Chapter 99
Information Security Practices in Small-to-Medium Sized Businesses: A Hotspot Analysis

Kent Marett
Mississippi State University, USA

Tim Barnett
Mississippi State University, USA

ABSTRACT

Small to medium-sized enterprises (SMEs) in North America do not always adequately address security. Based on responses from 232 SME owners and managers, the authors found that the adoption of security recommendations made by experts appear to be significantly influenced by the decisions of other local SMEs. A hot-spot analysis of information security practices suggested that local trends lead to prioritizing certain security practices and not adopting others. Follow-up interviews with business owners and Chamber of Commerce directors provided insights on how security hotspots developed or not. The study identified both hot spot and cold spot communities, and sought to assess how local business networking conduits like chambers of commerce help promote best security practices

1. INTRODUCTION

Despite recent high-profile information security breaches in large firms, small-to-medium sized business enterprises (SMEs) may be more vulnerable to information security breaches than large multinational organizations and Fortune 500 companies, for a number of reasons. For example, the majority of companies with 500 or fewer employees do not have a designated security professional and they are often not required to follow the same legal security standards as their larger counterparts (Verma, 2015). SMEs also lack larger firms' capacity to absorb losses due to such security breaches. A successful attack can

DOI: 10.4018/978-1-7998-8954-0.ch099

often lead to insolvency for an SME (Reckard & Hsu, 2014). Further, many of the recommendations put forth by security experts are geared toward larger firms with the requisite resources and experience to adopt them (Osborn & Simpson, 2017).

Because SMEs compose a significant part of the U. S. and world economy and due to their inherent susceptibility to information security breaches, it seems particularly important that the IS research community develop greater depth of knowledge related to (1) why such firms do or don't adopt recommended security practices and (2) what specific security practices they employ. For decades, a number of researchers (Dang-Pham, Pittayachawan, & Bruno, 2017; Dang & Nkhoma, 2017; Dhillon & Torkzadeh, 2006; Knapp, Marshall, Rainer, & Ford, 2006; Straub & Welke, 1998) have made considerable progress into learning how organizations with a relative abundance of financial resources, personnel, time, and access to expertise are able to methodically develop information security programs. Although our knowledge about the security practices of Fortune 500 businesses has accumulated at a desirable pace, the same cannot be said for our understanding of the security practices of SMEs. With the resource limitations that they have, how do SMEs learn about best practices in information security? Why do some SMEs (and not others) adopt recommended security practices? Where do they turn for help or advice?

In their conceptual exposition on institutional- and resource-based theories related to information privacy, Greenaway and Chan (2005) suggest that institutional theory (DiMaggio & Powell, 1983) offers one compelling theoretical framework that "…should be applied to privacy research within the information systems area" (p. 171). Institutional theory seeks to understand and explain homogeneity or isomorphism across organizations, which the theory posits results from their attempts "…to deal rationally with uncertainty and constraint" (DiMaggio & Powell, 1983, p. 147). According to DiMaggio and Powell, an isomorphism is "…a constraining process that forces one unit in a population to resemble other units that face the same set of environmental conditions" (p. 149) that can result from decision-makers' attempts to survive and thrive by adopting behaviors practiced by successful firms, but isomorphism can also result from institutional pressures exerted by social and economic forces, including other organizations that comprise a focal group or network for a given firm. These "other" organizations could be, for example, partners, suppliers, competitors within a given industry, customers, and/or those within a common geographic area (Besharov & Smith, 2014; Davis & Greve, 1997; Davis & Marquis, 2005; Pahnke, Katila, & Eisenhardt, 2015).

As applied to information privacy, isomorphism implies that firms will tend to adopt practices and behaviors that comply with and/or imitate those of socioeconomic networks in which they are situated (Greenaway & Chan, 2005). Prior research has drawn on the institutional approach to explain instances of firms seeking guidance from external sources on information security, including advice on complying with auditing regulations (Hu, Hart, & Cooke, 2007) and help with implementing security innovations (Hsu, Lee, & Straub, 2012). However, though isomorphism has effectively explained the security decision-making approach used by large firms, there seems to be a gap in the literature where SMEs are concerned. In this study, we apply ideas and concepts from the institutional framework to examine the potential for SMEs within the same geographic area to adopt similar information security practices. We posit that, for the smaller firm, geographically proximate organizations comprise an important socioeconomic network from which the firm will acquire external information on information security available to SMEs, and that the firms within these geographically proximate networks will exhibit similarity in terms of their information security behaviors. We also investigate the underlying reasons why businesses in some localities may be better at exchanging security advice than in others.