Perpetua: The UAH Journal of Undergraduate Research

Volume 2 | Issue 1 Article 3

12-1-2017

Source Credibility and Cybersecurity Behaviors

Bracken Sallin
University of Alabama in Huntsville

Source Credibility and Cybersecurity Behaviors

Bracken Sallin
Department of Computer Science

Abstract – In an increasingly interdependent society characterized by omnipresent online communications, Information Systems security research is an important contributor in helping protect people and organizations from cyber-attacks. Cyber-attacks are increasing in their number and scope. In May 2017 a series of ransomware attacks affected hundreds of thousands of computers across the globe, causing significant loss of business. Understanding how people interact with IT threats is an integral step to cyber-security. In this paper, I modify and extend the model developed by Liang and Xue in their Technology Threat Avoidance Theory to evaluate the effects of source credibility on computer user's behaviors.

I. Introduction

Cybersecurity is an umbrella term that relates both the technological and human domain. Because of this it is crucial to examine the extent of the impact the two have on each-other. To understand this connection it is important to examine the role of human behavior in cybersecurity attacks. Most victims' computers were not updated, or were running outdated software. Organizations may have standing policies in place dictating IT behaviors or systems, but so long as people do not act on these protocols, security vulnerabilities will persist.

It is this vulnerable element that IT security and information assurance literature seeks to understand. While the technical infrastructures underlying security issues are generally well understood, less well developed is research on the role human behavior and communications play in Cybersecurity (Zafar and Clark, 2009). The most significant development in recent decades is the ubiquity of the internet and its impact on communications and society in general. Internet communication is increasingly characterized by the pervasive use of social media throughout the world.

Social media like Facebook, Twitter, YouTube, Instagram, and other platforms, influence the way people communicate and interact with each other, exchange ideas, and support causes and campaigns (Siemans 2005). Communication in social media is of particular interest in marketing research, which has examined how consumers and brands interact with each-other. Social media communication is interesting in that studies have found that online communications (electronic word of mouth) differ from standard word of mouth communications. This distinction has important implications in IS research, and was a critical component as we constructed our research model.

II. Background and Related Work

In developing a Technology and Source Credibility model we considered the role social media might play in impacting Cybersecurity knowledge transfer, and how the characteristics of social media and social media networks enable this (Gupta, J; Patnayakuni, N; Patnayakuni, R., 2017). To approach this and build constructs for our model, we draw from two behavioral models from prior research: the Technology Threat Avoidance Theory – TTAT, and the Elaboration Likelihood Model – ELM. (Liang and Xue 2009; Cacioppo, Petty 1986).

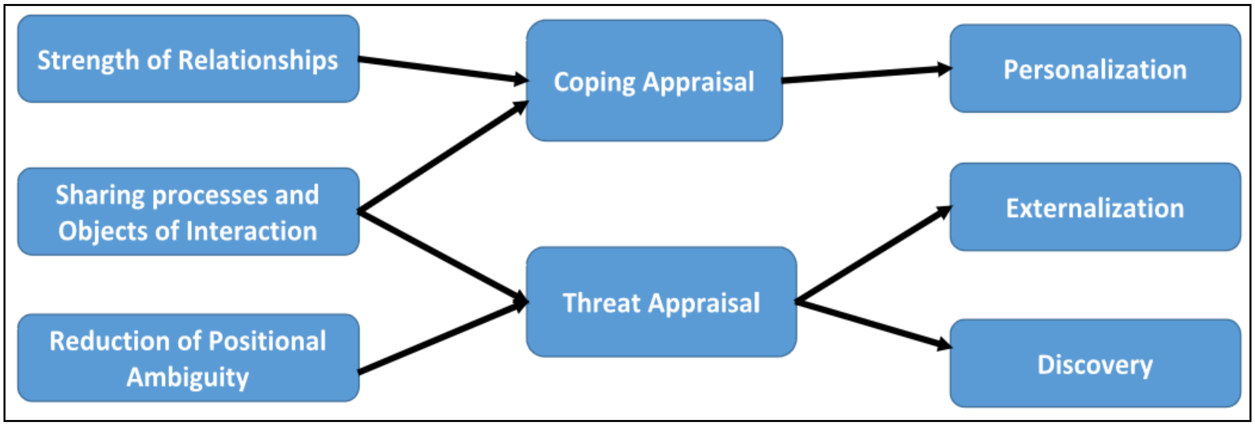

Strength of Relationships
Sharing processes and Objects of Interaction
Reduction of Positional Ambiguity
Coping Appraisal
Threat Appraisal
Personalization
Externalization
Discovery

Figure 1: Conceptual Model: (Gupta, J; Patnayakuni, N; Patnayakuni, R., 2017)

The TTAT model explains how individual users avoid IT threats in voluntary settings (Liang and Xue, 2009). Liang and Xue (2009) argue that security behaviors users engage in are a two part process that distinguishes threat appraisal from coping appraisal. Further, the TTAT posits that users are influenced by different mechanisms in each process. Threat appraisal is distinguished from coping appraisal based on the discrepancy between the two states. That is, the difference between the two is the dissonance created by an acknowledged threat and the impact it could have on the user. These distinctions are defined as driving individual attitudes and behaviors towards IT threats.

In identifying this difference, Liang and Xue (2009) developed a model using eight constructs: perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, avoidance motivation, and avoidance behavior. Liang and Xue (2009) hypothesized the relationships between these constructs in their model, and the empirical support they found for their model is the principle reason why we adopt the TTAT model for this summer’s research.

We extend the TTAT model of the threat appraisal process by adopting concepts from the Elaboration Likelihood Model into our Source Credibility model. The ELM is of interest to us in how it examines the influence of source credibility in the context of different communication types. The ELM examines cognitive processing based on how individuals respond to persuasive messages (Cacioppo, Petty 1986).

Considering the important role communication plays in influencing behavior we propose that people evaluate cybersecurity information differently in the online context than traditional news media when making appraisals of individual vulnerability. We propose that this can be evaluated using constructs adopted from the TTAT and ELM, and examined in the context of source credibility.

We define source credibility as the functional image of the source in the minds of the receivers. Studies demonstrate a strong correlation between source credibility and behavioral influence in standard communication transactions (Dholakia & Sternthal, 1977; Bansal & Voyer, 2000). As behaviors are the primary drivers behind responses to perceived threats, we adopt the TTAT’s model for our evaluative purposes.

III. Method

To test the hypothesis a questionnaire was developed that evaluated the characteristic behaviors of individuals when confronted with cybersecurity information. To distribute our questionnaire we used the online survey tool Qualtrics. Our survey was disseminated through email to all the students in the College of Business. We sent out 1223 emails, of which 489 were opened. From the opened emails we had 164 respondents. For the purposes of a pilot study, this 34% response rate was acceptable. The overall response rate of all respondents contacted, 13.4%, is also very respectable.

In the survey, two cybersecurity scenarios were created. One scenario identified the source of cybersecurity threat information as standard news media information. The other identified the source of cybersecurity threat information as social media for the same IT threat. To measure users' responses to our constructs, we used a modified Likert scale, as well as a personal inventory metric.

The first scenario we presented users with is as follows:

> "You receive the following news update from print media (for example The Wall Street Journal) or News and Cable news networks (for example NBC):
>
> Malicious software known as ransomware has been making headlines after hackers hijacked hundreds of thousands of computer worldwide. Ransomware locks up user's data and threatens to permanently delete the data if a ransom is not paid. The global impact has been across more than 150 countries across America, Europe and Asia.
>
> You have also heard that at least 66 computers on the UAH campus have been affected by the attack."

The second scenario we presented users with is as follows:

> "You receive a post from a member of your social media circle on one of your social media channels (for example Facebook):
>
> Massive ransomware attack! One of my friend's computers has been infected! She can't access her data! Pass on the information to everybody you know and ask them to be careful out there. Go to this site http://clover.vessel.com/wash/r3c5/mal.aspx to learn how to protect your computer.
>
> You have also heard that at least 66 computers on UAH campus have been affected by the attack."

This questionnaire had constructs adopted from Liang and Xue's (2009) Technology Threat Avoidance Theory and the Elaboration Likelihood Model. These constructs were: perceived susceptibility, perceived severity, perceived threat, avoidance motivation, avoidance behavior, perceived safeguard cost, and perceived safeguard effectiveness. In addition to this, we designed constructs measuring self-efficacy, issue involvement, and source credibility.

Our first three constructs were perceived susceptibility, perceived severity, and perceived threat. In our study we defined perceived susceptibility as an individual's subjective probability that a malicious IT would affect him or her. Put in the context of each scenario, we attempted to identify the strength of response to an itemized list of questions concerning this definition and how likely the individual felt they would be exposed to an IT threat.

Related to the construct of perceived susceptibility is the construct of perceived severity, which is defined as how an individual perceives the negative consequences of an IT threat. We measured this by a series of questions which examined how users felt about loss of personal information, property, or financial assets. Finally, we defined our perceived threat construct as the extent to which an individual perceived a malicious IT as dangerous or harmful. We asked people how they felt the likelihood they would be affected by the IT threat was based on the scenario they were given.

In addition to these we had three constructs measuring users' perception of safeguard measures and personal competence. In the context of these, they were: perceived safeguard effectiveness, self-efficacy, and perceived safeguard cost. We defined perceived safeguard effectiveness as an individual's subjective assessment of how effectively a given safeguard measure – such as spam filters, anti-virus, windows updating, is against a given IT threat.

With safeguard effectiveness we also designed a construct that attempted to measure a user's self-efficacy, or confidence in enacting these safeguard measures against IT threats. Finally, we designed a construct to measure safeguard cost. We defined safeguard cost as the physical and cognitive efforts required by an individual to use safeguard measures. Our intention was to evaluate individual perceptions of investment in dealing with IT threats.

The final constructs we adopted from the TTAT for our model were avoidance motivation and avoidance behavior. Avoidance motivation is defined as the degree to which IT users are motivated to avoid IT threats by taking safeguard measures. We asked survey participants if the scenario they were given influenced their security behaviors. These security behaviors are captured in the avoidance behavior construct, which is defined as the extent to which individual motivation influences action against IT threats.

Last, we created a construct measuring users' issue involvement. We adopted this construct from McQuarrie and Munson's (1987) personal involvement inventory, and defined it as the extent with which an individual user is engaged with cybersecurity. In designing this, we hoped that a strong involvement would correlate to a higher net avoidance motivation and behavior.

In addition to collecting data on these constructs, we collected general demographic information on survey respondents. This data included: gender, class standing, major, number of credit hours taken each semester, computer and internet usage, and educational experience of parents.

IV. Results and Analysis

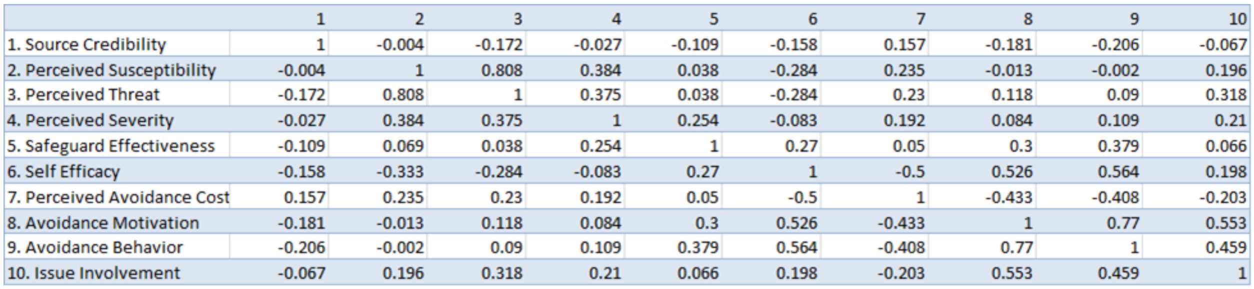
A series of statistical analyses were performed on our data. Using Excel, R, and SPSS we examined our data using a variety of statistical techniques, and for the purpose of this paper relied primarily on correlation analysis. We summarized our most important findings by their r values. Our findings are represented by the following correlation matrix. In the matrix the r value for each construct is given in relation to another construct.

R values denote the strength and direction of correlation between two variables in a linear relationship. While accepted or expected r levels vary by discipline and topic, studies like ours report a strong relationship for values of .7 or higher, and a moderate relationship of .5 or higher. The high r values displayed in our correlation matrix signify a need for more investigation on our model and research in this area.

In our data we found that source credibility was not found to have any noticeable effect on our model's constructs (no statistically significant r value above .157), but other worthwhile findings emerged (Figure 1). Not only did each scenario test differently, but pronounced relationships were found between several of our constructs.

First, we found a strong correlation of .808 between perceived susceptibility and perceived threat. We also found a suggestive r value of .564 between our self-efficacy and avoidance behavior constructs and an r value of .526 between our self-efficacy and avoidance motivation constructs. Furthermore, we found a strong positive correlation between avoidance motivation and avoidance behavior of .77. Finally, indicative r values of .553 and .459 were found between our issue involvement, avoidance behavior and avoidance motivation constructs. Taken together, these r values suggest a moderate to strong positive correlation between the mentioned constructs (Figure 1).

Other interesting relationships also emerged from the correlation matrix. The perceived severity and perceived susceptibility constructs had an r value of .384. As well, perceived severity and perceived threat had an r value of .375 (Figure 1). Though these have no effect on our hypothesis, these lower values may provide interesting avenues for future exploration and research.



	1	2	3	4	5	6	7	8	9	10
1. Source Credibility	1	-0.004	-0.172	-0.027	-0.109	-0.158	0.157	-0.181	-0.206	-0.067
2. Perceived Susceptibility	-0.004	1	0.808	0.384	0.038	-0.284	0.235	-0.013	-0.002	0.196
3. Perceived Threat	-0.172	0.808	1	0.375	0.038	-0.284	0.23	0.118	0.09	0.318
4. Perceived Severity	-0.027	0.384	0.375	1	0.254	-0.083	0.192	0.084	0.109	0.21
5. Safeguard Effectiveness	-0.109	0.069	0.038	0.254	1	0.27	0.05	0.3	0.379	0.066
6. Self Efficacy	-0.158	-0.333	-0.284	-0.083	0.27	1	-0.5	0.526	0.564	0.198
7. Perceived Avoidance Cost	0.157	0.235	0.23	0.192	0.05	-0.5	1	-0.433	-0.408	-0.203
8. Avoidance Motivation	-0.181	-0.013	0.118	0.084	0.3	0.526	-0.433	1	0.77	0.553
9. Avoidance Behavior	-0.206	-0.002	0.09	0.109	0.379	0.564	-0.408	0.77	1	0.459
10. Issue Involvement	-0.067	0.196	0.318	0.21	0.066	0.198	-0.203	0.553	0.459	1

Figure 2: Correlation Matrix

V. Conclusion

Future models for research like this should more strongly distinguish the constructs between individual scenarios. Due to significant time constraints it was impossible to design, test, refine, and analyze data from our model in a desired fashion. Different and more thorough statistical analyses might provide more revealing information about our data sets. Second, our survey was constrained to a small population of business students at the University of Alabama in Huntsville. As such, it is possible our results are not representative of a wider demographic. Differences we noted in scenario treatments might be more pronounced, or more suggestive provided a larger and more diverse sample set. Finally, it is possible our treatment of our individual constructs could be adjusted to make user evaluation of source credibility in response to each scenario more meaningful or personal.

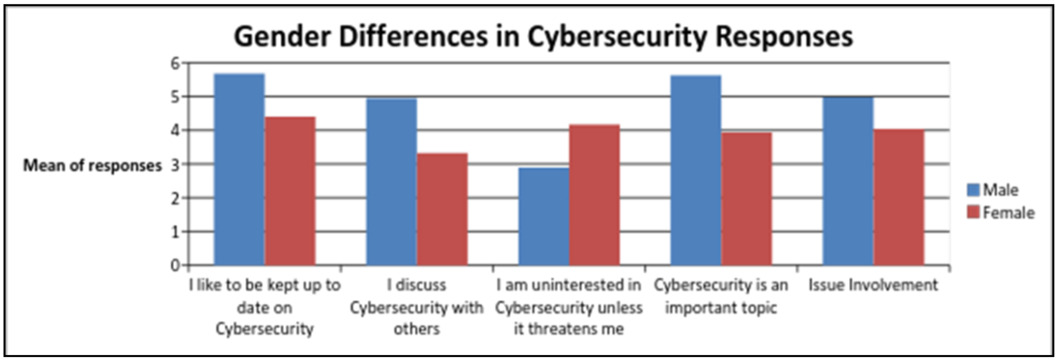


Figure 3: Gender Differences in Cybersecurity Responses

In spite of the data not immediately supporting our source credibility model, some meaningful observations emerge from the larger data-set in the context of demographic information collected. For example, an analysis of the constructs between genders shows that each scenario was treated differently. Further, a significant difference exists across the strength of IT engagement between genders. Women were found to be less involved and confident in enacting safeguard measures for IT threats. In the following chart the mean score of responses for men and women across our issue involvement constructs is listed. Each data point shows the disparity of responses between men and women.

This data may provide useful avenues of research in the future. Currently, there is a paucity of IT literature on gender involvement in cybersecurity. If our sample data is representative of the larger population, understanding why this disparity exists, and what mechanisms underlie it could prove useful in constructing cybersecurity responses to threats that considers both men and women's engagement.

Cybersecurity is a cybernetic process. It should consider both the hardware capital and human resources available. In the future, creating a secure environment in which governments, businesses, and individuals interact will require research in both the computer and behavioral sciences. No matter how efficient or failsafe a technical infrastructure is, human behavior will remain an integral part of IT security. Current consumer research – such as the use of big data in targeting customers, may be useful to businesses and organizations in understanding the IT behaviors of its employees or constituents. A successful IT infrastructure in the future may constitute of individual training armed by data in addition to anti-virus software, spam filters, and firewalls.

Bibliography

Siemens, G. (2005). “Connectivism: A learning theory for the digital age.” *International journal of instructional technology and distance learning*, 2(1), 3-10.

Gupta, Jatinder N.D., Patnayakuni, Nainika, Patnayakuni, Ravi. “Towards a Model of Social Media Impacts on Cybersecurity Knowledge Transfer: An Exploration.” (2017)

Liang, Huigang, and Yajiong Xue. “Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective.” *Journal of the Association for Information Systems* 11, no. 7 (2010): 394.

Cacioppo, John T. Petty, Richard E. “The Elaboration Likelihood Model of Persuasion.” *Advances in Experimental Social Psychology*, vol.19. Academic Press, 1986.

Dholakia, R., & Sternthal, B. Highly Credible Sources: Persuasive Facilitators or Persuasive Liabilities? The Journal of Consumer Research, 3, (1977): 223–232.

Edward F. McQuarrie and J. Michael Munson (1987),"The Zaichkowsky Personal Involvement Inventory: Modification and Extension", in NA - Advances in Consumer Research Volume 14, eds. Melanie Wallendorf and Paul Anderson, Provo, UT : Association for Consumer Research, Pages: 36-40