An Empirical Investigation of an Individual’s Perceived Need for Privacy and Security

Taner Pirim, Mississippi Center for Supercomputing Research, USA
Tabitha James, Virginia Polytechnic Institute and State University, USA
Katherine Boswell, University of Louisiana at Monroe, USA
Brian Reithel, University of Mississippi, USA
Reza Barkhi, Virginia Polytechnic Institute and State University, USA

ABSTRACT

Security and privacy issues have risen in importance as the use of technology increases. Newly developed technological devices for asset security can only be successful if people are willing to use them. Gaining an understanding of individuals’ acceptance and possible use of new security technologies would be beneficial to entities that are developing, marketing, and implementing new security technologies. This study develops an instrument to determine an individual’s need for security and privacy and investigates the relationship between these two constructs. The results show that the instrument developed is reliable and that a significant relationship exists between the two constructs.

Keywords: instrument development; privacy; security

INTRODUCTION

Privacy refers to the ability of an individual to “control the terms under which personal information is acquired and used” (Henderson & Snyder, 1999; Westin, 1967). A certain expectation of an individual’s right to privacy has always been present; however, there is some disagreement as to what this expectation should be (Milberg, Smith, & Burke, 2000). Privacy concerns have garnered much attention in recent years with the rise in identity fraud and the new capabilities to collect and process information brought about by technology. In the last 5 years, there have been a reported 27.3 million cases of identity fraud accounting for nearly $48 billion in losses to financial institutions and $5 billion worth of out-of-pocket expenses to consumers, according to the Federal Trade Commission (FTC) (2003). The public concern over this threat is evident in the report by the FTC to the
Ways and Means Committee of the U.S. House of Representatives in March, 2006. This report stated that the commission is contacted between 15,000 and 20,000 times per week by individuals requesting information about identity theft avoidance practices. The Identity Theft Data Clearinghouse, which is the national repository for identity theft and consumer fraud, has received over 1.06 million complaints since its inception (FTC, 2006).

One major reason for the rise of identity fraud is that increases in Internet transactions make the authentication of persons more difficult than ever before, because there is no human contact and less opportunity for identification checks. Hence, methods for identification and verification in e-commerce environments are becoming increasingly necessary to avoid potential issues such as identity fraud. Online banking, electronic financial transactions, online data stores, and Internet commerce, for example, are becoming extremely popular and the technologies to prevent misuse of these systems continue to expand as their importance increases and the potential for financial loss grows.

With advances in technology, companies have ever-increasing abilities to collect and analyze data to make assumptions about consumer behaviors. Increasing concerns about the misuse of such data, or the use of this information in a way not intended by the individual, have pushed privacy issues to the forefront of social consciousness.

Government regulations to control the collection and use of information illustrate the growing importance of privacy to individuals. Opt-out policies for secondary use of information from credit card companies, for example, now give individuals in the United States more control over who has access to their personal information. The use of information to derive valuable insights about individuals has become an increasingly important issue due to increased capabilities in collecting, processing and joining information by corporations and government entities. This information once collected can provide companies and government agencies with data that can be used for financial gain (Mason, 1986). These increased capabilities to collect and process data create an ethical dilemma in terms of financial profitability vs. an individual’s right to privacy (Mason, 1986).

Security as defined by the dictionary refers to “freedom from danger” or “freedom from fear or anxiety” (www.m-w.com/cgi-bin/dictionary). The importance of security has been highlighted in recent years due to uncertainties in world events as well as the ever-growing threat of vulnerabilities in systems crucial to normal operation of many functions of society. Physical security has always been a concern that individuals have placed importance upon. Recent events and rises in crime have compounded this concern as individuals are now more aware of threats to their physical safety in public areas such as airports, planes, sporting events, and their places of work, in addition to their normal safety concerns for their belongings and physical well-being in their homes and vehicles. The U.S. Department of Justice reported that in the summary findings of the National Crime Victimization Survey for 2004, 77% of all crimes were property crimes (Bureau of Justice, 2003). According to the FBI’s Preliminary Annual Uniform Crime Report for 2005, property crimes reported in just the larger cities in the US amounted to over 3.8 million (FBI, 2005).

Computer security is now becoming as ubiquitous as physical security due to the rising use of networked computers for personal and corporate use. The protection of corporate information has risen in importance due to the possible financial implications of misuse of important data. The 2006 CSI/FBI Computer Crime and Security Survey found that 52% of the participants of their study had unauthorized computer usage. The estimated losses by those participants who could provide a figure amounted to $52,494,290 (Gordon, Loeb, Lucyshyn, & Richardson, 2006). While this statistic quantifies organizational loss, on an individual level it is important for two primary reasons. First, with increases in both the reliance on personal electronic information and personal network connectivity, individuals