Teleworker's Security Risks Minimized with Informal Online Information Technology Communities of Practice

Loreen Marie Powell
Bloomsburg University of Pennsylvania, USA

INTRODUCTION

The advancements of technology have altered the way many small businesses operate in the United States of America (USA) (Butcher-Powell, 2006). Small businesses have been forced to embrace technology or lose valuable employees and business. As such, many small businesses have merged to wireless networks and adopted various forms of telework. Today, it is estimated that more than 60% of the workforce are teleworkers (Butcher-Powell, 2006; DecisionOne, 2002). While moving to a remote workforce is good for small businesses, it also places a substantial amount of security risks upon the small business. Butcher-Powell (2006) documented some of the security risks associated with corporations employing a remote workforce, indicating that teleworker's lack of information systems and security training can compromise the corporation's network.

The study investigates one particular method for aiding teleworker's: informal information technology communities of practice in cyberspace. One hundred and forty four teleworker's were surveyed on what sort of IT-related activities they devote time to, how much problem-solving they attempt via technology discussion groups with respect to those activities, and their perceived community and organizational benefits to participating in such discussion groups. The study found significant differences in perceived value of technology discussion groups among teleworkers.

BACKGROUND

Telework

Telework is often defined as an agreed upon working arrangement whereby the employee is permitted to officially perform their job tasks in another location other than the typical place of business (United States Department of Defense, n.d.). Most telecommunication elements include laptop computers, the Internet, and various wireless routers, a firewall, and a virtual private network (VPN). Each teleworker is typically provided with a laptop that contains locally installed corporate software. Each laptop typically uses a client and Microsoft's Point-to-Point Transfer Protocol (PPTP) to enable remote access to the small business's network. The client is configured to allow TCP/IP connections on the small business's network as needed (Butcher-Powell, 2006). The client contains a designated Internet protocol (IP) address, and a valid log-on user name and password needed to establish a relationship with the small business's network. The relationship between the client and the small business's network is established by utilizing client software to connect to the small business's firewall via tunneling. Once the client is authenticated, the teleworker gains access into the network.

Problems with Telework

While telework offers substantial benefits, including reduced overhead costs and expanded labor pools without geographic restrictions (Carlson, 2000; Hirsh, 2004; Mehlman, 2002; Motskula, 2001), it also offers substantial security risks to small businesses. One of the largest security risks associated with telework is the teleworkers lack of IT skills and training (Hirsch, 2002; Mehlman, 2002). Teleworkers lack of IT skills and knowledge are costing small businesses thousands of dollars and their business. Research has shown that teleworkers do not have an understanding of authentication, data tampering, encryption, firewalls, and scavenging. Therefore, many corporations have conducted IT training courses for teleworkers. However, the research has also shown that IT training for teleworkers is not enough. First, many small business cannot afford training. Second, teleworkers have been resistant to IT training (Butcher-Powell, 2006). Third, the train-

ing is not specific enough. As such, small businesses are seeking for an additional solution. One possible solution is to create informal online communities of practices (CoPs) for teleworkers (McDermott, 2000; Wenger, McDermott, & Snyder, 2002).

Communities of Practice

CoPs were first used by Wenger in 1991 and popularized more widely in two major works (Wenger et al., 2000, 2002). CoPs are the idea of sharing information for the purpose of learning from one another within a small group (Mitchell, 2002). Traditionally CoPs were created spontaneously in a workplace. However, today, there has been increasing interest in the creation of teleworking CoPs (Cameron & Powell, 2006; Snyder, 2000; Wenger et al., 2002).

RESEARCH

The goal of this research was to investigate how informal online IT CoPs could reduce network security risks associated with telework. A 32-question survey was developed and administered via the Internet. The survey collected background information (gender, professional responsibilities, education, career status, etc.), technology information (time spent on specific technology tasks, resources and practices at the organization, and problem-solving methods), and technology discussion group information (personal and organizational methods for discussing technology issues, membership in technology groups, perceived benefits of participation in technology groups, etc.).

ANALYSIS

A total of 144 teleworkers completed the survey. There were 113 female respondents and 31 male respondents. The age range of teleworkers was somewhat evenly distributed among 18–60 year-olds. Eight participants completing the survey were 61 or older. Nearly all participants (122) indicated that they had attended college. Only one had received an associate's degree, eight held a bachelor's degree, and four had gone on to a master's or PhD.

Teleworkers were asked to complete a five-point Likert-scale response (strongly agree to strongly disagree) to participation in technology discussion groups influencing IT organizational benefits (IT knowledge sharing, IT collaboration, IT consensus generating, and IT community reputation). A multiple analysis of variance (MANOVA) was used to analyze the responses via age, gender, education, and technology-specific education. There were significant differences found between the overall main effect of organizational benefits and age ($p=.02$), gender ($p=.04$), education ($p=.01$), and technology-specific education ($p=.00$). These results indicated that the teleworkers perceived that informal online IT CoPs as a valid resource to help secure their information technology. Interviews with the teleworkers further indicated that they would be more likely to log on, read security posted, search IT problems, and attend online chats sessions rather attend a traditional IT training session. These results are not surprising since several other research studies have documented that CoPs are being used in teleworking.

CONCLUSION

Many small businesses information networks features sensitive and confidential data relevant to internal and external transactions. Research has shown that telework connections put data at risk due to the potential of intrusion and eavesdropping from the teleworker's laptop (Dhillion & Backhouse, 2000). Every teleworker's laptop is susceptible to a variety of computer threats. Teleworkers need to be educated to help protect their laptop and network. One possible solution other then training is forming and having your teleworkers participate in informal online IT CoPs. This study investigated teleworker's perceptions regarding CoPs. Significant differences were found among IT organizational benefits and teleworkers. Since IT organizational benefits were found to be significant, this study assumed that if teleworkers are likely to use IT CoPs, then the education learned in the CoPs will help to further eliminate security risks associated with teleworking. However, further research needs to be conducted over an extended period of time is necessary to determine whether the informal online CoPs will in fact directly reduce the number of security risks.