IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4673

Information Security Policies in Large Organisations: Developing a Conceptual Framework to Explore their Impact

Neil F. Doherty and Heather Fulford
The Business School, Loughborough University, Loughborough, UK,
T: + 44 (0) 1509 223128, F: + 44 (0) 1509 223960, n.f.doherty@lboro.ac.uk

ABSTRACT

Whilst the importance of the information security policy (ISP) is widely acknowledged in the academic literature, there has, to date, been little empirical analysis of its impact. To help fill this gap a study was initiated that sought to explore the relationship between the uptake, scope and dissemination of information security policies and the accompanying levels of security breaches. To this end a questionnaire was designed, validated and then targeted at IT managers within large organisations in the United Kingdom. The aim of this paper is to provide a progress report on this study by describing the objectives of the research and the design of the conceptual framework.

INTRODUCTION

It has been claimed that '*information is the lifeblood of the organisation*' [CBI, 1992], as it is the critical element in strategic planning and decision-making, as well as day to day operational control. Consequently, organisations must make every effort to ensure that their information resources retain their accuracy, integrity and availability. However, the increasing integration of information systems both within and between organisations, when coupled with the growing value of corporate information resources, have made information security management a complex and challenging undertaking [Gerber et al., 2001]. Indeed, the high incidence of security breaches suggests that many organisations are failing to manage their information resources effectively [Angell, 1996; Gaston, 1996]. One increasingly important mechanism for protecting corporate information, and in so doing reducing the occurrence of security breaches, is through the formulation and application of an information security policy (ISP) [Hone & Eloff, 2002]. Gaston [1996; p. 175] defines an ISP as:

"*broad guiding statements of goals to be achieved; significantly, they define and assign the responsibilities that various departments and individuals have in achieving policy goals.*"

Whilst the high incidence of security breaches and the importance of information security policies are both areas that have attracted significant attention in the literature, there is little evidence that these topics have been explicitly combined. To help fill this gap a research study was initiated that sought to empirically explore the relationship between the uptake and application of information security policies and the incidence of security breaches. The aim of this paper is to provide a progress report on this study by describing the objectives of the research and the design of the conceptual model. The remainder of this paper is organised into three sections: a discussion of the research objectives and method, a description of the conceptual framework, and the conclusions and recommendations for future research.

RESEARCH OBJECTIVE AND METHODS

The aim of this section is to describe the study's broad objective before reviewing the methods by which it is to be explored. Given the lack of empirical research in the area it was felt that an exploratory piece of work that embraced a wide range of issues would be most appropriate. To this end the aim of the study was to explore how a variety of issues relating to the uptake and application of information security policies impacted upon the incidence of security breaches, within large organisations. This broad objective was ultimately broken down into a number of distinct research hypotheses, which are fully described in Section 3 and graphically presented in Figure 1.

To effectively explore the research hypotheses, it was necessary to develop a series of measures that, when incorporated into a questionnaire, would adequately describe an organisation's information security activity. To this end, the questionnaire was designed through an iterative process of review and refinement. It sought to capture a significant amount of information with regard to the respondent's organisation, in addition to the information required to explicitly address the six research hypotheses. The initial draft of the questionnaire was developed from a thorough review of the literature. The first phase of the '*review and refinement*' process was accomplished through a series of pre-tests with four academics, each of whom had an interest in information security. The questionnaire was then modified accordingly before a further series of pre-tests was conducted with five IT practitioners. To complete the validation process a pilot study of 10% of the sampling frame was conducted. Together, these validation exercises resulted in a number of significant changes that greatly enhanced both the content and wording of the questionnaire, before the full survey was ultimately distributed.

In terms of the sampling frame, we wanted to target senior IT managers as these were most likely to be responsible for the formulation and application of an ISP. Moreover, only large organisations [firms employing more than 250 people] were targeted, as previous research has found that small firms tend to have few, if any, dedicated IT staff [Prembukar & King, 1992]. To this end, a list of the addresses of IT directors, from large UK-based organizations, was purchased from a commercial market research organization. Each of the sample of 2838 IT directors was mailed a questionnaire, with an accompanying letter, that explained the study, and a pre-paid envelope.

THE CONCEPTUAL FRAMEWORK

The aims of this section are to describe and justify the conceptual framework, discuss the proposed analysis strategy and then review the anticipated results and their importance.

It was anticipated that a number of distinct aspects of the ISP might influence the incidence of security breaches. Each of these was explicitly covered by the questionnaire and is described below:

- **The existence of a policy:** The questionnaire sought to determine whether the responding organisation had formulated a documented ISP. Consequently, this question was operationalised as a simple dichotomous variable. If the organisation did have a policy the following questions were also then asked.
- **The age of the policy:** If an ISP was in use, respondents were asked to specify the number of years that it had actively been in operation.
- **The updating of the policy:** Respondents were also asked to identify the frequency with which the policy was typically updated, using a five

point, ordinal scale [< every two years; every two years; every year; every six months; > every six months].

- **The dissemination of the policy:** Policies are of little use unless all employees are made aware of their rights and responsibilities, in relation to it. In addition to explicitly asking whether policies were disseminated via a *company intranet* or the *staff handbook*, respondents were asked to stipulate any *other* dissemination mechanisms.
- **The scope of the policy:** Policies may vary greatly in their scope. Consequently the questionnaire included a list of eleven distinct issues, such as disclosure of information, Internet access and personal usage of systems, that might be covered by the policy. For each issue, the respondent was asked whether it was covered by the policy document, a stand-alone procedure, by both policy and procedure, or neither.
- **The adoption of success factors:** It has been suggested that organisations will only be successful in the adoption of their ISP if they apply a range of success factors [BSI, 1999]. The British Standard identifies eight distinct factors, such as *ensuring the policy reflects business objectives* and *conducting a risk assessment.* For each factor, the respondent was asked to assess their importance, using a five point Likert scale, and identify how successful his / her organisation had been in its adoption, also using a five point Likert scale.

The '*incidence of security breaches*' was operationalised as a multi-dimension construct. A number of potential risks to the security and integrity of computer-based information systems were identified from the literature [e.g. BSI, 1999], and included in the survey. A total of eight distinct threats, including computer viruses, hacking, human error, fraud and natural disasters, were identified and ultimately included in the research instrument. Each of these threats were operationalised in the following two ways:

1) **Occurrence of threat:** Respondents were asked to estimate the approximate number of occurrences of a specified threat that they had experienced in the previous two years, using a four item ordinal scale [**0**; **1-5**; **6-10**; **>10**].
2) **Severity of threat:** Respondents were also asked to estimate the severity of the worst incident, over the same two year period, using a five point Likert scale [**1** = fairly insignificant; **5** = highly significant].

It is anticipated that there may be important relationships between each of the six independent variables, relating to the uptake and application of the ISP, and the dependent variables: '*incidence of security breaches.*' Moreover, it is envisaged that the data will be analysed using either ANOVA or Pearson correlation, depending upon whether the independent variables have been operationalised as ordinal or metric scales. The anticipated results of the analysis can best be described as a series of hypotheses [see also Figure 1]:

H1: Those organizations that *have a documented ISP* are likely to have fewer security breaches, in terms of both frequency and severity, than those organisations that *don't.*

H2: Those organizations that have had an ISP in place for *many years* are likely to have fewer security breaches, in terms of both frequency and severity, than those organisations that *haven't.*

H3: Those organizations that update their ISP *frequently* are likely to have fewer security breaches, in terms of both frequency and severity, than those organisations that *don't.*

H4: Those organizations that *actively disseminate* their policy are likely to have fewer security breaches, in terms of both frequency and severity, than those organisations that *don't.*

H5: Those organizations that have a policy with a *broad scope* are likely to have fewer security breaches, in terms of both frequency and severity, than those organisations that *don't.*

H6: Those organizations that have been adopted a wide variety of *success factors* are likely to have fewer security breaches, in terms of both frequency and severity, than those organisations that *haven't.*

Whilst the hypotheses have been formulated to represent the outcomes that the researchers believed to be the most likely, it was recognised that in some cases alternative, yet equally plausible results, might be produced. For example, it might be that the existence of an ISP is associated with a high incidence of security breaches, in circumstances in which the policy has been implemented in direct response to a poor security record.

CONCLUDING REMARKS

At this point in time, the full survey has now been distributed and a follow-up mailing is underway, in an attempt to generate more responses. It is envisaged that the statistical analysis of the research hypotheses will begin in the near future and should generate some very interesting results. In terms of future work, a series of follow-up interviews is planned to provide deeper insights into the nature of any significant relationships that the quantitative analysis might uncover. As the project unfolds, it is anticipated that the findings will help organisations to better understand the value of security policies and to pinpoint the policy areas for prioritisation.

REFERENCES

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

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

C.B.I. (1992) *IT The Catalyst for Change*, Confederation of British Industry, London.

Gaston, S. J. (1996) *Information Security: Strategies for Successful Management*, CICA, Toronto.

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

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

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.

Figure 1.

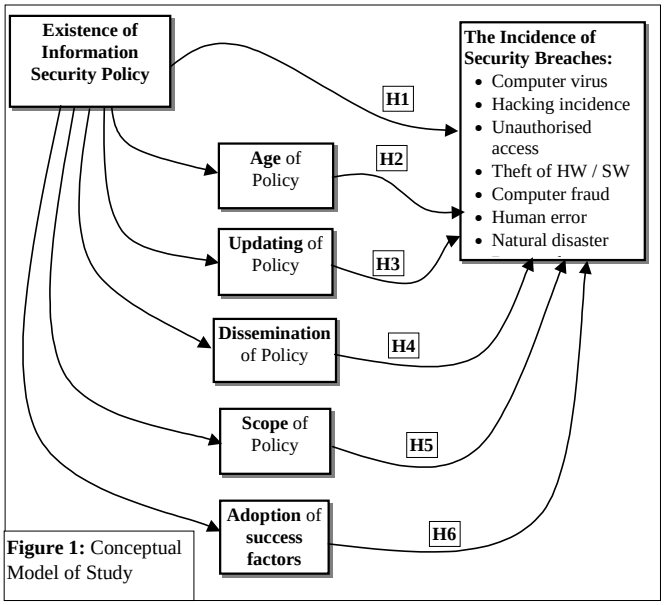

Figure 1: Conceptual Model of Study