2015

End User Information Security: How InfoSec Literacy Affects Business

Michael Aiello
Johnson & Wales University - Providence, MAiello01@wildcats.jwu.edu

End User Information Security: How InfoSec Literacy Affects Business

Submitted by

Michael Aiello

Johnson and Wales University

College of Management

Graduate Studies, MBA

IT6544

Professor Martin Sivula, Ph.D.

Abstract

It is commonly stated that the end user is one of the biggest security risks in a company. All it takes is once user to be socially manipulated into divulging confidential information, and critical company data can become compromised. This study will investigate the correlation between a user's InfoSec Literacy, credulousness, and their willingness to divulge information that can be used to compromise company data. A sample of the general population will be given a survey that will be presented to them as a general IT survey. On this survey, they will be first polled on their overall InfoSec literacy and social habits (as well as general computer usage and malware statistics). The participants will then be asked to divulge both public and private information about their accounts and usage patterns. Based on results we will be able to correlate InfoSec literacy and trusting behavior with the willingness to divulge their confidential information to an untrusted source. The results could impact how companies go about their training, and also may bring a change to general HR hiring practices.

End User Information Security: How InfoSec Literacy Affects Business

This research is in the area of social engineering as it pertains to the end user. Social engineering is the art of manipulating people so they give up confidential information. This can include passwords, credit card info, or to access your computer to install malware. (Criddle, 2015) In the analysis of the findings, this study will attempt to reveal factors that correlate either positively and negatively to willingness to divulge data. The hope is that a risk model can be developed to try to determine how much of a security risk any employee, or the risk of an applicant interviewing for a non-IT position.

Several studies on this topic (Stanton, Stam, Mastrangelo, & Jolton, 2005; A. Jusoh, 2006; Boon & Xu, 2006) show that end users are a major security concern for both public and private entities. Lack of self-efficacy is stated to be a concern and was identified as a contributor to risky IT behaviors. Another boundary to proper IT security was identified as a lack of understanding of the basic security functionalities of the computer.

Statement of the Problem

Many existing studies already confirm that end users are a vulnerability to information security. The problem is that the root behaviors of these users are not studied in depth. This is important to research because this study will be able to determine what factors contribute this user behavior. Knowing this will allow IT departments to train properly and will also allow HR departments to recognize IT red flags during the interview process.

Purpose of the Study

The purpose of this study is to try to find a correlations between InfoSec literacy, Credulousness, and a person's willingness to divulge confidential data. Perfect IT security is impossible, the study will look to uncover if having technologically and socially competent end users would be beneficial to both IT and the business. This is an important area of study because security breaches are becoming more common as businesses leverage technology for their critical systems. Theses breaches can cost a company hundreds of millions of dollars in losses, and may even bankrupt the company.

A sample of the general population will be given a survey that will be presented to them as a general IT survey. The responses will be logged not only for their content, but also for if they decided to abstain from answering certain questions that could compromise their IT security.

Research Question/Hypothesis

1. What effect does end user credulousness and InfoSec literacy have on a user's willingness to divulge confidential data?

As part of this study, investigation included one research hypothesis:

1. Lower rates of InfoSec literacy and higher tendency for end users to trust others will greatly increase their tendency to divulge confidential information.

Definition of Terms

1. *Credulousness* - having or showing too great a readiness to believe things. (Oxford Dictionary, 2015)
2. *IT Literacy* - Level of familiarity with the basic hardware and software (and now

Internet) concepts that allows one to use personal computers for data entry, word processing, spreadsheets, and electronic communications. (Business Dictionary, 2015)

3. *InfoSec* - The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. (The Free Dictionary, 2015)
4. *Social Engineering* - The art of manipulating people so they give up confidential information. (Criddle, 2015)

Theoretical Framework

The underlying theoretical framework is that end users are a major security vulnerability for companies. Research has been done that shows that lack of awareness on how a computer works can lead to an end user being unintentionally reckless during its use (A. Jusoh, 2006). Another study on an analysis of end user security behaviors (Stanton, Stam, Mastrangelo, & Jolton, 2005) give insight into the fact that "low technical knowledge behaviors related to password creation and sharing showed that password "hygiene" was generally poor but varied substantially across different organization types (e.g., military organizations versus telecommunications companies). Further, evidence was documented that good password hygiene was related to training, awareness, monitoring, and motivation." Meaning that less informed users show a higher rate of non-malicious reluctance to conform to password and

security policies.

Literature Review

Analysis of end user security behaviors (Stanton, Stam, Mastrangelo, & Jolton, 2005)

In this study, a survey of 1,167 American computer users was conducted to collect data on their tendencies related to password security. Along with this, they also analyzed if their reasons for their level of security was malicious, neutral, or benevolent. Another breakdown was done to show differences between the sectors they worked in. The results show that well informed and well trained employees have stronger passwords. It was also discovered that the military and finance sectors have the highest password security.

The challenges of understanding and using security: A survey of end-users (A. Jusoh, 2006)

The main focus of this research is that since end users do not understand the security functionalities of their computers, then they cannot maintain the level of security that is expected of them. The results conclude that in order for businesses to realistically protect themselves, they have to put an effort into education their users on it security practices and tools.

Methodology

Research Design

A four part survey will be conducted that will provide all the data necessary to draw conclusions on user habits. Part one will include general background info such as name, age, email address, sex, nationality, religion, Place of work, Date of birth, Nicknames, names of pets, and personality type. This section will be used to try to see if a certain culture or

attribute makes a person inherently more or less cautious with their data. Some of these questions will also be used to gauge (in addition to the responses in section 4) how willing they give information that can compromise accounts (nickname, pet names, date of birth)

Section two will include questions on general computer usage and knowledge. Likert scales will be used to gauge general computer knowledge. General computer usage, purchasing habits, perceived usefulness of computers, general attitudes toward security, and general attitudes toward computing will be measured.

Section 3 will test InfoSec Literacy. The questions to be asked in this section will provide the following data:

- How often they give passwords to other people
- Where do they store their passwords
- How often they write down passwords
- Who they trust their passwords with
- How often passwords are reset
- How complex are passwords
- How often do they get malware/viruses
- How many times have they had their identity stolen

Section 4 will test their willingness to divulge private/confidential information that can be used to compromise their own/their company's data. The purpose of this section will be to analyze only if the participant abstains from answering a question. The actual content of the responses will not be analyzed for the study. For this section, the participant will be asked to divulge:

- Email Password length
- Usernames for various sites
- Last 4 digits of social security number
- Most Commonly used password
- Length of most commonly used password

Sampling

A stratified sample of participants will be selected with a quota of 300, the participants will be working class computer users, both male and female, from 18 to 65. To get meaningful results, the sample should represent the average working class computer user. The quota of 300 should allow a five percent error tolerance for the total population of American computer users.

Instrumentation

Survey

The survey will be used because it is a good way to collect a large amount of data from a lot of people. It also has the advantage of having a vail of legitimacy, allowing the study to examine credulousness. Since the survey seems official, the hope is that some participants will divulge information that they may not have though other instrumentation methods.

Data Collection and Analysis Procedures

The surveys will be administered at various public locations (parks, coffee shops, and grocery stores) with the owners / states consent. The letter of consent for the participants will be signed before taking the survey and will be stapled to the results. An analysis of variance (ANOVA) will be performed to find correlation between participant attributes and

their security behaviors. This will provide predictive insights into behaviors based on certain attributes.

Protection of Human Rights

Participants' data will not be shared with 3rd parties and will not be used in any way that does not pertain to the study. Individuals' data will not be used on an individual basis, it will be used only as aggregated data. A copy of the study results will be mailed to the email addresses provided. No other communications will be sent to that email address and the address will not be released publically or to any 3rd parties.

Discussion

This study will provide greater insight into end user security and will provide not only recommendation for improvement, but also could reform hiring practices. The results could alter how companies go about their training, and also may bring a change to general HR hiring practices, as companies should be concerned about the InfoSec literacy of their employees. Based on results, we will be able to correlate end user attributes and InfoSec literacy with the willingness to divulge their confidential information to an untrusted source. A possible weakness that the study presents is that HR departments may value the experience of the employee more than how much of a security risk they pose. In the future, as technology advances, research might build more justification on hiring for both technology literacy as well as the fit for the position.

References

A. Jusoh, D. K. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 27-35.

Boon, N. Y., & Xu, C. (2006). Studying Users' Computer Security Behavior. *11th Pacific-Asia Conference on Information Systems*, (p. 31). New Zeland.

Business Dictionary. (2015, May 9). *IT Literacy*. Retrieved from Business Dictionary: http://www.businessdictionary.com/definition/computer-literacy.html#ixzz3ZeRwtthY

Criddle, L. (2015, May 3). *What is Social Engineering?* Retrieved from Webroot.com: http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

Oxford Dictionary. (2015, May 9). *Oxford Advanced Learners Dictionary*. Retrieved from Oxford Dictionaries: http://www.oxforddictionaries.com/us/definition/american_english/credulous

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, 124-133. Retrieved from sciencedirect: http://www.sciencedirect.com/science/article/pii/S0167404804001841

The Free Dictionary. (2015, May 9). *InfoSec*. Retrieved from The Free Dictionary: http://www.thefreedictionary.com/Infosec