the client. Overall 26.2% of respondents agree, and 50.3% disagree, with the statement.



Once again, there are variations according to job title and age. Among student respondents, more than half agree and just 31.6% disagree that it is acceptable to, effectively, deceive the client. Among the overlapping groups of those under 25 years of age, half agree and 22.9% disagree with the statement. With each age band the level of disagreement grows until it reaches over 60% with the over 50s; the level of agreement correspondingly decreases to just 19.3%. These results confirm the evidence from previous surveys. It remains a cause for concern that there is such a high level of endorsement of a business practice that lacks openness with the IT services customer.





The response to the statement that, *'If a project is significantly behind schedule or over budget, it is acceptable to cut down on testing effort'* is more encouraging. The minority agreeing that to cut down on testing is acceptable had grown in each of the surveys between 1998 and 2004. In 2006 there was a decrease in the level of agreement and an increase in disagreement; this has continued in 2009:

	Agree/ Strongly Agree	Indifferent	Disagree/ Strongly Disagree
2009	8	12	78
2006	12	10	77
2004	22	5	68
2002	19	9	69
2000	17	10	74
1998	15	3	82

Among student respondents, 15.8% agree with the statement, as compared with a much smaller proportion of respondents with each of the other job titles. Likewise, among those aged under 25 and with less 4 years or less experience, nearly 14% agree that it is acceptable to cut down on testing effort, twice the proportion of older, more experienced respondents. This supports the findings of previous surveys.

It is encouraging to note that the majority of respondents recognise that it is not acceptable to cut down on testing effort when a project is subject to time or budget pressures. Nevertheless, it remains the case that employing organizations have a responsibility to provide an environment that encourages ethical practice and to ensure that commercial pressures to meet budgetary and other deadlines do not lead to ethically dubious practices such as cutting down on testing. Project leaders have a responsibility not to agree to unrealistic deadlines that could result in such pressures being applied; professional societies have a supportive role to play in helping members to maintain their integrity in the face of pressure from employers.

4.9 Licensing of IS Professionals

A statement to the effect that, 'The licensing of computer professionals should be introduced into my country' was introduced in the 2000 survey. The overall responses to this statement are similar to those of previous surveys. Unlike 2006 (when we found students less likely to agree with, and more likely to be indifferent to, the statement), there is a similar response this time from all 'job title' groups. However, there is some variation between respondents from different countries.



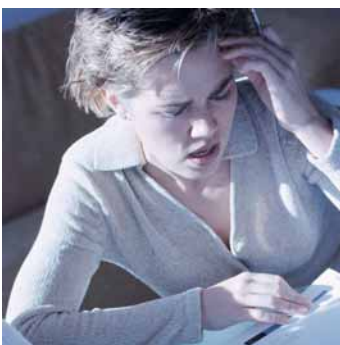
There is, this time, a sufficient number of respondents from some countries to be able to compare their responses; for others, where there are only a handful of respondents in a country, it is possible to look at them by continent. A comparison on this basis gives the following results:



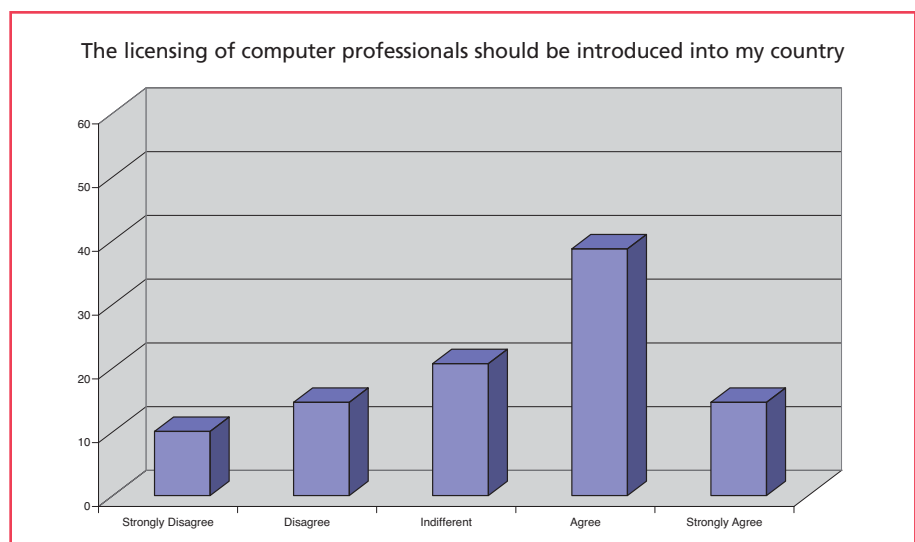
Country/Continent	Number of respondents	Agree/Strongly Agree	Indifferent	Disagree/Strongly Disagree
Africa	39	84.6%	7.7%	7.7%
Australia	11	63.6%	9.1%	27.3%
UK	154	42.2%	24.7%	31.8%
Rest of Europe	32	65.6%	25%	9.4%
USA	27	29.6%	22.2%	48.1%



The high level of support from African respondents is in line with findings from the 2002 and 2004 surveys which both had a significant number of African respondents. The 2009 survey is the first one to include a reasonable number of respondents from the USA and Australia. There are too few Australian respondents to be able to draw much conclusion from their responses, but it is interesting to note that they are in line with the views of Europeans, when excluding the UK. The lowest level of support for licensing is found among respondents from the USA, with UK respondents falling between them and the rest of Europe/Australia.



These findings have to be treated with caution, given the low numbers from each geographical area. Nevertheless they highlight some intriguing differences which are worthy of further investigation. Overall, there remains scope for a more widespread debate about the licensing of professionals, led by the professional bodies.

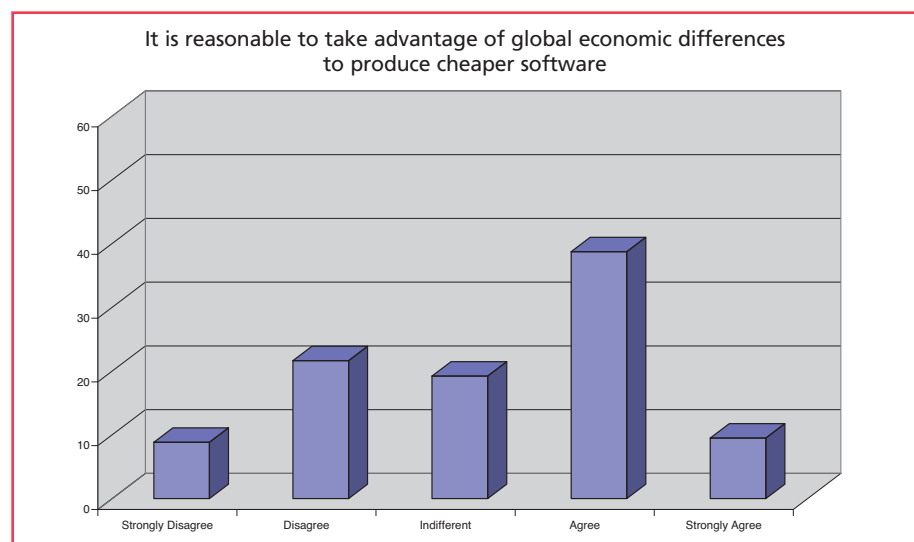




4.10 Globalization

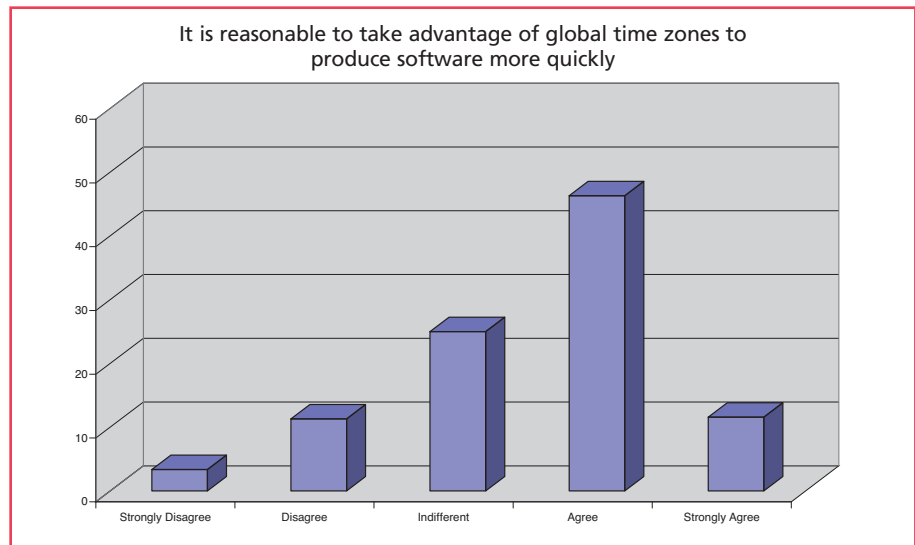
Two statements concerning globalization have been included since the 2000 survey. These are, *'It is reasonable to take advantage of global economic differences to produce cheaper software'*, and *'It is reasonable to take advantage of global time zones to produce software more quickly'*.

The responses to producing cheaper software have a different profile to the 2006 and 2004 surveys. Overall those agreeing or strongly agreeing slightly decreased to around 49%. Those disagreeing or strongly disagreeing increased to around 30%. At 19% more are indifferent. There are differences across countries. The responses from Australia and USA agree or strongly agree the most at around 55% and 63% respectively. Around 29% of respondents in the UK are indifferent but at around 45% the UK has the lowest number agreeing or strongly agreeing. At around 51% Africa has the second lowest responses that agree or strongly agreed and at around 38% has the highest disagreeing or strongly disagreeing.



The responses regarding producing software more quickly have a different profile to the 2006 and 2004 surveys. Overall those agreeing or strongly agreeing increases to around 58% compared with 2006 but is the same when compared to 2004. Those disagreeing or strongly disagreeing reduces to around 15%. At 25% more are indifferent. There are differences across countries. Around 70% of the responses from Australia and USA agree or strongly agree. A third of respondents in the UK are indifferent. At around 51% Africa has the lowest responses that agree or strongly agree.

As in previous surveys it is of concern that the largest number of respondents agree that it is reasonable to exploit global economic differentials to produce cheaper software. However, there is less indifference and a greater number opposing this strategy with Africa having the greatest opposition. The responses from the USA show the greatest desire to exploit economic differences to achieve cheaper software. As a so-called developed country, the profile of the UK is surprising and perhaps reflects the multicultural backgrounds of respondents.



The use of global time zones to produce software more quickly seems to have become an accepted norm since less than 15% are opposed to the concept. However there are large differences between countries. The very high support in Australia and USA suggests a need for software on demand. However there is significant opposition in both countries resulting in the greatest polarisation of responses. Africa has the least support for this strategy whilst the UK has the largest indifference.



4.11 Responsibility for loss of personal data

Two questions were included for the first time in the 2009 survey concerning responsibility for the loss of personal data. The first asked, ‘When security breaches occur, meaning that substantial amounts of personal data could potentially be accessed by unauthorised people, who do you consider responsible?’

Few respondents considered any groups to have ‘sole responsibility’, with 4.6% attributing ‘sole responsibility’ to end users and 3.7% to senior managers.

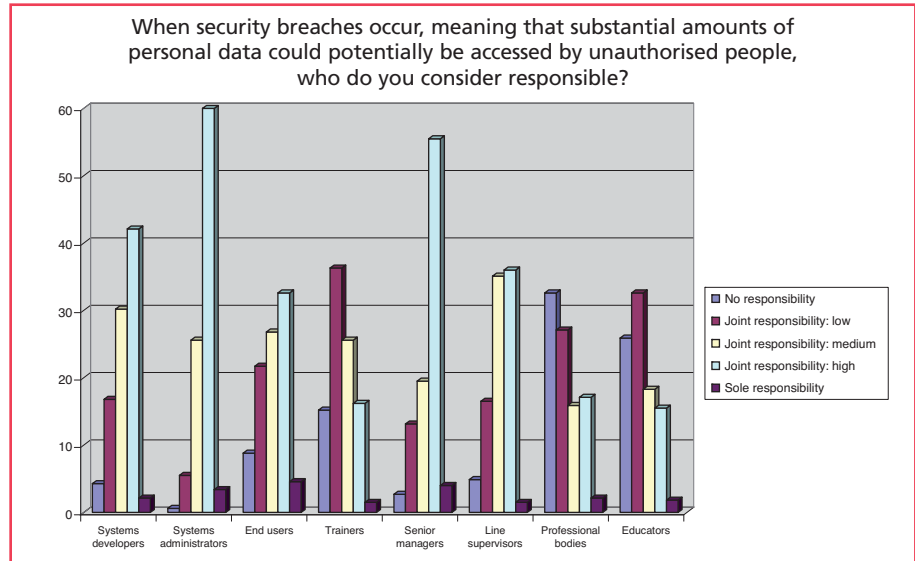
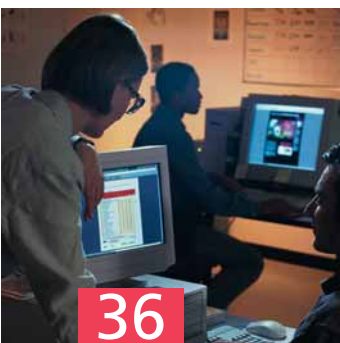
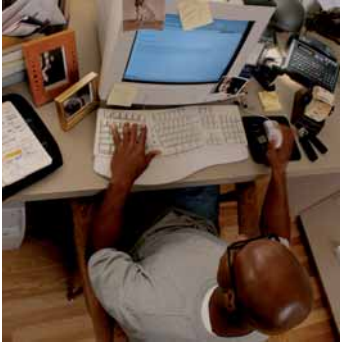
Where joint responsibility was attributed, respondents considered the levels of responsibility to be as follows (with those considered to have the highest levels at the top of the table):

	Joint Responsibility		
	High	Medium	Low
Systems Administrators	60.2%	25.9%	5.6%
Senior Managers	55.6%	19.4%	13.3%
Systems Developers	42%	30.6%	16.4%
Line Supervisors	35.8%	35.2%	16.7%
End Users	32.7%	26.9%	21.9%
Professional Bodies	17%	16%	26.5%
Trainers	16%	25.6%	36.4%
Educators	15.7%	17.9%	32.4%

It is interesting to notice that unlike for sole responsibility, ‘end users’ are well down the ranking for a high level of joint responsibility. For ‘line supervisors’, ‘systems developers’ and ‘systems administrators’, for every 20 people, or so, who say these groups had a high level of joint responsibility, one would say that the group had ‘sole responsibility’. By contrast, for every 7 people who said ‘end users’ have a high level of responsibility, one would say they had ‘sole responsibility’. This suggests not so much a difference in degree of responsibility attributed, as a difference in thought processes towards end users among (at least some of) those who attributed sole responsibility to end users.

While few respondents considered any groups to have ‘sole responsibility’, around one-third said ‘professional bodies’, one-quarter ‘educators’ and 16% that ‘trainers’ have *no responsibility*. There is little variation between respondents from different types of employer, with different job titles or from different countries.

Thus all the groups listed were considered to have some responsibility by a majority of respondents. Senior managers were clearly given more responsibility than line supervisors by our respondents: this was not just a case of greater numbers attributing high responsibility *instead* of sole or medium responsibility, though, since a total of 78.7% of our respondents attributed one of ‘sole, high or medium’ responsibility to senior managers, against 72.2% for line supervisors. Our respondents were both overall more willing to attribute responsibility to senior managers and within that more willing to attribute greater shares of responsibility to senior managers than line supervisors.

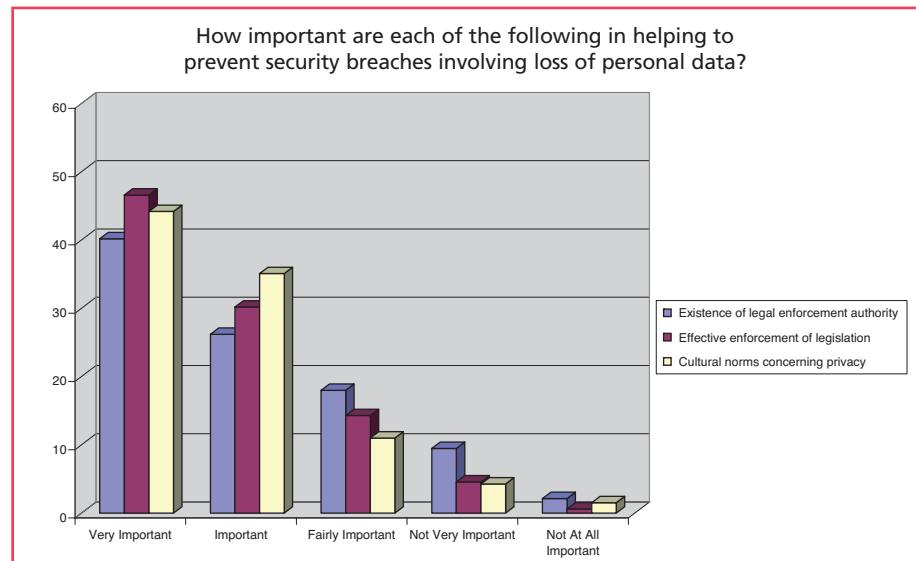


In terms of 'other' groups with responsibility, several respondents mentioned the perpetrators of the security breach (crackers/hackers). Others named as having responsibility were Security Officer, Risk Manager, Business Owners, CEO, Directors, Systems Testers, corporate culture and 'everyone'.

The overall messages from our respondents seem to be that responsibility is shared, but many are willing to attribute a higher level of responsibility to (more senior) managers and systems administrators. While many attribute some responsibility to each of trainers, professional bodies and educators, in none of those cases were a majority of our respondents willing to attribute more than a low level of responsibility to these groups.



The second question asked, 'How important are each of the following in helping to prevent security breaches involving loss of personal data?' It can be seen from the chart of responses that the mere existence of a 'legal enforcement authority' is considered less important than 'effective enforcement' of legislation. It is noteworthy that cultural norms are considered to be almost of as much importance as effective enforcement, and of more importance than the existence of a legal enforcement authority.



Our respondents are clearly aware that there is a danger of a facade of enforcement, and could well prove sceptical if faced with an 'initiative' that results in a new enforcement authority.

The responses were consistent across the different groups of respondents.

5. RECOMMENDATIONS

The change in distribution method of the 2009 survey enabled responses to be gathered from a larger number of respondents than to earlier surveys, representing a range of age, experience, employing organization and country of employment. While there is a high level of ethical awareness among all respondents to many of the issues raised, the findings tend to confirm the observation made in previous survey reports that age and (lack of) experience have an affect on the attitude to some issues. There remain a number of areas where more discussion during the education and preparation for professional practice is required, and where more guidance and support for individuals in the workplace is desirable to encourage consistently responsible behaviour.



Among those respondents working in an academic setting there appears to be a different attitude towards intellectual property rights than those working for other types of employer, as well as less support for policies at the organizational level and a higher level of support for the use of employer's facilities for non-work-related activities. Those working for academic institutions also have less confidence in their organization's data security measures. There are some clear messages here for the senior management in academic institutions to heed.



Our recommendations for organizations, for professional societies and for educators are intended to promote more socially responsible practices within the Information Systems community.



Over the six surveys we have found some issues about which there is a fairly consistent level of agreement despite the changing profile of our respondents. We have also found some interesting differences between groups of respondents, with age, employing organization and geography possibly influencing attitudes towards some issues. However, our findings raise more questions than they answer and further research is required to investigate their validity. We have included suggestions for further research among our recommendations for the academic community, however it is to be hoped that organizations and professional bodies will lend their support to such research efforts with the aim of promoting a greater understanding of the factors that will help foster socially responsible practice.





It is recommended that organizations should:

- seriously consider adopting a Code of Conduct for all employees;
- increase efforts to promote awareness among all employees of:
 - ethical issues
 - the organization's Code of Conduct
 - how the organization's Code of Conduct may be applied to guide ethical decision-making;
- establish 'whistle-blowing' procedures to encourage employees who become aware of unethical practices within the organization to come forward;
- introduce a clear policy concerning the use of computing resources by employees for their own activities, and consider allowing the use for selected non-profit-making activities as a contribution to the local community or as a legitimate perk for employees;
- establish clear guidelines for the introduction and operation of any electronic surveillance process, including email and internet usage monitoring, ensuring that all employees are fully consulted and that their rights to privacy in the workplace are respected;
- review on a regular basis the security of computer-held data with attention to both technical aspects and management aspects affecting potential threats;
- consider and clarify their policy concerning the re-creation of intellectual property such as a product, program or design by employees when they move to another employer;
- ensure that all policies are clearly communicated to employees, in particular to student and new graduate employees, and are deployed throughout the organization;
- promote an approach to systems development that encourages genuine stakeholder involvement in decision-making;
- improve the promotion of data protection awareness among staff and review the means by which compliance with data privacy and data protection requirements are assured;
- make greater efforts to provide a working environment that encourages ethical practices, supporting employees in resisting the temptation to allow commercial pressures to lead to ethically dubious practices - instead, promoting their ethical stance to their commercial advantage.

It is recommended that professional societies representing the IS profession should:



- ensure that their Code of Conduct remains up-to-date and relevant to the profession, increasing efforts to promote awareness of the Code among members and providing guidance how it can be applied in practice;
- provide a greater degree of particular support for their younger members, helping them to acquire greater awareness of the ethical issues they will encounter throughout their careers;
- promote debate of the continuing applicability of legislation such as the software licensing laws, in the light of current developments, opinion and practice;
- promote debate concerning the desirability of licensing for information systems professionals;
- promote members' awareness of the role that IS staff play in the designing of data privacy and data protection compliance into information systems.

It is recommended that the academic community responsible for the education of future IS professionals and for research into IS-related issues should:

- address ethical issues more extensively in their curriculum, to raise the awareness of young, aspiring professionals concerning all of the issues covered in this survey;
- include in their research agenda the issues identified by this survey as requiring further investigation, for example:
 - the effects of factors such as age, geography and culture on attitudes to issues such as intellectual property, privacy and security, the use of employer's computing facilities, software and systems testing and the licensing of IS professionals;
 - the factors affecting the IS professional's ability to choose and choice of what projects they work on;
 - the effect of workplace monitoring on employees and guidelines for the ethical use of employee surveillance;
 - the implications of the globalization of the IS profession and recommendations for socially responsible practice in this area.



APPENDIX

SURVEY OF IS PROFESSIONALS' ETHICAL ATTITUDES

2009 ETHICOMP® SURVEY OF ETHICAL ATTITUDES

The purpose of this questionnaire is to determine the attitude of managers, practitioners, trainees, educators and students to a range of ethical issues.



This sixth ETHICOMP® survey is being sponsored by the Institute for the Management of Information Systems and we would appreciate you spending a few minutes of your time to take part.

Your responses may be made anonymously and will be treated with the strictest confidence.

However, you have the option of identifying yourself if you are willing to take part in any follow-up to the survey.

The survey results will be discussed in a future issue of the IMIS Journal, and a full report of the findings will be published. Thank you for your co-operation.



Please circle the answer which represents the extent to which you agree or disagree with each statement:

If a question does not apply to you, please leave it and go on to the next one.



1. It is acceptable for me to make unauthorised copies of commercial software to use at work.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------

2. I would refuse to work on a project that I considered to be unethical.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------

3. Ongoing consultation with representatives of all those affected should occur throughout the information systems development life cycle.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------

4. It is acceptable to use my employer's computing facilities for my own *non-profit-making* activities if this has no adverse affect on my employer.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------

5. It is acceptable to use my employer's computing facilities for my own profit-making activities if this has no adverse affect on my employer.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------



6. If an organization has purchased/developed software for use in the office, it is acceptable for employees to make unauthorised copies of this software for use at home.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------

7. I think that all organizations should require all employees to abide by a code of professional ethics.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------



8. If a project is significantly behind schedule or over budget, it is acceptable to cut down on testing effort.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------



9. The licensing of computer professionals should be introduced in my country.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
10. Employees should be allowed to recreate a product / program / design for another organization if they change jobs and are no longer employed by the organization who paid them to create it.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
11. When disagreements arise between development personnel and those affected by the system, it is the project manager who should have the final say.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
12. Providing a systems development project provides me with an interesting challenge, I do not care about its overall objectives or purpose.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
13. It is acceptable for me to use other employees' access codes *with* their permission to access data I am not authorised to see.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
14. It is acceptable for me to use other employees' access codes *without* their permission to access data I am not authorised to see.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
15. It is acceptable for me to make unauthorised copies of commercial software for my own private use.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
16. My organization's security arrangements are sufficient to ensure that information held on its computer systems is safe from unauthorised access from *internal* sources.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
17. My organization's security arrangements are sufficient to ensure that information held on its computer systems is safe from unauthorised access from *external* sources.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
18. Organizations should develop and administer an ethics awareness programme for all employees.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
19. It is acceptable for a software contractor, provided with a brief specification, to go ahead and develop the system knowing that in the future re-work under another contract will be essential.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
20. Consideration of the overall working environment is not part of the IS professional's responsibility.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|
21. It is reasonable to take advantage of global economic differences to produce cheaper software.
- | | | | | |
|-------------------|----------|-------------|-------|----------------|
| strongly disagree | disagree | indifferent | agree | strongly agree |
|-------------------|----------|-------------|-------|----------------|



22. It is reasonable to take advantage of global time zones to produce software more quickly.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------

23. The increasing need for privacy and data protection has changed the way in which I design or develop information systems.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------

24. Consultation with all stakeholders in an information systems development project is not always possible; to keep stakeholders informed is sufficient.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------

25. I think that all organizations should require IS/IT employees to abide by a code of professional ethics.

strongly disagree	disagree	indifferent	agree	strongly agree
-------------------	----------	-------------	-------	----------------

26. Employers are entitled to use electronic surveillance to monitor employees' performance:

a	strongly disagree	disagree	indifferent	agree	strongly agree
---	-------------------	----------	-------------	-------	----------------

(a) *with* their consent & *with* their knowledge

b	strongly disagree	disagree	indifferent	agree	strongly agree
---	-------------------	----------	-------------	-------	----------------

(b) *without* their consent & *with* their knowledge

c	strongly disagree	disagree	indifferent	agree	strongly agree
---	-------------------	----------	-------------	-------	----------------

(c) *with* their consent & *without* their knowledge

d	strongly disagree	disagree	indifferent	agree	strongly agree
---	-------------------	----------	-------------	-------	----------------

(d) *without* their consent & *without* their knowledge.

27. To what extent do you feel able to refuse to work on a given project?

I have a free choice of projects to work on	I can sometimes choose not to work on a project	I have no choice about the projects I work on
---	---	---

Does your employing organization have a policy concerning the use of computing facilities by employees for non-work related purposes?

28	Formal, written policy	Informal policy	No policy	Don't know
----	------------------------	-----------------	-----------	------------

28. Software (e.g. game playing)

29	Formal, written policy	Informal policy	No policy	Don't know
----	------------------------	-----------------	-----------	------------

29. Printers and other peripherals

30	Formal, written policy	Informal policy	No policy	Don't know
----	------------------------	-----------------	-----------	------------

30. Email

31	Formal, written policy	Informal policy	No policy	Don't know
----	------------------------	-----------------	-----------	------------

31. Internet

32. Anything other than above? Please state for what, and whether it is a formal or informal policy.

32	Formal, written policy	Informal policy	No policy	Don't know
----	------------------------	-----------------	-----------	------------



When security breaches occur, meaning that substantial amounts of personal data could potentially be accessed by unauthorized people, who do you consider responsible? Please indicate the level of responsibility held by each of the groups below:

	No Responsibility	Joint Responsibility			Sole Responsibility
		Low	Medium	High	
33. Systems developers					
34. Systems administrators					
35. End users					
36. Trainers					
37. Senior Managers					
38. Line supervisors					
39. Professional Bodies					
40. Educators					
41. Other groups? <i>Please state who, and the level of responsibility held</i>					

How important are each of the following in helping to prevent security breaches involving loss of personal data?

42. Existence of a Legal Enforcement Authority	very important	important	fairly important	not very important	not at all important
43. Effective enforcement of legislation in cases of security breaches	very important	important	fairly important	not very important	not at all important
44. Cultural norms concerning privacy	very important	important	fairly important	not very important	not at all important

Finally, some questions about you to provide us with a profile of respondents. Please tick the appropriate box.

45. Are you a member of one or more Computing/IS Professional bodies? If so, please indicate which one(s):

IMIS ACS HKCS IFIP
 ACM BCS IEEE

46. Please add the name of any other Computing / IS Professional bodies that you belong to: _____

47. Please indicate which job title best describes your current position:

Manager/Director of IS Business/Systems Analyst
 Project Leader Programmer
 Database Manager Web/Internet Designer
 Network Manager Lecturer/Teacher
 Technical Services Manager Student
 Website Manager Researcher

48. If your job title does not appear in the previous question, please state what it is: _____

49. Please indicate your organization's business:

Private enterprise: Computer industry
 Private enterprise: Non-computer industry
 Public service
 Academic
 Self-employed

50. What is the total number of employees in your organization?

Less than 10
 11-100
 101-500
 501-1000
 1001-5000
 Over 5000

51. In what country are you currently working? _____

52. How long have you worked for your current employing organisation?

Less than one year
 1-4 years
 5-9 years
 10-14 years
 15< years

53. How long have you worked in total as an IS professional?

Less than one year
 1-4 years
 5-9 years
 10-14 years
 15< years

54. Gender: Male
 Female

55. Age: Under 25
 25-40
 41-50
 Over 50

Thank you for taking the time to fill in this questionnaire. Please return it to the following address:
2010 ETHICOMP Survey, Centre for Computing and Social Responsibility, Faculty of Computing Sciences and Engineering, De Montfort University, The Gateway, Leicester, LE1 9BH, UK

All individual responses will be treated as strictly confidential. If you are willing to be contacted as part of any follow-up to the survey, please provide your name and contact details below.

56. Name and contact details if you are willing to take part in further investigation of the ethical attitudes of IS professionals:

I am willing to take part in further investigation of ethical attitudes of IS professionals.

Signature: _____

Name (block capitals): _____

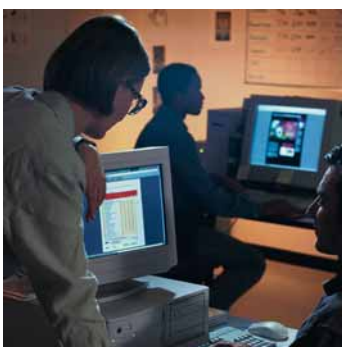
Address: _____

Tel. no. / Email: _____

57. Please indicate which, if any, of the previous IMIS surveys you have taken part in:
 1998 2000 2002 2004 2006

58. If you have taken part in any previous IMIS surveys: may we have your permission to compare your responses to this survey to your responses to the previous one(s)?
 Yes No

Once again, thank you very much for taking part in this survey.





Institute for the Management of Information Systems
5 Kingfisher House New Mill Road
Orpington Kent BR5 3QG UK
Tel: 44 700 00 23456 Fax: 44 700 00 23023
Email: central@imis.org.uk www.imis.org.uk

IMIS

ISBN: 978-0-9535116-1-7
Price: £10