Computers & Security

The information security digital divide between information security managers and users

Eirik Albrechtsen[a,b,*], Jan Hovden[a]

[a]Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology, N-7491 Trondheim, Norway
[b]Department of Safety Research, SINTEF Technology and Society, N-7465 Trondheim, Norway

ARTICLE INFO

ABSTRACT

Empirical findings from surveys and in-depth interviews with information security managers and users indicate that a digital divide exists between these groups in terms of their views on and experience of information security practices. Information security professionals mainly regard users as an information security threat, whereas users believe themselves that they are an untapped resource for security work. The limited interaction between users and information security managers results in a lack of understanding for the other's point of view. These divergent views on and interpretations of information security mean that managers tend to base their practical method on unrealistic assumptions, resulting in management approaches that are poorly aligned with the dynamics of the users' working day.

1. Introduction

Traditionally, "digital divide" has been understood as a socio-economic perspective, dealing with access to information communication technology, particularly the Internet, and the ability to use this technology to participate fully in business, political and social life (Partridge, 2005). However, several authors argue that the digital divide should also be understood in psychological, cultural and sociological terms. For example, Warschauer (2002) has stated that the digital divide is not only about physical access to computers and connectivity, but also about people's ability to make full use of the systems. Jung et al. (2001), Harittai (2002), and DiMaggio et al. (2004) argue that the question of unequal access must be expanded to address people's skills, scope of use, autonomy,

and ability to maximise the utility of the technology to achieve their goals. Based on these interpretations, a social digital divide (Partridge, 2005) can be understood as a product of differences in self-efficacy, individual skills and perceptions, cultural aspects, and interpersonal relationships, all of which contribute to a gap in the use of information systems.

From a socio-technical perspective, a digital divide in information security can be viewed as consisting of the existing differences with regard to information security skills and knowledge, perceptions of information security, social norms, and interpersonal relationships, any or all of which can result in differences in information security performance between individuals. A digital divide in information security within organisations is thus not only a question of access to information systems that have implemented adequate

* Corresponding author. Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology, SINTEF Teknologi og Samfunn, N-7491 Trondheim, Norway.
E-mail address: eirik.albrechtsen@iot.ntnu.no (E. Albrechtsen).

information security technology; it is also a question of considerable differences in skills, knowledge, responsibilities, perceptions and interpersonal relationships between the various members of the organisation. From this perspective, several digital divides may exist within information security, related to, for example, age, gender, IT experience, education and occupation. In this article we will discuss the digital divide in information security in terms of any existing differences in information security views and expectations between information security professionals and users.

An organisation consists of its members and their interactions. Each member has his own role to play, and his own sphere of responsibility, which contribute towards realising the organisation's goals. Preserving information security is among the goals of any organisation, and every member has a responsibility for ensuring such security in practice. Whereas information security managers have a particular responsibility because of their expert knowledge, for other users at all levels of the organisation the responsibility for acting in a manner that is safe and secure for the organisation comes on top of the other demands they are faced with in their everyday work. An information security digital divide between users and information security managers with regard to skills, knowledge and responsibilities is therefore to be expected.

This article aims at discussing an information security digital divide between information security managers and users by exploring *similarities and differences between their views on and experience of information security practices in organisations*. This purpose is approached by looking at how managers and users view their own role compared to how they experience the role of the other, and at how they experience administrative security measures. Furthermore, given that there are differences, how are these differences reflected in the actors' judgement of risk? A two-fold approach is adopted. First, empirical findings from an interview study of information security managers are compared with the results of a similar interview study concerning users' views on information security performed by the authors (Albrechtsen, 2007) and other relevant research results on the human aspects of information security. Second, quantitative data from two different surveys of, respectively, users' and information security managers' judgement of IT-related risks are compared.

Although some studies have addressed information security user performance and information security management (for an overview, see Stanton et al., 2005), few attempts have been made at research which seeks to combine and compare the role and views of users and information security managers. A study in the health domain by Adams and Blandford (2005) showed contrasting perspectives among security professionals and users on the role of users and on security practices. Kuttschreuter and Gutteling (2004) showed that experts and lay people had different perceptions of the risk associated with the Y2K problem.

Our study mainly considers the administrative information security system and the role of users and managers. Technological issues are dealt with only in a brief manner. Focusing on non-technological issues of information security makes comparisons easier as well as richer, as it is likely that many users have no specific insight into the technological aspects of information security.

The next section presents the data sources and the analytical approach used to study possible information security divides. The results, as well as a discussion of each of the aims of the article described above, are presented in the subsequent sections. On the basis of qualitative data, Sections 3–5 present and compare the ways in which security managers and users experience the role of security managers, the user aspect of information security, and user-directed measures. Subsequently, survey data are used to show how users and security managers assess IT-related risks, and some interpretations of these results are discussed. In Section 7, these results and discussions are summarised, and the indication is indeed that a digital divide in information security exists between users and managers. The article concludes with a statement that the social digital divide between users and managers creates unrealistic assumptions about sharp-end activities among information security managers, who base their practical management approach upon these assumptions.

2.   Data and analysis

2.1.   Analytical approach

Data from four independent empirical sources form the basis for this article:

- *An interview study of managers*: a qualitative interview study of information security managers in large Norwegian organisations.
- *An interview study of users*: a qualitative interview study of users in a Norwegian bank and a Norwegian IT-company.
- *A survey of managers*: a survey among information security managers in several Norwegian organisations.
- *A survey of users*: a survey among users working in a Norwegian public agency

These sets of data were collected for purposes that differed slightly from the objective of this study. In this respect, the present approach is a secondary analysis of available data. With exception of the manager interview study, the studies are all published elsewhere: Albrechtsen (2007, 2018) and Hagen et al. (2008). However, the research designs of the four studies were all created in a way that made the present comparative study possible, since the two interview studies covered the same topics, and the two surveys included a set of questions relevant to the present comparative study.

Fig. 1 shows the analytical design of the article. The views held by users and information security managers with regard to different information security activities and characteristics are subjected to a comparative study in order to explore whether indications may be found of a digital divide in relation to information security in organisations. The figure also shows how the different sets of data described in the bulleted list above are used in comparative analyses of different information security topics.