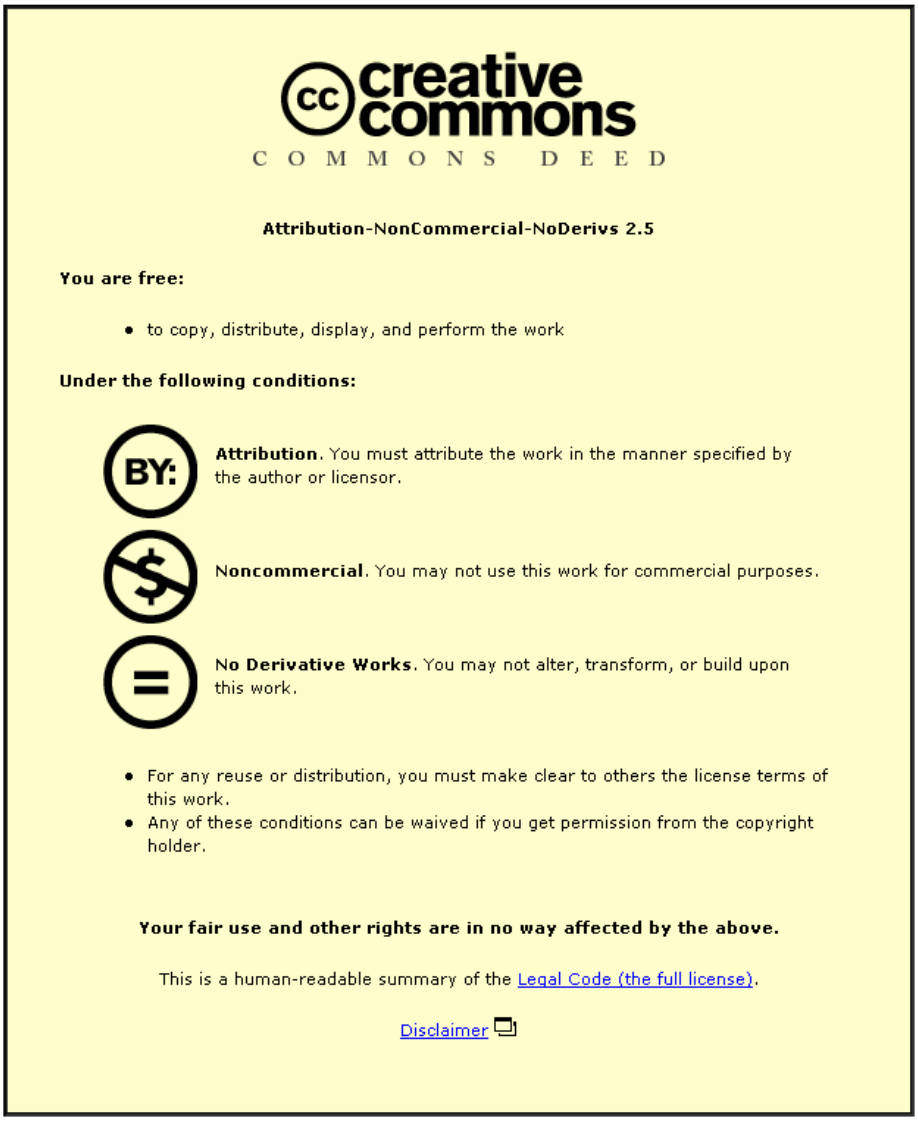

creative commons

COMMONS DEED

Attribution-NonCommercial-NoDerivs 2.5

You are free:

- to copy, distribute, display, and perform the work

Under the following conditions:

BY: **Attribution**. You must attribute the work in the manner specified by the author or licensor.

Noncommercial. You may not use this work for commercial purposes.

No Derivative Works. You may not alter, transform, or build upon this work.

- For any reuse or distribution, you must make clear to others the license terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

Your fair use and other rights are in no way affected by the above.

This is a human-readable summary of the Legal Code (the full license).

Disclaimer

An investigation into the uptake, content, dissemination and impact of information security policies in large UK-based organizations

by Heather Fulford and Neil Doherty

Business School

Research Series
Paper 2002: 4
ISBN 1 85901 180 2

Loughborough University

An investigation into the uptake, content, dissemination and impact of information security policies in large UK-based organizations

by

Heather Fulford and Neil Doherty

Business School Research Series
Paper 2002: 4
ISBN 1 85901 180 2

November 2002

An investigation into the uptake, content, dissemination and impact of information security policies in large UK-based organizations

Dr. Heather FULFORD and Dr. Neil F. DOHERTY

The Business School, Loughborough University,
Loughborough, Leicestershire LE11 3TU, UK.

Mailing Address:

Dr Neil Doherty
The Business School,
Loughborough University,
Loughborough, LE11 3TU,
United Kingdom.

Telephone: 01509 223328 Email: n.f.doherty@ lboro.ac.uk

Fax: 01509 223960

An investigation into the uptake, content, dissemination and impact of information security policies in large UK-based organizations

Abstract: *Despite its widely acknowledged importance, the information security policy has not, to date, been the subject of explicit, empirical scrutiny, in the academic literature. To help fill this gap an exploratory research project was initiated that sought to investigate the uptake, content, dissemination and impact of information security policies in large UK-based organizations. The results of this research have indicated that whilst policies are now fairly common, at least amongst our sample, there is still a high degree of variety in terms of their content and dissemination.*

1. Introduction

Organisations of all shapes and sizes are having to enthusiastically embrace information systems and technologies if they wish to survive, and hopefully thrive, in a highly competitive environment, in which effective operational control and strategic direction are increasingly dependent upon the availability and exploitation of high quality information. Consequently it is vital that adequate security and control procedures are introduced to ensure that all the information embedded within organisational information systems retains its integrity, confidentiality and availability (Dhillon & Backhouse, 2001). However, there is also extensive evidence to suggest that the threat, to the security of organizational information and information systems, are now growing in number, variety and most importantly the severity of their impact (Angell, 1996).

To a very large extent such threats are growing because of higher levels of interconnectivity both within, and between, organisations (Dinnie, 1999:113; Barnard & von Solms, 1998:72; DTI, 2002). In particular, it is the increasing incidence of intra-organisational systems that is creating problems for organisations, as information security is upgraded from being merely a '*domestic*' issue to one that involves third parties, such as external business partners (von Solms 1998:174). The rise of electronic commerce has also heightened awareness amongst organizations of the security threats to which they are likely to be exposed. Indeed, it has been reported that security threats, and fear of security breaches, constitute the greatest inhibitors to an expansion in the uptake of electronic commerce (Ernst and Young survey 2001:1). Increased interconnectivity, is not however, the only factor making computers, and the information therein, less secure. For example, the recognition that information now constitutes a '*key corporate asset*', which is of great commercial value (Gerber, von Solms and Overbeek 2001:32), has also brought information security nearer to the top of the management agenda.

Perhaps inevitably, the increased risk of information security problems has led to a growing awareness among the managers of organizations of the need for careful and effective information security management. For example, it is widely acknowledged that effective information security management is dependent on a number of key factors (von Solms 1998:174; Siponen 2000:31), most notable among these being:

- the need for senior management commitment and support to information security management;
- the detailed assessment of potential security risks and threats;
- the implementation of appropriate controls to minimize or guard against those risks and threats;
- the thorough communication of security issues to users of both information and information systems through relevant education and training.

However, it has also been recognised that effective security management, including all the above factors, is predicated upon the formulation, dissemination and operation of an information security policy. As Hone and Eloff (2002) acknowledge: '*one of the most important controls is the information security policy*', whilst Higgins (1999) notes: the information security *'policy is the start of security management*'.

The importance of the information security policy, as a document of strategic importance within organizations today, is widely acknowledged. Indeed, in the UK, the British Standards Institute have developed a standard (BSI, 1999). Moreover, the issue of information security policies has now become an integral part of a variety of commercial surveys into information security breaches and safeguards (e.g.: Andersen, 2001; Ernst and Young, 2001; DTI, 2002). However, there is little evidence that any empirical research, specifically targeting the uptake, dissemination and impact of information security policies within organizations, has been conducted and published in the academic literature.

The present study seeks to fill this gap by investigating the uptake, content, dissemination and impact of information security policies in UK organizations. Before presenting the methodology, findings and analysis of this study, a focused review of the pertinent literature on information security policy formulation and application is provided.

2. Literature review

This literature review commences with an assessment of some recent surveys into the key issues surrounding information security, which provides a useful context for study, before focussing more specifically on the formulation, dissemination and content of information security policies. The section concludes with a critique of this literature, before presenting the research objectives for this study. It should be noted that the body of literature, reviewed for this section, includes contributions

that are termed '*computer security*' or '*IT security*', rather than '*information security*'. However, in the interests of simplicity, the most commonly used term '*information security*' will be used throughout the paper.

2.1 Information security surveys

A number of major studies of information security have been conducted recently in Europe, most notable among these being the Ernst and Young 2001 survey, the Andersen 2001 survey, and the 2002 DTI study of UK-based large and small businesses and public sector organizations. Table I below summarizes some background details about these studies.

Table I: Background details of recent information security surveys

Survey	Sample size	Location	Research method
Ernst and Young 2001	273	European businesses	Telephone interviews using structured questionnaires with CIOs, IT directors and business executives
Andersen 2001	Approx. 900	European businesses	Questionnaires distributed during business seminars to IT specialists or senior managers
DTI 2002	1000	UK organizations (private and public sector)	Telephone interviews using structured questionnaires with individuals responsible for information security management

Each of these studies has highlighted the prevalence and range of security incidents that European organizations have faced in the past couple of years. A general upward trend has been noted in the number of incidents occurring and in the severity of individual incidents. A key discussion area arising from the studies, and particularly from their emphasis on the impact of internet use on an organization's information security, is that as well as an increase in the number of security incidents occurring, a shift has also been witnessed from internal to external security incidents. More specifically, malicious intrusions in some shape or form (virus, hacking attack, and so on) from outside an organization seem to be more prevalent, and indeed more serious, than the previously more frequent internal issues such as employee error or deliberate damage caused by employees.

These studies, particularly the DTI (2002) study, further suggest that, whilst organizations are generally confident that they have detected the majority of recent attempted security breaches, they expressed less confidence about future security issues, noting that security incidents were increasing both in terms of number and complexity. These survey reports, therefore, convey an important message that there is increasingly good reason for information security management to be high on an organization's agenda, most especially if an organization is conducting any of its operations via the Internet.

2.2 Information security policy: importance and uptake

As noted in the introduction, there is a growing recognition that effective information security management is predicated on the existence and execution of an information security policy. As Higgins (1999) notes: '*without a policy, security practices will be developed without clear demarcation of objectives and responsibilities*'. However, there is also a growing concern that too many organisation are failing to heed this advice, as Moule and Giavara (1995) observe: '*anyone associated with IT will have observed situations where documented policies were grossly inadequate*'. Whilst the importance of, and concerns about, information security policy are widely recognised, this interest has not, as yet, been translated into detailed empirical surveys explicitly targeting the utilisation of information security policies in organizations. However, some interesting insights about information security policy can be gained from the more general studies described in the previous section.

With regard to the uptake of information security policies, the Andersen (2001) study reports that 65% of the organizations surveyed (most of which were large organizations) had an information security policy in place, and the DTI (2002) survey reports that 27% of UK businesses have a policy in place. The DTI study further reports that 59% of the large organizations surveyed had implemented a policy. Significant in these DTI results is that again an upward trend is noted from earlier studies: the DTI (2000) study, for example, reported that only 14% of the organizations surveyed had an information security policy in place. Moreover, the 2002 study noted that a higher proportion of organizations with a policy were undertaking annual policy updates than was the case in 2000.

Interesting in the Andersen (2001) study is the discrepancy between the views of business managers and those of IT managers: 82% of the business managers surveyed believed that their organization had a comprehensive policy in place, whereas only 66% of the IT managers believed this to be the case. This could suggest that a survey targeting IT managers, who presumably typically have a more detailed knowledge of information security issues than do business managers, is likely to yield a more realistic assessment of the information security situation in an organization.

The Ernst and Young (2001) survey found that organizations believed '*employee awareness*' to be the greatest '*challenge to achieving the required level of security*'; a message that is strongly echoed by Siuponen (2000). Given this finding, it seems somewhat concerning that, of the 27% of organizations in the DTI (2002) survey having an information security policy, only 7% of them implemented their policy in order to make employees aware of security issues. The primary motivation reported (by 67% of organizations having a policy) for having a policy was that it was recognized as '*good*

practice' to do so. It was further reported in the DTI (2002) survey that few organizations make their employees aware of information security issues upon induction. It seems, therefore, that whilst policy formulation might be on the increase, an emphasis on dissemination of security concerns to employees and practical policy implementation is very low on the agenda of many organizations.

2.3 Policy content and BS 7799 compliance

The studies undertaken to date have not investigated the specific areas covered by the information policies organizations have adopted, and neither do they appear to have considered the specific impact those policies are having in organizations. A strong indication of the paucity of research in the area of information security policy is provided by Dhillon & Backhouse (2001). Their comprehensive review of the information security literature concluded that existing research tends to focus upon '*checklists* [of security controls], *risk analysis and evaluation*'; information security policy was not explicitly featured in their review. Consequently, little or no empirical data exists on the important issues of policy uptake, content and implementation.

One document that does explicitly tackle the content of the information security policy is the '*Information Security Management'* standard (BSI, 1999). However, the DTI (2000) survey reported that only 25% of the UK businesses surveyed were aware of the existence of this standard. Moreover, in their 2002 survey, disappointment was expressed that only 15% of organizations were aware of the contents of this standard, and only 38% of those aware of its contents had actually adopted the standard in their organization. The standard contains a number of factors cited as critical to the success of information security management in organizations, such as ensuring the policy reflects business objectives, effective marketing of security to employees, provision of security training, and policy performance measurement. To date, despite the existence of the major studies of security issues mentioned in this paper, there seems to be little empirical data to indicate whether organizations are adopting these individual factors, or on the impact the adoption of these factors is having on information security in organizations.

2.4 Research Motivations and objectives

This brief review of the literature has found that whilst the importance of information security is being increasingly recognised, a number of significant gaps exist, particularly in the academic literature. An obvious gap is that whilst a number of major surveys have been conducted to investigate security issues, these have largely been commercially-oriented, rather than formal academic studies. Moreover, these empirical studies have covered a broad range of information security issues, rather than focusing specifically on information security policies. To help fill these gaps an empirical study of the uptake

and application of information security policies was initiated. More specifically, the study addressed the following four research objectives:

1. To investigate the prevalence and updating of documented information security policies, within the UK;
2. To explore the methods used by organisations to disseminate information security policies to their employees;
3. To review the specific area covered by the information security policies that organizations are deploying;
4. To achieve an understanding of the factors that impact upon the successful deployment of the information security policy.

It is envisaged that the present academic-oriented study will, therefore, make an important contribution to the existing body of literature providing insights in security and policy issues from an academic perspective. It is anticipated that these findings can, in turn, be fed back to the relevant practitioner communities, as well as to those involved in the compilation of appropriate national and international standards and guidelines.

3. Research Design

This section describes how a detailed questionnaire, which sought to explore the three stated research objectives, was designed, validated and ultimately executed.

3.1 Questionnaire development, validation and targeting

A draft questionnaire was developed, based primarily upon the results of the literature review, summarised in section 2. As there are few published academic papers explicitly addressing the use of information security policies, the literature was used primarily to generate ideas and insights, rather than as a source of specific questions and item measures that could be utilised directly in this study. The resultant questionnaire was organized into the following four sections:

1. **The existence and dissemination of the information security policy:** This section sought to determine whether a responding organisation had a documented information security policy, and if it did, how long the policy had been in existence, how often it was updated, and how the policy was disseminated.

2. **The coverage of the information security policy:** This section of the questionnaire was designed to evaluate the scope of the information security policy. The respondent was presented with a list

of eleven distinct issues, such as '*disclosure of information*', '*Internet access*' and '*viruses, worms & trojans*' that an information security policy might reasonably be expected to cover. Whilst most of these items had been explicitly identified in the British Standard - BS7799 (BSI, 1999) others had been highlighted in other sources (e.g. Higgins, 1999). For each of these issues, the respondent was invited to indicate whether the issue was covered in '*the policy document only*', '*a stand-alone procedures only*', '*the policy document and a supplementary procedure*', or the issue is '*not explicitly covered*'.

3. **Factors affecting the success of the information security policy:** The British Standard on '*Information Security Management'* - BS7799 (BSI, 1999) suggests that there are ten distinct factors that might influence the success of an information security policy, such as '*visible commitment from management*' and '*a good understanding of security requirements*'. For each of these factors, the respondent was asked indicate its importance, and the extent to which his / her organisation was successful in adopting that factor, using two separate 5 point Likert scales.

4. **Demographics:** Demographic information [organizational size, geographical spread and sector] was also collected so that the potential moderating effect on the statistical analyses could be explored.

The draft questionnaire was initially validated through a series of pre-tests, first with four experienced IS researchers, and then after some modifications it was re-tested with five senior IT professionals, all of whom had some responsibility for information security. The pre-testers were asked to critically appraise the questionnaire, focusing primarily on issues of instrument content, clarity, question wording and validity, before providing detailed feedback, via interviews. The pre-tests were very useful, as they resulted in a number of enhancements being made to the structure of the survey and the wording of specific questions. Having refined the questionnaire, a pilot study exercise was also undertaken, which provided valuable insights into the likely response rate and analytical implications for the full survey.

It was recognised that only those individuals who had a high degree of managerial responsibility for information systems and technology would be able to comment knowledgeably about the uptake and scope of information security policies. Senior IT managers were, therefore, chosen as the '*key informant'*, as they would be able to provide the requisite perspective. A list of the addresses of IT Directors, from large UK-based organizations, was purchased from a commercial research organization. The decision to target only large firms [firms employing more than 250 people] was based on the premise that small firms have few, if any, dedicated IT staff [Prembukar & King, 1992].

A total of 208 valid responses were received from the 2838 questionnaires mailed out, representing a response rate of 7.3%.

3.2 Sample Characteristics

The sample could be characterised in terms of both the size of the responding organizations and the sectors in which they are primarily operating. Of the valid respondents, 45% were employed in medium-sized organizations having less than 1000 employees, 32% were based in organizations with between 1000 and 5000 employees and the remaining 23% in larger organizations with over 5000 employees. Whilst the responses were also found to have come from a wide variety of industrial sectors, four were particularly well represented; manufacturing [23% of sample]; public services [19%], health [7%], and wholesale / retail [6%]. Respondents were also asked to indicate the geographical spread of their organisation as it was envisaged that this might have an impact on their need for a formal information security policy. The majority of responding organisations [50%] operated from multiple locations within the UK, whilst a further 32% of organisations operated from multiple sites, both within the UK and abroad, and the final 17% of the sample were located at a single site within the UK.

4. Findings

To make the following presentation of the research findings more meaningful they are related to the four specific research objectives, proposed at the end of section two of this paper.

4.1 The prevalence and updating of information security policies

In response to the question 'does your '*organisation have a documented information security policy*', 76% of respondents answered '*yes*', whilst the remaining 24% of the sample answered '*no*'. To determine whether the existence of an information security policy was in anyway related to the type of organisation responding, a series of chi-squared analyses were conducted. The results of these provided interesting evidence that the existence of an information security policy is not statistically associated with the sector in which the organisation operates [$\chi^2 = 4.06$; df = 3; p = 0.254], the size of the organisation [$\chi^2 = 3.62$; df = 3; p = 0.305] nor the geographical spread of the organisation [$\chi^2 = 0.22$; df = 11; p = 0.215]. These findings are in some ways counterintuitive, in that it might be anticipated that security threats, and therefore the need for security policies, might be greater in larger organisations and those operating across geographically disparate sites.

For those organisations that had a documented information security policy, the average length of time for which the policy had been actively used was 4.13 years [$\sigma = 4.11$]. Moreover, in terms of the

frequency with which policies are updated [see table 1], the majority of respondents [46%] updated their policies on an annual basis, whilst a further 38% updated their policies every two years or less, and the remaining 16% of the sample updated their policies every 6 months or more.

Table 1: Frequency with which policy is updated

Frequency of update	Number of responses	Percentage of sample
Less than every 2 years	33	21%
Every 2 years	26	17%
Every year	71	46%
Every 6 months	16	10%
More than every 6 months	8	5%

4.2 Methods for the dissemination of information security policies

Respondents, from organisations that had an information security policy, were asked to indicate the methods by which the policy was disseminated. Of the 158 organisations that had a documented information security policy, 43% of them disseminated it through their '*staff handbooks*', whilst 60% made the policy available via their '*company Intranet*', and 42% adopted '*other methods*'. As respondents were able to select more than one method, it is also informative to review the combinations of methods adopted. It can be seen from the findings presented in table 2 that whilst 60% of organisations used a single method for dissemination, 29% used two methods and 9% adopted all three approaches. In 3 instances, organisations had gone to the expense and effort of developing a policy, but there was no indication that the policy was being disseminated to employees.

Table 2: Methods of Dissemination

Method of dissemination	No. of responses	% of sample
Company Intranet + hand-book + other	14	9%
Company Intranet + hand-book	24	15%
Company Intranet + other	18	11%
Hand-book + other	5	3%
Company Intranet only	39	25%
Hand-book only	25	16%
Other only	30	19%
Strategy not disseminated to all employees	3	2%
Total	158	100%

An analysis of the 'other methods' adopted [see table 3] also provides some interesting insights. It is possible to divide the other methods into three broad categories:

1. **Policy dissemination:** Many of the '*other methods*' specified by respondents related to approaches that were designed to ensure that all employees had a personal copy of the full policy document. Methods for disseminating this personal copy included: electronic networks, email, hardcopies etc.
2. **Employee awareness:** Many organisations were adopting approaches to remind / inform employees of the policies existence or their specific responsibilities. Such methods included message delivered via: memos, leaflets, emails, notice-boards, logons, payslips etc.
3. **Employee education:** A final group of approaches were designed to provide education to all employees to ensure that can fulfill their responsibilities with respect to the requirements of the information security policy. Such education was delivered through formal, and often mandatory, training programs, seminars and induction courses.

Table 3: Other Methods

Dissemination Method	**Number of responses**
Hardcopy sent to each individual (for signature)	11
Information to all new employees / induction	9
Electronic networks other than '*company intranet'*	8
Training / seminars / presentations / briefings	7
Letters / leaflets / memos / circulars to employees	7
Copy emailed to employees	6
Leaflet in wage packet / pay-slip	4
Email reminders	4
Contract of employment	3
Operations manual	3
Part of logon procedure	2
Notice-boards	1
Hardcopy on request	1
Departmental representatives	1
On the desktop	1

4.3 The coverage of the information security policy

A key objective of this research study was to investigate the range of security issues covered by the information security policy, and the media by which the policy requirements were made available. An inspection of findings, presented in table 4, indicates that all the issues, other than '*encryption*' are explicitly covered, through the policy, a stand-alone procedure or both, by the vast majority of responding organisations. This is perhaps not such a surprising result, as encryption is a fairly technical issue, and therefore of limited interest to the majority of employees. An inspection of the findings also indicates that for the majority of issues, most organisations will address them either solely through the information security policy or will publish both a policy document and a supplementary procedure or standard. This is particularly the case for issues, such as *'internet access*', '*system access control*' and '*violations and breaches*', that should be of interest to all employees who are regular users of information systems. In cases where the issue is of more interest to IT professionals than the wider user community, such as 'software development' or 'contingency planning', there is an increased likelihood that the issue will be addressed solely through the publication of a stand-alone procedure or standard. A final point to note, from the findings presented in table 4, is that a small, but potentially significant, proportion of responding organisations are failing to explicitly address issues, such as '*personal usage of information systems*' and '*disclosure of information*', that should be of interest to the majority of system users.

Table 4: The Coverage of the Information Security Policy

IT security issue	Policy Document ONLY	Stand-alone procedure or standard ONLY	Policy document AND Supplementary procedure or standard	Issue NOT covered by policy
Disclosure of information	38%	9%	44%	9%
System Access control	33%	8%	58%	2%
Internet access	30%	9%	60%	1%
Viruses, worms & trojans	34%	9%	53%	4%
Software development	25%	20%	28%	27%
Contingency planning	17%	25%	39%	18%
Encryption	25%	10%	10%	55%
Mobile computing	32%	10%	29%	30%
Personal usage of IS	45%	6%	42%	8%
Physical security	37%	6%	46%	11%
Violations and breaches	36%	6%	49%	8%

4.4 Factors affecting the success of the information security policy

The British Standard for 'Information Security Management' [BS 7799] strongly advocates the formulation of an '*information security policy*' with the specific objective of providing '*management direction and support for information security*'. Moreover it identifies ten distinct factors that are '*critical to the successful implementation of information security within an organisation'*. For each of these factors the respondent was asked to indicate, using a five point '*Likert*' scale, their perceived importance and the extent to which their organisation was successful in adopting each factor. An average value for '*perceived importance'* and *'success of adoption*' was calculated for each of these 8 factors. The results of this analysis are presented in table 5, in descending order of the mean value for '*perceived importance'*.

The results of this analysis indicate that on average *'visible commitment from management'*, *'a good understanding of security risks', 'distribution of guidance on IT security policy' and 'a good understanding of security requirements'* are perceived to be the most important factors [see table 5, column 2]. It can be seen that these same four factors also attract the highest average scores for *'success of adoption'*. Indeed, there is a statistically significant correlation between the '*perceived importance'* and *'success of adoption'* score for each of the eight factors [5 at the .01 level and 3 at the 0.05 level]. These results are generally encouraging as they suggest that organisations are perhaps putting most effort into the successful adoption of those factors that are perceived to be of most importance. However, the results of a paired sample 't' test [table 5, columns 4 & 5] indicate that whilst the '*perceived importance'* and *'success of adoption'* scores might be correlated there is a significant difference between them. More specifically, for all the factors the '*perceived importance'* score is significantly higher than the *'success of adoption'* score. This results suggests that the responding organisations are failing to achieve a degree of success in the adoption of each factor that is commensurate with its perceived importance.

Table 5: Factors affecting the success of the information security policy

Factors	**Importance** of each factor to **the successful implementation of IT security** policy	**Success of** organizations in **adopting each factor**	**Paired sample 't' test**	
			T value	**Sig.**
Visible commitment from management	4.60	2.99	17.8	.000
A good understanding of security risks	4.48	3.24	14.9	.000
Distribution of guidance on IT security policy to all employees	4.36	3.30	12.1	.000
A good understanding of security requirements	4.35	3.23	13.1	.000
Effective marketing of security to all employees	4.26	2.65	17.8	.000
Providing appropriate employee training and education	4.26	2.59	18.8	.000
Ensuring security policy reflects business objectives	4.11	3.18	11.7	.000
An approach to implementing security that is consistent with the organizational culture	3.93	3.17	9.2	.000
Comprehensive measurement system for evaluating performance in security management	3.56	2.36	14.3	.000
Provision of feedback system for suggesting policy improvements	3.52	2.39	12.7	.000

5 Discussion: The incidence and application of information security policies

This section discusses the key results and contextualizes them in the literature. The implications of this study for IT managers and researchers are then reviewed before the study's potential limitations are highlighted.

With regard to the uptake of information security policies, the findings of the present study indicate a larger proportion of organizations implementing policies than was found in the other studies discussed in the literature review presented in section 2. More specifically, the present study found that 76% of the sample had an information security policy in place, whereas only 65% of the organizations in the Andersen (2001) survey had one, and only 27% of the organizations (59% of the large organizations) reported having one in the DTI (2002) survey. This finding may very well indicate that the uptake of information security policies is on the increase among large organizations. However, the possibility of respondent bias (Churchill, 1997; p662) must also be acknowledged: our study focused more explicitly on security policy than the other studies, and hence more those organisations having a policy might have been more inclined to respond.

Dissemination of policies: seems to represent an interesting area for investigation. Findings of previous studies (DTI, 2002; *DT, 2000)* suggest that, despite its recognised importance (Siponen, 2000), in practice, organisations do not appear to be too concerned about dissemination. Whilst the present study provides important new evidence about the variety of mechanisms used to disseminate policy, it also confirms that the majority of organisations are not perhaps giving dissemination the priority it deserves; most organisation still rely on a single mode of dissemination. The research presented in this paper also provides important new evidence concerning the scope and content of information security policies. Whilst it has been found that: policies seem to cover a broad range of issues, a number of key user issues, such as '*personal usage*' and '*disclosure of information*', are not commonly covered. This may be because many organizations have implemented policies because it is deemed to '*good practice*' (DTI, 2002), rather than as a working tool for informing users about their responsibilities. Finally, the paper also provides some important new insights into the factors that facilitate the successful application of information security policies. In particular, the gap between the perceived importance of each success factor and the degree to which responding organisations are successful in their adoption, is very worrying. Clearly, organisations must make the adoption of these success factors a far higher priority if they are to successfully formulate, disseminate and operate successful information security policies.

These findings have a number of important implications for IT managers, especially those directly responsible for information and IT security. For example, they explicitly highlight the issues that should be covered in the policy, the ways by which it can be communicated and the factors that facilitate its successful adoption. This study should also be of interest to the research community, as a new data collection instrument, based upon the literature, has been developed and rigorously tested, which can be adapted for use in follow-up studies. It also provides a broad picture of the current incidence and application of information security policies in the UK and can therefore be used to help contextualize the findings of the many studies of information and computer security that are likely to be undertaken in the near future.

Social inquiry, within the organizational context, is always an ambitious undertaking, and therefore contains a number of inherent limitations. In particular, the adoption of the survey format results restricts the range of issues and constructs that can be explored, and there is also the potential for response bias, associated with targeting only managerial stakeholders. It must also be recognised that the results of this study are based upon statistical analysis and they are therefore identifying general trends, and measuring '*association*' rather than '*causality*'. These limitations, therefore, highlight the need for further research to be conducted that adopts different methods, and targets different populations and respondents. In particular, there is a need for more qualitative studies that will allow

the statistical patterns and relationships identified here to be more fully explored and hopefully explained.

6 Concluding Remarks

There is a high degree of consensus that effective information security management is predicated upon the formulation and utilisation of an information security policy. However, our knowledge of the uptake, scope and dissemination of such policies is fairly limited, and so an exploratory, empirical study of this domain was initiated. The results of a statistical analysis suggest information security policies are now widely applied, but there is little commonality in terms of the scope of such policies and the methods by which they are disseminated. Whilst this research presents many important new insights, into the uptake and application of information policies, there is still the need for many more follow-up studies. In particular, it is important that future studies focus in detail on the methods by which policies are formulated, applied and evaluated, and studies that seek to explore the relationship between policy application and the effective management of information security.

References

Andersen, I. T.-(2001) Sicherheit in Europa, Studie 2001, Status Quo, Trends, Perspektiven.

Angell, I. O. (1996)Economic Crime: beyond good and evil. *Journal of Financial Regulation & Compliance*, **4** (1).

Barnard, L. and von Solms, R. (1998) "The evaluation and certification of information security against BS 7799", *Information Management and Computer Security*, **6** (2), pp. 72-77.

B.S.I. (1999) *Information security management -BS 7799-1:1999*, British Standards Institute, London, UK.

Churchill, Gilbert A. Jr (1997). *Marketing Research, Methodological Foundations.* The Dryden Press.

Dinnie, G. (1999) The Second annual Global Information Security Survey. *Information Management and Computer Security*, **7** (3), pp. 112-120.

Dhillon, G. & Backhouse, J. (2001) "Current directions in IS security research: towards socio-organisational perspectives", *Information Systems Journal*, **11**, pp 127-153.

D.T.I. (2002), *Information Security Breaches Survey 2002*, Technical Report, April Department of Trade and Industry, London.

D.T.I. (2000), *Information Security Breaches Survey 2002*, Technical Report, April Department of Trade and Industry, London.

Ernst and Young, (2001), *Information Security Survey,* Ernst & Young, London.

Gaskell, G. (2000), "Simplifying the onerous task of writing security policies", *Proceedings of the First Australian Information Security Management Workshop*, School of Computing and Mathematics, Deakin University, Geelong.

Higgins, H. N. (1999), "Corporate system security: towards an integrated management approach", *Information Management and computer Security*, **7** (5), pp 217-222.

Hone, K. 7 Eloff, J. H. P. (2002) "Information security policy- what do international security standards say?", *Computer & Security*, **21** (5), pp 402-409.

Gerber, M., von Solms, R. and Overbeek, P., (2001), "Formalizing information security requirements". *Information Management and Computer Security*, **9** (1), pp. 32-37.

Premkumar, G. and King, W. R. (1992), "An empirical assessment of information systems planning and the role of information systems in organisations. *Journal of Management Information Systems*, **19** (2), pp 99-125.

Moule, B. and Giavara, L. "Policies, procedures and standards: an approach for implementation" . *Information Management and Computer Security*, **3** (3), pp.7-16.

Siponen, M. T. (2000) "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, **8** (1), pp.31-41.

von Solms, R. (1998) "Information security management (1): why information security is so important" *Information Management and Computer Security*, **6** (5), pp. 224-225.