Behavioral Experiments Exploring Victims' Response to Cyber-based Financial Fraud and Identity Theft Scenario Simulations

Heather Rosoff
Sol Price School of Public Policy
University of Southern California
rosoff@usc.edu

Jinshu Cui
Department of Psychology
University of Southern California
jinshucu@usc.edu

Richard John
Department of Psychology
University of Southern California
richardj@usc.edu

ABSTRACT

We conducted two scenario-simulation behavioral experiments to explore individual users' response to common cyber-based financial fraud and identity theft attacks depend on systematically manipulated variables related to characteristics of the attack and the attacker. Experiment I employed a 4 by 2 between-groups factorial design, manipulating attacker characteristics (individual with picture vs. individual vs. group vs. unknown) and attack mode (acquiring a bank database vs. obtaining personal bank account information) in response to a bank letter scenario notifying respondents of a data breach. Respondents' positive and negative affect, perceived risk, behavioral intention and attitude towards the government's role in cyber security were measured. Results suggest that respondents experienced greater negative affect when the attacker was an individual, as well as experienced more positive affect when the attack target was an individual bank account. In addition, a picture of an individual attacker increased intended behavioral changes and expectations of the bank to manage the response in the bank database attacks only. Experiment II utilized a 4 by 3 between-groups factorial design, manipulating attacker motivation (fame vs. money vs. terrorism vs. unknown) and attack resolution status (resolved vs. still at risk vs. unknown) in response to an identity theft scenario that evolves over four time points. In this experiment, respondents' affect, perceived risk and intended short- and long-term behavior were measured at each time point. Results suggest that respondents reported less perceived risk when the attacker's motivation was to fund terrorism. Respondents also reported lower negative affect and lower perceived risk when the identity theft case was reported as resolved. Respondents also were more willing to pursue long-term behavior changes when the attack outcome was still at risk or unknown. In both experiments, respondents' sex and age were related to affect, risk perception, and behavioral intentions. The paper also includes discussion of how further understanding of individual user decision making informs policy makers' design and implementation of cyber security policies related to credit fraud and identity theft.

1. INTRODUCTION

With the advent of the information age, cyber attacks have exploded as a major concern. As stated by the Officer-in-charge at the United National Interregional Crime and Justice Research Institute (UNICRI), "The likelihood of suffering from a real crime, like being robbed in the street, is now smaller than the possibility of suffering a virtual crime, such as an online identity theft or a credit card fraud." Individual users' decision making is critical to determining whether a cyber attack can be committed and what the extent of that damage might be (Rosoff, Cui, & John, 2013). This is complicated by the information asymmetry between the attackers and individual users. With limited information as to the causes and consequences of cyber threats, individual users often trigger attacks unintentionally and consequently react poorly and suffer from severe outcomes. While the characteristics and motivations of attackers have been investigated thoroughly by defenders to better understand how to detect threats and protect cyber systems (D'Amico, Whitley, Tesone, O'Brien, & Roth, 2005; Liu, Yu, & Mylopoulos, 2003; Nykodym, Taylor, & Vilela, 2005), there is limited research on how information about attackers influences individual users' emotional, cognitive and behavioral responses to cyber threats.

This paper reports the results of two scenario-based experiments of a cyber-based financial fraud or identity theft attack. These experiments utilize a scenario simulation methodology that includes an experimental manipulation, instead of the traditional survey-based scenario, as well as stimulus material to enhance the scenario's realism. More specifically, in Experiment I we explored whether attacker characteristics and attack mode influenced the victim's reaction and behavioral response to a data breach at their bank. In Experiment II, we assessed whether the attacker's motivation and the resolution status of the attack affected the victim's emotional, cognitive, and behavioral response for an identity theft case. We believe the use of narrative scenarios and images are more compelling and concrete to respondents, and increase the likelihood of obtaining valid responses compared to less concrete scenario stimuli. Furthermore, in both scenario simulations, all but the manipulated variables are held constant so that any significant findings can be attributed to the manipulated variables.

In Experiment I, we hypothesized that attacker characteristics, specifically those accompanied by a photograph, would decrease feelings of vulnerability and result in fewer behavioral changes in response to the cyber-based data breach at the bank (financial fraud). This hypothesis follows from construal theory (Trope and Liberman, 2010); pictures are more concrete representations, resulting in a lower level of construal, compared to words which are more abstract and distant representations associated with higher level construal. This finding has been reported in the disaster literature and has shown that images have the potential to lower negative affect and perceived risk (Peters and Slovic, 1996; Leiserowitz, 2006). Furthermore, the direction of behavioral decision making, with respect to level of involvement in response efforts, tends to coincide with affective and risk reactions; lower perceived risk and negative affect more often predict more moderated behavioral changes in response to an event (Terpstra, 2011).

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9-11, 2014, Menlo Park, CA.

Also for Experiment I, we anticipated that there would be some influence of attack mode on affective reactions and behavioral responses to the bank data breach. Crime research has shown that personal victims of crime experience increased fear and vulnerability that translates into a greater willingness to adopt crime reduction measures. This is compared to widespread neighborhood crime where collectively victims also experience increased feelings of vulnerability, yet their willingness to act is moderated by their expectation of local officials to be proactively involved in the response (Skogan and Maxfield, 1982; Norris et al., 2008; L.W., 2012). We anticipated that in the cyber context, individual victims of an attack on a personal bank account or group victims of an attack on a bank database also would have a negative reaction to the event. We expected that for the victims of the personal bank account attack this would lead to more proactive efforts to resolve the consequences associated with the data breach compared to the database victims.

In Experiment II we anticipated that the attacker's motivation would depend on the perceived psychological distance from the cyber-based identity theft case, and in turn, this would influence users' perceived risk and decision making. This expectation is also based on construal theory which suggests that the more distant an object is from the individual, the more abstract it will be thought of, while the closer the object is, the more concretely it will be thought of (Trope & Liberman, 2003, 2010; Trope, Liberman, & Wakslak, 2007). In the cyber context, we expected that the more concrete the attacker motivation, the greater the perceived risk of identity theft.

Also in Experiment II we explored the extent to which the resolution of the identity theft case influenced victim's thinking and behavioral reactions to the attack. We hypothesized that the level of uncertainty associated with an unresolved or unknown outcome would threaten victims' sense of control, resulting in increased negative affect and heightened risk perceptions (Slovic, Fischhoff and Lichtenstein, 1980; Vlec and Stallen, 1980) Furthermore, respondents are believed to perceive the unresolved and unknown identity theft case outcomes as putting them in harm's way, which also is a determinant of elevated behavioral responses (Slovic, Fischhoff and Lichtenstein, 1984; Slovic, 1987).

Lastly, we considered how demographic variables affect the strength and/or the direction of the relationship between the manipulated variables, attacker characteristics, attacker motivation, attack mode, and attack resolution status, and the dependent variables, affect, perceived risk and behavioral intention. For example, one possibility is that the perceived risks posed by financial fraud or identity theft tend to be judged lower by men than women (Garbarino et al., 2004; Bhatnager and Misra, 2000); consequently, women are expected to have a stronger desire than men to modify their cyber behavior. Another possibility is that the reliance on a third party to assist in the necessary behavior change in response to financial fraud or identity theft would be less for younger users because they are more familiar and comfortable with the nuances of internet security options. Overall, we anticipated that there would be some difference in the patterns of response as a function of sex and age for Experiment I, and sex for Experiment II.

The next section of this article describes the methods, results, and a brief discussion for Experiment I, and Section 3 describes the methods, results, and a brief discussion for Experiment II. The paper closes with a discussion of study limitations and how these results have the potential to enhance and improve cyber security by taking into account end-user decision making.

2. EXPERIMENT I

2.1 Methods

In August of 2013, we conducted an experiment involving a cyber-based bank attack with two manipulated variables, attacker characteristics and attack mode, to evaluate individual's emotional response, perceived risk, and behavioral intention in response to the event. The bank data breach scenario was developed to capture a common financial fraud event that significantly affects individual users. More specifically, the dependent variables focused on individuals' positive and negative feelings about the event, the perceived risk to financial security and the likelihood of a second event, and decision making related to banking, ranging from relying on the bank to manage the attack response versus discontinuing all banking activity.

Table 1. Scenario and Manipulations (Experiment I)

Manipulations	Scenario			
	August 2, 2013 Dear Valued Customer, We are writing to notify you that two days ago,			
Attack mode	there was an unauthorized attempt to withdraw all of your current funds. *(personal)*	there was an unauthorized breach into our customer information center, which stores credit card and personal information for all 10 million of our clients *(database)*.		
Attacker characteristics	As of now, we know an individual online hacker is responsible for the breach into your account. The hacker acted alone in carrying out the attack. *(individual)*	As of now, we know a hacking group is responsible for the breach into your account. An organization of hackers coordinated the attack. *(group)*	As of now, we do not know if a hacking group or an individual hacker is responsible for the breach. *(unknown)*	As of now, we know the individual online hacker pictured below is responsible for the breach into your account. The hacker acted alone in carrying out the attack. *(individual with picture)*
	We are working with law enforcement officials and regret any concern or inconvenience this incident may have caused you. We will keep you informed as we make progress in his capture. Kindest Regards, Your Bank			

2.1.1 Design Overview

A 4 (attacker characteristics) by 2 (attack mode) between-groups factorial design was used to explore responses to a bank letter notifying respondents of a data breach. Each respondent was randomly assigned to one of eight conditions. The four attacker characteristics are (1) individual with picture, (2) individual, (3) group, and (4) unknown; the two attack modes are (1) acquiring a bank database and (2) obtaining personal bank account information. The experiment was submitted to the University of Southern California's Institutional Review Board (IRB) and the IRB determined that study qualified for Exempt, Category 2 research.

The experiment opened with respondents first providing demographic information (sex and age) and answering a series of questions regarding their previous online experience. They were then presented with the bank notification letter. The content of the notification and manipulations contained is provided in Table 1.

After reading the bank notification, respondents were asked to evaluate their negative affect, positive affect, cyber risk perception, threat belief, intended behavioral response, and attitudes toward the role of government in preventing cyber attacks.

2.1.2 Measures

Respondents' current feelings, risk perception, behavioral intention and attitude towards the government's role in cyber security were measured following receipt of a bank notification alerting the respondent to the cyber attack. Details of the items in each measure are included in Table 2.

Affect. The Positive Affect Negative Affect Scale (PANAS) was included to measure self-reported emotion (Watson, Clark, & Tellegen, 1988). The version used was an abbreviated 10-item PANAS (Rosoff, Siko, John, & Burns, 2013). Each affect item was rated from 1(not at all) to 5 (extremely). Principal axis factoring was performed on the 10-item PANAS and two factors were extracted. Items were internally consistent with Cronbach's alphas = .94 and .84 for negative and positive affect, respectively.

Risk Perception. Respondents also were asked to estimate personal financial safety using a scale from 0 (not at all risky) to 10 (extremely risky), vulnerability to identity theft using a scale from 0 (not at all vulnerable) to 10 (extremely vulnerable), likelihood of an attempted second attack using a scale from 0% (not at all likely) to 100% (very likely), and likelihood of a successful second attack using a scale from 0% (not at all likely) to 100% (very likely). The scores for the first two items were multiplied by 10 to equal the ranges of the likelihood items. Principal axis factoring was performed and one factor was extracted. Items were internally consistent with a Cronbach's alpha = .83.

Behavioral Intention. Respondents assessed their intended behavior on a 5-point scale (1=strongly disagree to 5=strongly agree). From the six behavioral intention questions, two factors were extracted. The first factor, moderate behavioral intention, captured expectations relative to the bank's response to the event. This included "get credit checked", "expect bank to enhance security", and "expect bank to reimburse" with a Cronbach's alpha = .63 and rotated loadings all above .68. The second factor, severe behavioral intention, addressed behavioral decisions related to discontinuing the use of financial services. This factor included "no longer online bank", "cancel credit cards", and "discontinue all online financial activities" with a Cronbach's alpha = .75 and rotated loadings all above .69.

Attitude towards the Government's Role in Cyber Security. Respondents evaluated their attitude towards the government's role in online protection on a 5-point scale (again 1=strongly disagree to 5=strongly agree) for 4 items listed in Table 2. The four items were internally consistent with a Cronbach's alpha = .71.

Table 2. Measures of Experiment I

Scales	Items
Negative affect	distressed, afraid, upset, nervous, scared
Positive affect	enthusiastic, inspired, strong, determined, active
Risk perception	(1) What do you believe the risk is to your personal financial safety?
	(2) How vulnerable do you believe you are to becoming a victim of identity theft?
	(3) What do you believe to be the likelihood of an attempted second cyber attack on your bank?
	(4) What do you believe to be the likelihood of a successful second cyber attack on your bank?
Intended behavior	(1) I would start using another bank.
	(2) I would no longer online bank.
	(3) I would get my credit checked.
	(4) I would cancel my credit cards.
	(5) I would expect my bank to enhance its security.
	(6) I would expect my bank to reimburse me for any fraudulent charges on my account.
	(7) The hacker(s) responsible for the cyber attack described should go to jail.
	(8) I would discontinue all online financial activities.
Attitudes toward government role in cyber security	(1) I am not willing to give up some of my privacy for greater online protection.
	(2) The government needs to increase its Internet security initiatives.
	(3) I don't mind if the government has access to my personal information in order to increase security.
	(4) I am not worried about cyber attacks on the American government.

Table 3. Demographic Information and Cyber-related Experience

Variables (N = 239)	Response Category	Number and Percentage
Do you shop online?	Yes	235 (98.3%)
	No	4 (1.7%)
	I don't know	0 (.0%)
Do you bank online?	Yes	222 (92.9%)
	No	16 (6.7%)
	I don't know	1 (.4%)
Has your identity ever been stolen?	Yes	15 (6.3%)
	No	214 (89.5%)
	I don't know	10 (4.2%)
Has your credit card ever been stolen?	Yes	51 (21.3%)
	No	186 (77.8%)
	I don't know	2 (.8%)
Have you been trained in Internet security either independently or by your employer?	Yes	54 (22.6%)
	No	182 (76.2%)
	I don't know	3 (1.3%)
Sex	Male	136 (56.9%)
	Female	103 (43.1%)
Age	18-25	68 (28.5%)
	26-30	50 (20.9%)
	31-35	37 (15.5%)
	36-40	25 (10.5%)
	41-45	21 (8.8%)
	46-50	10 (4.2%)
	51-55	9 (3.8%)
	56-60	10 (4.2%)
	61-65	5 (2.1%)
	66+	4 (1.7%)

2.1.3 Respondents

The experiment was hosted on Qualtrics.com and respondents were recruited from Amazon Mechanical Turk (AMT). Two-hundred and forty-three adult respondents participated and were paid $0.55 for their participation. Four of the 243 respondents were removed for answering the attention check question incorrectly. Two-hundred and thirty-nine respondents were included in the analysis. The number of respondents assigned to each of the eight design conditions ranged from 29 to 31. The median time for completion was 6 minutes. Table 3 provides demographic information and a summary of cyber-related experience for the respondents.

Composite scores were calculated across items using equal weighting for the six dependent variables: negative affect, positive affect, risk perception, severe behavior, moderate behavior, and attitudes toward government role.

2.2 Results

Least squares regression was used to predict respondents' scores on the six dependent variables (positive affect, negative affect, risk perception, moderate behavioral intention, extreme behavioral intention and attitude towards the government's role in cyber security) from the two manipulated variables (attacker characteristics and attack mode), and respondent characteristics (sex and age). To fully examine the influence of attacker characteristics, three orthogonal contrasts were created and entered into the regressions as independent variables: (1) individual and individual with picture vs. group and unknown, (2) individual vs. individual with picture, and (3) group vs. unknown.

Results indicate that respondents' negative affect was significantly greater when the cyber attack was conducted by an individual attacker compared to an individual attacker with a picture (standardized $\beta = .135$, $t = 2.088$, $p = .038$, $R^2 = .068$). No significant difference was found between an individual attacker and an individual attacker with picture for reported positive affect, risk perception, intended behavior and attitudes toward the government. In addition, positive affect was found to be significantly influenced by the attacker's selected attack mode (standardized $\beta = .143$, $t = 2.275$, $p = .024$, $R^2 = .108$). Respondents experienced more positive affect when their personal account was directly attacked compared to a compromised bank database. Negative affect, risk perception, intended behavior and attitude towards the government were not significantly influenced by the attacker's selected attack mode.

A significant interaction between attacker characteristics and attack mode relative to respondents' expectations of bank services was also found (standardized $\beta = .137$, $t = 2.106$, $p = .036$, $R^2 = .044$). Interestingly, there was an expectation from all respondents that the bank would enhance its security in response to the security breach. Moreover, respondents had even higher expectations of the bank to resolve the cyber attack when the attack was targeted against their personal account versus the bank's database, independent of the attacker's characteristics. In addition, when the attacker directly targeted only the personal account of the victim, the expectation for bank involvement was significantly greater when the individual attacker was presented with a picture compared to no picture. No significant interaction effect was found between the two manipulated variables for negative affect, positive affect, risk perception, intended behavior, and attitude towards the government. Moreover, emotional, cognitive, and behavioral reactions were found to not differ significantly between individual attacker and individual attacker with a picture vs. group and unknown attacker and between group vs. unknown attacker. Figure 1 displays the mean negative affect, positive affect and expectation of the bank/intent to continue bank service for different attacker characteristics and attack modes.

Lastly, regression results indicated that sex was predictive of negative affect (standardized $\beta = .165$, $t = 2.466$, $p = .014$), risk perception (standardized $\beta = .155$, $t = 2.301$, $p = .022$), and attitudes toward the role of government in preventing a cyber attack (standardized $\beta = .151$, $t = 2.324$, $p = .021$). Female respondents tended to experience more negative affect, perceive more risk, and were more likely to support the government's intervention. Sex was not significantly predictive of positive affect and behavioral intention. Age also was found to significantly predict positive affect (standardized $\beta = .278$, $t = 4.295$, $p < .001$) and attitudes toward the government's role in online protection (standardized $\beta = .189$, $t = 2.924$, $p = .004$). Older respondents tended to experience more positive affect and greater support for the government's intervention in online security. Age was not found to significantly predict negative affect, risk perception, and behavioral intention.

2.3 Discussion

The results of Experiment I suggest that respondents negative affect, positive affect and expectation of the bank's response (moderate behavioral intention) to the cyber-based bank data

breach were significantly influenced by the manipulation of attacker characteristics and attack mode. Consistent with our hypothesis, respondents appear to have experienced less negative affect because the picture is interpreted as a more concrete, less distant representation of the attacker. While traditional construal level theory research has found that more concrete objects are associated with greater negative affect, in the cyber attack context this pattern of results is reversed. This is because the perception of the attacker in cyber space is abstract and distant, resulting in a baseline of high negative affect. As such, as the attacker becomes more familiar and close through a picture, negative affect is shown to decrease.

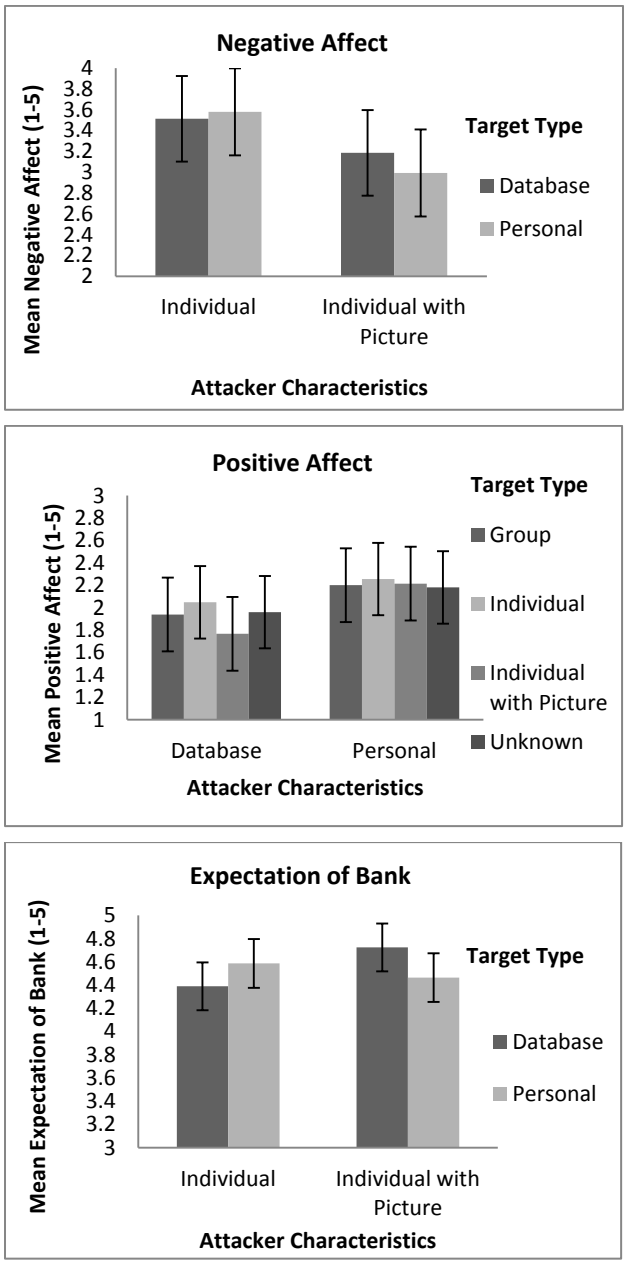


Figure 1. Mean negative affect, positive affect, moderate behavioral intention - to continue using banking services - for attacker characteristics and attack targets. Note: Error bars are +/- 2 SE.

We also found that respondents felt more enthusiastic, inspired, strong, determined, and active when only their personal account was victimized than when their bank's account database was compromised. As described above, positive affect includes words suggestive of the amount of energy one would expend in response to the cyber threat. As such, respondents expressed a greater desire to take action only when their personal account was hacked compared to victims of the database hack for which the responsibility to act tended to be diffused. One explanation is that the attack mode (in this case, the bank) is likely to take the lead in the response effort to protect again the potential cost of the attack to their reputation and profit/success. One might expect that banks make the needs of database victims a priority, which diffuses the desire to act between the attack mode owner and database members.

In addition, there was a significant interaction between attacker characteristics and attack mode. When a personal account was hacked, respondents were more likely to count on the bank if the picture of the attacker was presented. Conversely, when the bank database was compromised, respondents were indifferent to whether the picture of the attacker was provided.

Also, as anticipated, we found that female respondents experienced more negative affect, perceive more risk, and were more likely to support the government's intervention in online security. Disaster risk perception studies also have shown that risks tend to be judged higher by females (Kung and Chen 2012; Bourque et al. 2012) and that females tend to have a stronger desire to take preventative and preparedness measures compared with males (Ho et al. 2008; Cameron and Shah 2012). We also found an age effect suggesting that older respondents tended to experience more positive affect and in turn, were more likely to support government intervention in online security. Results related to the role of victim age in the crime and disaster literature have been conflicting (Hale, 1996; Fischhoff, 2003; Sjöberg, 2005; Henson, Reyns, & Fisher, 2013) and our findings reflect the perspective that there are significant age differences.

The overall policy implications of these findings depend on the financial institutions' respective objectives. If the ultimate goal is to calm bank members down following a cyber breach, as opposed to enhance their concern and increase their avoidance behavior, our findings suggest that sharing a photo has the potential to be helpful. However, if the financial institution is interested in having both the bank and bank members engage in protective behaviors, sharing a photo of the attacker does not appear to be the best tactic for encouraging member emotional investment in threat resolution and engagement in avoidance behavior. Gender and age findings further suggest that females and older respondents have the potential to be more inclined to support policy recommendations. However, additional research relative to specific policy compliance with a larger sample is needed for an assessment of the moderating effects of demographic variables. Overall, such variations in policy considerations allow for financial institutions to more effectively assess the trade-offs between the social impacts and costs associated with policy implementation.

3. EXPERIMENT II

3.1 Methods

In Experiment II, we continued to manipulate attacker attributes. Particularly, we manipulated attacker's motivations to commit a

cyber attack and measured the impact on respondents' emotional reactions, perceived risk and decision making. We also continued to explore the impact of financial fraud in the context of an identity theft scenario that evolves over four time points (compared to the bank data breach scenario described at a single time point). Similar to the bank data breach scenario, identity theft has the potential to present serious inconveniences for the victim. The time and effort a victim might have to spend responding to and resolving an identity theft case could be substantial. Therefore, we also manipulated the level of resolution associated with the outcome of the identity theft scenario. In order to ensure that the significant findings were attributed to the manipulated variables, attacker motivations and resolution status were manipulated at two separate time points. Ultimately, this experimental design consisted of a 4 (attacker's motivation – fame, money, terrorism and unknown) by 3 (attack resolution status – resolved, still at risk, and unknown) between-groups factorial design.

3.1.1 Design Overview

This experiment was conducted in November, 2013 and based on a 4 (attacker's motivations) by 3 (resolution status) between-groups factorial design. Each respondent was randomly assigned to one of twelve conditions. The four levels of attacker's motivations were fame, money, terrorism, and unknown, and the three levels of resolution status were resolved, still at risk, and unknown. The unknown conditions were included as levels in both variables as no information control conditions for comparison. The experiment was submitted to the University of Southern California's Institutional IRB and it was determined that the study qualified for Exempt, Category 2 research.

The scenario unfolds over four time periods (or scenes). During Scene 1, respondents received a credit card statement in their name from a company with which they do not have account and there were charges totaling $500. During Scene 2, respondents received a voicemail from the identity theft unit of the local police department indicating an investigation was underway and they believed the respondent's computer had been compromised by the attacker, resulting in his/her identity theft. Attacker motivation was manipulated in the content of the investigator's voicemail. He indicated that the attacker was stealing the respondent's identity to either: (1) increase his visibility and reputation within the attacker community, (2) use the compromised identity to purchase luxury items, (3) use the identity to provide financial support to a middle eastern terrorist group, or (4) was unknown (control condition).

Table 4. Scenario and Manipulations (Experiment II)

Time 1	This morning in the mail you received a credit card statement in your name from a company with which you do not have an account. As you looked over the statement, you noticed several cash advances totaling $500.
Questions	PANAS
Time 2	One week following your receipt of the suspicious credit card statement, you receive the following voice mail: "Good morning, my name is Gabriel Dawson from the Identity Theft Unit of the Police Department. Our investigation into a cyber perpetrator has led us to believe your personal computer has been compromised. We believe this individual hacked into your computer and obtained access to your email account and the cache data of your online activities. In doing so, he was able to obtain your usernames, passwords, banking information, and other personal information. Our investigation thus far shows no evidence that can confirm the perpetrator's intent. (**unknown perpetrator's intent**) / Our investigation thus far shows that the perpetrator is hacking into victims' computers to increase his visibility and reputation within the attacker community. (**fame**) / Our investigation thus far shows that the perpetrator is using the victims' identities to purchase luxury items. (**money**) / Our investigation thus far shows that the perpetrator is using the victims' identities to provide financial support to a Middle Eastern terrorist group. (**terrorism**) I plan to be in touch in the coming weeks to report on the progress of our investigation. Please be vigilant in reporting to us any suspicious mail, email, or phone call. Thank you."
Questions	PANAS, risk perception, short-term behavior
Time 3	In the days following the call from the Identity Theft Unit, you notice an increase in suspicious activity. You are receiving more spam emails, junk mails and phone calls from solicitors. More notably is your receipt of a phone call from the Department of Motor Vehicles confirming the issuance of a new driver's license you did not order. You also receive a letter in the mail from the Internal Revenue Service inquiring about your filing of duplicate income tax returns, suggesting that fraudulent returns were submitted in your name.
Questions	PANAS
Time 4	Moving ahead to several weeks following the call from the Identity Theft Unit of the Police Department, you receive yet another credit card statement in the mail from a company with which you do not have an account. This statement has a $1,500 balance. It is clear that you are continuing to experience complications as a result of your identity theft and that you are still at risk. (**still at risk**) / Moving ahead to several weeks following the call from the Identity Theft Unit of the Police Department, you recently have not received any suspicious communications or an update from the police indicating whether your identity remains at risk or not. It is unclear whether you will continue to experience complications as a result of your identity theft and if this situation has been resolved. (**resolved**) / Moving ahead to several weeks following the call from the Identity Theft Unit of the Police Department, you receive a second voicemail from Gabriel Dawson at the Police Department. He is calling to inform you that the perpetrator has been arrested and they have seized all software and electronic devices containing compromised personal data, and removed all sources online containing this information. Fortunately, you are no longer experiencing complications as a result of your identity theft and the situation is resolved. (un**resolved**)
Questions	PANAS, risk perception, long-term behavior

By Scene 3, additional evidence as to how the respondents identify was being used for identity theft was presented. Lastly during Scene 4, the resolution status of the identity theft case was reported and manipulated. Subjects either (1) received another suspicious credit card statement indicating their identity was still at risk, (2) received another call from the police indicating the attacker had been arrested and that all appropriate security measure had been take to resolve their identity theft case, or (3) received no additional information, indicating the outcome was unknown (control condition).

Following each scene, respondents were asked to evaluate their current feelings in response to the identity theft scenario. In addition, following Scene 2, respondents were asked to evaluate their perceived risk and intended short-term behavioral changes, if any. Also following Scene 4, respondents were asked to assess their perceived risk and long-term behavioral intentions. At the close of the experiment, respondents were asked to provide basic demographic information and answer questions regarding their cyber experiences and what measures they take to currently protect themselves from identity theft. A complete description of all four scenes, including the manipulations and questions following each scene, is provided in Table 4.

3.1.2 Measures

Respondents' current feelings, risk perception, intended short-term behavior and long-term behavior were measured. Details of the items in each measure are included in Table 5.

Affect. Positive Affect Negative Affect Scale (PANAS) (Watson, et al., 1988) was included following each scene to measure self-reported emotion. Only the 10-item negative affect scale was included. Each item was rated from 1(not at all) to 5 (extremely). Principal axis factoring was performed on the ten negative items of the PANAS scale from Scene 1 through Scene 4. Eight items were extracted when the number of factors was constrained to one. The two items not included in the factor were ashamed and guilty. The eight items were internally consistent with a Cronbach's alpha = .93, .92, .92 and .95, for each scene respectively.

Table 5. Measures of Experiment II

Scales	Items
Negative affect	scared, afraid, upset, distressed, jittery, nervous, ashamed, guilty, irritable, hostile
Risk perception	(1) it is just amount of time before my personal financial information is obtained
	(2) credit card fraud is very common
	(3) credit card fraud creates a major financial loss for consumers and credit card companies
	(4) identity theft is a major threat to personal privacy
	(5) identity theft cases are difficult to resolve
	(6) identity theft typically results in long-term inconveniences to the victim
	(7) the risk of identity theft is not of concern to me
	(8) if my identity is stolen, I will have to spend a lot of money fixing the problem
Short-term behavioral intentions	(1) contact the credit card company
	(2) contact the consumer credit reporting agencies
	(3) call the police
	(4) contact the Department of Motor Vehicles (DMV)
	(5) contact the Social Security Administration (SSA)
	(6) contact the Internal Revenue Service (IRS)
	(7) do nothing
	(8) cancel all your credit cards
	(9) discontinue online financial transactions
	(10) other (text box)
Long-term behavioral intentions	(1) I will use my credit card for purchases significantly less than before
	(2) I will prefer to pay for purchase items in cash
	(3) I will request the free 90 days "fraud alert" service from one of the consumer credit reporting agencies that notifies me of any request for a new line of credit in my name
	(4) I would be willing to pay $10/month ($120/year) to subscribe to a protection service that lowers my risk of identity theft
	(5) I will check my credit more often than before
	(6) I will use pseudonyms in my social network accounts
	(7) I will not visit websites with which I am not familiar
	(8) I will not make online transactions that require my personal information (e.g., online shopping, online banking, apply for credit card)
	(9) I will install better protection software on my computer
	(10) I will regularly clean and delete unnecessary documents, emails, and websites in my cache on my computer
	(11) I will use completely different password for each of my online accounts and change them regularly
	(12) I would be willing to pay for an identity theft protection service that notifies me of any requests for a new line of credit in my name

Risk Perception. An 8-item Likert scale about perceived risk of identity theft was included after scene 2 and scene 4; respondents indicated agreement on a 6-point scale from 1 (strongly disagree) to 6 (strongly agree).Factor analysis was also performed on eight items of risk perception for scene 2 and scene 4. Five items (item 3, 4, 5, 6, 8) were extracted as a factor when the number of factor was constrained to one. Cronbach's alpha = .81 and .83 for scene 2 and scene 4 respectively.

Short-term behavioral intention. Following scene 2, respondents were asked to check from ten items of actions they would intend to take if a suspicious credit card statement was received.

Long-term behavioral intention. A 12-item Likert scale about long-term intended behavior were included following scene 4; respondents indicated agreement on a 6-point scale from 1 (strongly disagree) to 6 (strongly agree).Nine (item 1, 2, 3, 4, 5, 8, 9, 11, 12) out of the twelve items were extracted as a factor when factor number was constrained to one. Cronbach's alpha = .84.

Table 6. Demographic Information and Cyber-related Experience (Experiment II)

Variables (N = 419)	Response category	Number and percentage
Have you ever had an account opened fraudulently in your name that you know of?	Yes	32 (7.6%)
	No	386 (92.1%)
Do you currently pay for an identity theft protection service (e.g. LifeLock, TrustedID, Equifax ID patrol)?	Yes	25 (6.0%)
	No	393 (93.8%)
Do you have a personal computer?	Windows	356 (85%)
	Mac	57 (13.6%)
	don't have	4 (1.0%)
Do you have a credit card?	more than one	169 (40.3%)
	only one	132 (31.5%)
	don't have	117 (27.9%)
Sex	male	233 (55.6%)
	female	103 (44.2%)
Education	less than high school	2 (.5%)
	high school	120 (28.6%)
	2-year college	89 (21.2%)
	4-year college	167 (39.9%)
	master's degree	34 (8.1%)
	PhD degree	6 (1.4%)
Personal annual gross income range before tax	below $20,000/year	131 (31.3%)
	$20,000 - $29,999/year	84 (20.0%)
	$30,000 - $39,999/year	54 (12.9%)
	$40,000 - $49,999/year	50 (11.9%)
	$50,000 - $59,999/year	30 (7.2%)
	$60,000 - $69,999/year	23 (5.5%)
	$70,000 - $79,999/year	19 (4.5%)
	$80,000 - $89,999/year	7 (1.7%)
	$90,000/year or more	20 (4.8%)
Age	range	18-114
	percentiles	25^{th} 24
		50^{th} 29
		75^{th} 39

3.1.3 Respondents

The experiment was hosted on Qualtrics.com and subjects were collected through AMT. Four hundred and twenty eight adult subjects participated in the experiment, and were compensated $0.75 for their time. Nine subjects were removed for not completing the experiment. Four hundred and nineteen subjects were included in the analysis. Table 6 presents demographic information for the sample.

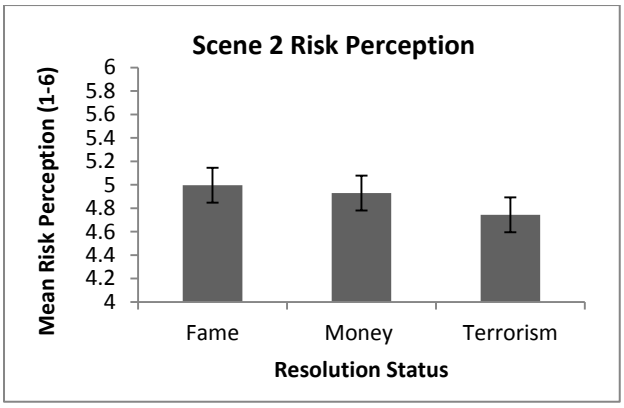
The number of respondents in each of the twelve conditions ranged from 29 to 41. Again, composite scores using equal weighting were calculated for three dependent variables: (1) negative affect, (2) risk perception, (3) long-term behavioral intention; scores for short-term behavior were calculated by counting the number of actions respondents checked from the eight items presented.

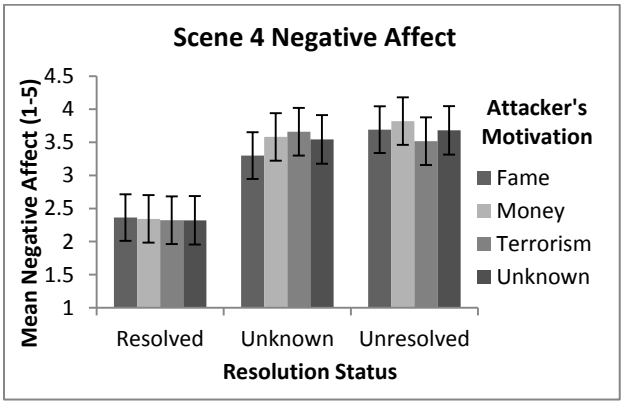
3.2 Results

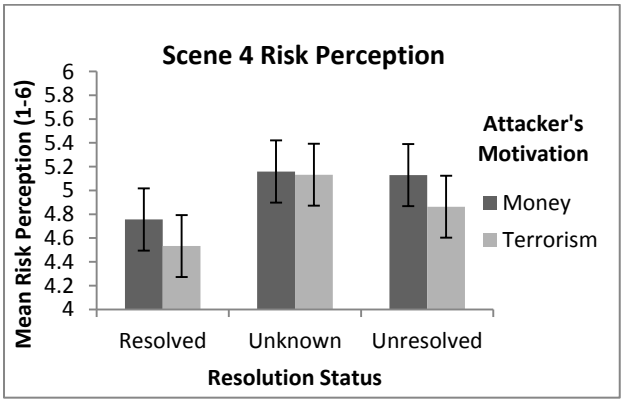
OLS regression analyses were conducted to predict the four dependent variables (affect, risk perception, short-term behavioral intentions, and long-term behavioral intention) from the two manipulated variables (the attacker's motivations---fame, money, terrorism or unknown and resolution status --- resolved, still at risk, or unknown), and respondents' sex. To examine the influence of the attacker's motivations, three orthogonal contrasts were created and entered the regressions as independent variables: (1) unknown vs. fame, money and terrorism, (2) terrorism vs. fame and money, (3) fame vs. money. To examine the influence of resolution status, the resolved condition was contrasted against the unresolved and unknown conditions.

Results indicate that following Scene 2 respondents perceived the risk of identity theft to be lower when the attacker's motivation was to fund terrorism compared to gaining money or fame (standardized $\beta = .109$, $t = 2.307$, $p = .022$, $R^2 = .084$). No significant difference was found between the motivations funding terrorism, personal financial gain, or fame for reported negative affect and short-term behavior following Scene 2. In addition, negative affect, perceived risk and short-term behavior were not significantly different between unknown vs. fame, money and terrorism and fame vs. money. Following Scene 4, respondents reported less negative affect at Scene 4 when the identity theft case was reported as resolved compared to unresolved or uncertain (standardized $\beta = .496$, $t = 11.463$, $p < .001$, $R^2 = .262$). It was also found that the perceived risk of identity theft was lower when the outcome of the scenario was reported as resolved compared to unresolved or uncertain (standardized $\beta = .104$, $t = 2.175$, $p = .030$, $R^2 = .076$). Following Scene 4, respondents were more willing to pursue long-term behavior change, such as discontinuing online transactions that require personal information or purchasing an identity theft protection service, when the outcome of the identity theft case was unresolved or uncertain compared to the resolved condition (standardized $\beta = .098$, $t = 1.984$, $p = .048$, $R^2 = .025$). Figure 2 displays the mean negative affect, perceived risk, and long-term behavioral intentions for different attacker motivations and the scenario resolution status following Scenes 2 and 4.

Lastly, results from the regression analyses indicate that sex significantly predicts perceived risk (standardized $\beta = .256$, $t = 5.370$, $p < .001$) and short-term behavioral intentions (standardized $\beta = .135$, $t = 2.714$, $p = .007$) following Scene 2, and negative affect (standardized $\beta = .124$, $t = 2.834$, $p = .005$), perceived risk (standardized $\beta = .238$, $t = 4.959$, $p < .001$), , and long-term behavioral intentions (standardized $\beta = .121$, $t = 2.435$, $p = .015$) following Scene 4. Overall, female respondents reported higher negative affect, more perceived risk, and a greater intention to seek help (short-term) and pursue online identity protection (long-term).







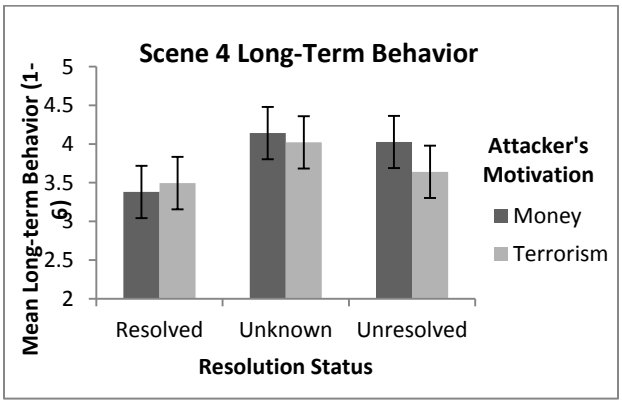


Figure 2. Mean risk perception, negative affect, and long-term behavior for attacker's motivation and resolution status. Note: Error bars are +/- 2 SE.

3.3 Discussion

Responses to a cyber-based identity theft attack in Experiment II were found to be significantly predicted by the attacker's motivations and the resolution status of the scenario. Consistent with our hypothesis, the closer and more personal the attacker's motivation was perceived to be, the greater the perceived risk of identity theft. In particular, respondents who were told the attacker's motivation was for personal financial gain interpreted the scenario as more realistic and familiar compared to the attacker who stole the respondent's identity to fund terrorism.

No difference in response was found across respondents who were told the attacker's motivations were for money, fame, or unknown. We suspect this might be a result of all three motivation types being driven by the same underlying means – money. That is, the theft of money is necessary to meet the desired end, whether the attack motivation is for personal gain, fame or an unknown reason. Furthermore, these three factors are perceived to be more personally motivated compared to the politically-driven motivation to fund terrorism (Brenner, 2007).

Following Scene 4 when scenario resolution status was manipulated, the findings suggest that lower levels of negative affect and perceived risk resulted from the resolved scenario compared to the unresolved and unknown scenarios. Consistent with our hypothesis, it is reasonable to assume that resolved outcomes create feelings of security for respondents and are less likely to induce any desire or need for behavioral change. This was reflected in responses by those in the resolved condition who following Scene 4 perceived the risk of identity theft to be lower as well as were less inclined to make behavioral changes that would protect their identity for the long-term.

We also found that respondents responded similarly to the unresolved and unknown outcome conditions. It is reasonable to expect that the level of uncertainty associated with the unresolved and unknown outcomes is perceived similarly, and for this reason respondents are more willing to engage in long-term behavioral change. Interestingly though, respondents indicated that on average they were only "somewhat willing to agree" to engage in long-term behavioral changes. This is consistent with recent poll results showing that the majority of U.S. adults (93 %) recognize identity theft is a growing problem, yet are failing to practice simple safeguards; e.g. more than half (55 %) of respondents indicated that they do not always check to see if a website is secure before shopping online, and more than three out of five respondents who had online accounts (63 %) do not use a unique password for each of their online accounts (PRNewswire, 2013).

Lastly, as in Experiment I, we found an anticipated sex effect, indicating that female respondents reported greater negative affect, greater perceived risk, greater intent to pursue short-term behavior and long-term behavior. This finding continues to be consistent with results showing that males have a greater tendency to engage in risky behaviors online (Milne et al., 2009) and females tend to demonstrate higher security procedure compliance (Herath and Rao, 2009).

Victims of identity theft are often in the position where they must take the initiative to address and manage the privacy breach. Services are available to support their needs, such as the police department referenced in the scenario, yet the process of resolution is largely self-motivated. As such, the policy implications of our findings provide potential insight into the type

of response to expect from identity theft victims, and how to communicate with such victims given awareness of the attacker motivation and attack resolution. More specifically, victims of attacks for which the outcome is uncertain and the attacker is motivated by financial gain are more likely to modify their behavior and seek out the support of identity theft-related social services. To the contrary, victims for which the attacker motivation is more distant (not financially driven) and the attack outcome is resolved, additional effort by the social service providers, and in turn additional money, will likely be needed to generate the desired behavioral response for managing the ongoing risks of identity theft. Again, findings suggest that females have the potential to be more inclined to support policy recommendations, yet additional research is needed to fully understand the moderating effects of demographic variables.

4. CONCLUSIONS

These experiments were designed to explore how individual computer users' responses to common cyber-based financial fraud and identity theft scenarios are influenced by attacker characteristics and attack mode (Experiment I) and attacker motivation and attack resolution status (Experiment II). The same response constructs were used in both studies, but were defined slightly differently given variations in the scenario contexts.

Both of these experiments utilized a scenario simulation methodology and an experimental manipulation design with concrete, realistic stimulus materials to explore respondents' predictions about their feelings, perceived risk and behavioral intentions to respond to the simulated financial fraud and identity theft attacks. As suggested by construal theory (Trope & Liberman, 2003, 2010; Trope, Liberman, & Wakslak, 2007), it is hard for people to assess their reactions when the context is more distant and unobservable. While surveys and focus groups are useful, one of their limitations is the reliance on cognition in the absence of any attention to affect (Slovic et al., 1994). The scenario simulation methodology is designed to present scenarios that are both believable and effective in evoking emotional responses from respondents.

Across the two experiments, results indicate that attacker characteristics and attack mode (Experiment I) and attacker motivations (Experiment II), influenced the perception of vulnerability of respondents to the financial fraud and identity theft scenarios. In Experiment I, the pictorial identification of the attacker resulted in more proximal and concrete interpretations of the attacker characteristics, resulting in lower negative affect. In Experiment II the more concrete and "real" attacker motivations were associated with higher perceived risk. Interestingly, the use of pictures in the characterization of the manipulated variables changed the direction of the reaction to the cyber attack.

Studies of cyber security have shown that management of affective reactions and perceived risk strongly influence individual users' decisions. For example, individual users experiencing lower perceived risk were more likely to purchase a product online; likewise, users feeling greater negative affect were less likely to sign-up for online banking services (Kim, Ferrin & Rao, 2008; Lee, 2009). This result is consistent with our experimental findings, suggesting that when respondents felt that they were vulnerable, they responded with heightened behavioral response. More specifically, in Experiment I all respondents felt some level of vulnerability in response to the cyber-based bank hacking scenario and for this reason had an expectation that the bank would take action to mitigate the consequences of the attack. The respondents' behavioral intentions following the attack varied as a function of the manipulated characteristics of the simulated financial fraud attack scenario. Similarly, in Experiment II, respondents recognized the perceived risk associated with identity theft and expressed a willingness to engage in long-term behavior change. Again, the degree of intended behavior change varied relative to the resolution status indicated in the simulated identity theft scenario.

There is limited research on the influence of attacker attributes on individual user decision making. The scenario simulation approach used in our experiments presents a more emotionally evocative and realistic method for assessing individual reactions and decision making compared to traditional descriptive survey studies and post-hoc field studies. However, given the global reliance and dependence on the internet and the frequency with which cyber attacks occur, a study of actual victims emotional reactions, perceived risk and decision making following a real attack would be an important next research step.

In addition, more studies are needed to further understand whether the identified relationships are generalizable to other cyber threat scenarios. Given that safety and security in the cyber context are abstract concepts, it would be worthwhile to further explore how attacker attributes influence reactions and decision making in response to cyber attacks. This research design also could be used to evaluate differences across a varied set of cyber-based attacks to examine the robustness of the relationships identified in our research. Lastly, future studies could also be designed to specifically address policies designed to assess privacy preferences given attacker attributes. This experimental design would be more directed at studying specific policy tools and educational approaches for addressing the cyber threat in the present, similar to work reported 15 years ago by Ackerman, Cranor and Reagle (1999).

5. ACKNOWLEDGEMENTS

This research was supported by the National Science Foundation under grant number SES-1314644. It was also supported by the U. S. Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events under the cooperative agreement number 2010-ST-061-RE0001. However, any opinions, findings, conclusions, and recommendations in this document are those of the author and do not necessarily reflect views of the National Science Foundation or the U. S. Department of Homeland Security. We would like to thank Lauren Ladd-Reinfrank for her support in the planning and execution of Experiment I.

6. REFERENCES

[1] Ackerman, M.S., Cranor, L.F., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. *EC '99 Proceedings of the 1st ACM Conference on Electronic Commerce,* 1-8.

[2] Bhatnagar, A., Misra, S., & Rao, H. R. (2000). On risk, convenience, and Internet shopping behavior. *Communications of the ACM, 43*(11), 98-105.

[3] Bourque, L. B., Regan, R., Kelley, M. M., Wood, M. M., Kano, M., & Mileti, D. S. (2013). An examination of the effect of perceived risk on preparedness behavior. *Environment and Behavior, 45*(5), 615-649.

[4] Brenner, S. W. (2007). " At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare. *The Journal of Criminal Law and Criminology*, 379-475.

[5] Cameron, L., & Shah, M. (2013). Risk-taking behavior in the wake of natural disasters. *National Bureau of Economic Research*.

[6] D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. *Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting.*

[7] Fischhoff, B., Gonzalez, R. M., Small, D. A., & Lerner, J. S. (2003). Judged terror risk and proximity to the World Trade Center *The Risks of Terrorism* (pp. 39-53): Springer.

[8] Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research, 57*(7), 768-775.

[9] Hale, C. (1996). Fear of crime: A review of the literature. *International Review of Victimology, 4*(2), 79-150.

[10] Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization. *Journal of Contemporary Criminal Justice, 29*(4), 475-497.

[11] Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

[12] Ho, M. C., Shaw, D., Lin, S., & Chiu, Y. C. (2008). How do disaster characteristics influence risk perception? *Risk Analysis, 28*(3), 635-643.

[13] Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544-564.

[14] Kung, Y. W., & Chen, S. H. (2012). Perception of earthquake risk in Taiwan: Effects of gender and past earthquake experience. *Risk Analysis, 32*(9), 1535-1546.

[15] Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications, 8*(3), 130-141.

[16] Leiserowitz, A. (2006). Climate change risk perception and policy preferences: the role of affect, imagery, and values. *Climatic Change, 77*(1-2), 45-72.

[17] Liu, L., Yu, E., & Mylopoulos, J. (2003). Security and privacy requirements analysis within a social setting. *Paper presented at the Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International.*

[18] Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43*(3), 449-473.

[19] Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *American Journal of Community Psychology, 41*(1-2), 127-150.

[20] Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Digital Investigation, 2*(4), 261-267.

[21] Peters, E., & Slovic, P. (1996). The role of affect and worldviews as orienting dispositions in the perception and acceptance of nuclear Power1. *Journal of Applied Social Psychology, 26*(16), 1427-1453.

[22] PRNewswire. (2013). Many consumers fear identity theft yet still engage in risky behavior. Available online at http://www.prnewswire.com/news-releases/many-consumers-fear-identity-theft-yet-still-engage-in-risky-behavior-228595151.html.

[23] Reponses, P., Model, A. N., & Westbrook, L. (2012). Private crises/public reponses: A nascent model. *Proceedings of the American Society for Information Science and Technology, 49*(1), 1-12.

[24] Rosoff, H., Cui, J., & John, R. S. (2013). Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions, 33*(4), 517-529.

[25] Rosoff, H., Siko, R., John, R., & Burns, W. J. (2013). Should I stay or should I go? An experimental study of health and economic government policies following a severe biological agent release. *Environment Systems & Decisions*, 1-17.

[26] Sjøberg, S., & Schreiner, C. (2005). *Young people and science.* Paper presented at the Attitudes, values and priorities. Evidence from the ROSE project. Keynote presentation at EU's Science and Society Forum.

[27] Skogan, W. G., & Maxfield, M. G. (1981). *Coping with crime: Individual and neighborhood reactions*: Sage Publications Beverly Hills, CA.

[28] Slovic, P. (1987). Perception of risk. *Science, 236*(4799), 280-285.

[29] Slovic, P., Fischhoff, B., Lichtenstein, S., & MacGregor, D. (2004). Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality. *Risk Analysis, 24* (2), 311-322.

[30] Slovic, P., Fischhoff, B., & Lichtenstein, S. (1980). Facts and fears: Understanding perceived risk. *Societal Risk Assessment* (pp. 181-216): Springer.

[31] Slovic, P., Fischhoff, B., & Lichtenstein, S. (1984). Behavioral decision theory perspectives on risk and safety. *Acta Psychologica, 56*(1), 183-203.

[32] Terpstra, T. (2011). Emotions, trust, and perceived risk: Affective and cognitive routes to flood preparedness behavior. *Risk Analysis, 31*(10), 1658-1675.

[33] Trope, Y., & Liberman, N. (2003). Temporal construal. *Psychological Review, 110*(3), 403.

[34] Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review, 117*(2), 440.

[35] Trope, Y., Liberman, N., & Wakslak, C. (2007). Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior. *Journal of Consumer*

Psychology: The Official Journal of the Society for Consumer Psychology, 17(2), 83.

[36] Vlek, C., & Stallen, P.-J. (1980). Rational and personal aspects of risk. *Acta Psychologica, 45*(1), 273-300.

[37] Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: the PANAS scales. *Journal of Personality and Social Psychology, 54*(6), 1063.