San Jose State University
SJSU ScholarWorks

Master's Theses | Master's Theses and Graduate Research

Spring 2016

# Trust and Complacency in Cyber Security

Ashley Allison Cain
*San Jose State University*

Follow this and additional works at: https://scholarworks.sjsu.edu/etd_theses

Recommended Citation
Cain, Ashley Allison, "Trust and Complacency in Cyber Security" (2016). *Master's Theses*. 4679.
DOI: https://doi.org/10.31979/etd.a4nf-q57u
https://scholarworks.sjsu.edu/etd_theses/4679

This Thesis is brought to you for free and open access by the Master's Theses and Graduate Research at SJSU ScholarWorks. It has been accepted for inclusion in Master's Theses by an authorized administrator of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.

# TRUST AND COMPLACENCY IN CYBER SECURITY

A Thesis

Presented to

The Faculty of the Department of Psychology

San José State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

by

Ashley Cain

May 2016

© 2016

Ashley Cain

ALL RIGHTS RESERVED

The Designated Thesis Committee Approves the Thesis Titled

TRUST AND COMPLACENCY IN CYBER SECURITY

by

Ashley Cain

APPROVED FOR THE DEPARTMENT OF PSYCHOLOGY

SAN JOSÉ STATE UNIVERSITY

May 2016

| | |
|---|---|
| Dr. David Schuster | Department of Psychology |
| Dr. Sean Laraway | Department of Psychology |
| Dr. Clifton Oyamot | Department of Psychology |

ABSTRACT

TRUST AND COMPLACENCY IN CYBER SECURITY

by Ashley Cain

Improved understanding of conditions that foster appropriate use of security tools by cyber security professionals is crucial for protecting companies from financial losses. Trust has been an important topic in the literature because of its role in allowing for cooperation among humans and automation and because of its relationship with appropriate use. The current study aimed to extend the finding that high trust leads to complacency in the domain of cyber security and to clarify a discrepancy in the literature about complacency's operationalization by measuring information sampling behaviors directly. The sample consisted of 101 first year psychology students. The independent variable was the reliability of an intrusion detection system (IDS), and complacency and self-report trust were dependent measures. Trust was measured by a self-report questionnaire (Jian et al., 2000). Complacency was measured by reverse coding the number of clicks used to drill down for information in log files in a simulated IDS. Information sampling behavior provides a more direct and accurate measure of complacency than previously used performance measures. It was hypothesized that when supervising an IDS, high reliability of the IDS would lead to complacency, and trust with automation would mediate this relationship. Although reliability was found to predict both trust and complacency, the mediation was not supported. Results suggest new considerations in measuring trust in laboratory and field settings.

TABLE OF CONTENTS

List of Tables ..... viii

List of Figures ..... ix

Introduction ..... 1

Statement of the Problem ..... 1

Trust in Automation ..... 2

Trust and Complacency ..... 3

Existing Approaches ..... 5

Deficiencies in Past Literature ..... 7

Research Needs Addressed by the Current Study ..... 8

Purpose of the Current Study ..... 9

Hypothesis 1 ..... 9

Hypothesis 2 ..... 9

Hypothesis 3 ..... 9

Method ..... 10

Participants ..... 10

Materials ..... 10

Measures ..... 12

Baseline for Trust ..... 12

Trust ..... 12

Complacency ..... 12

Performance ..... 13
Workload ..... 13
Boredom ..... 13
Demographic Questionnaire ..... 13
Procedure ..... 14
Results ..... 155
Test of Mediation Model ..... 16
Test of Moderated Model ..... 21
Effects on Performance ..... 22
Discussion ..... 23
Conclusion ..... 26
References ..... 28
Appendix A ..... 34
Consent Form ..... 34
Appendix B ..... 38
Automation-Induced "Complacency" Scale ..... 38
Appendix C ..... 39
Checklist for Trust Between Humans and Automation ..... 39
Appendix D ..... 41
Demographic Questionnaire ..... 41
Appendix E ..... 42

Boredom Measure....42
Appendix F....43
NASA-TLX....43
Appendix G....44
IRB Approval....44

LIST OF TABLES

1. Descriptive Statistics for Reliability on Trust (Subjective Ratings) and on Complacency (Reverse Coded Number of Clicks) ……..……18

2. Pearson Correlation Results ……19

3. Regression Results for Moderation Test ……..22

LIST OF FIGURES

1. Trust as a Mediator ……10

2. List of Log Files …… 11

3. Histograms of Measures ……..…. 20

4. Trust and complacency plots …… 20

5. Mediation Results ……..…… 21

# Introduction

## Statement of the Problem

Data breaches at 54 midsize US companies cost an average of 5.4 million dollars over a ten month period in 2013 ("2013 cost of data," 2013). In 2014, Target alone spent one billion dollars in response to a breach of security (Johnson, 2014) in which hackers shared 110 million customers' debit and credit card numbers (Sheridan, 2014). In May of 2014, security experts solved a crisis caused by Gameover Zeus, which infected 200,000 computers and stole 100 million dollars from individuals and large and small businesses (Grossman, 2014).

In order to prevent costly attacks, we depend on timely and accurate decision-making by human operators. Decisions are supported by information provided by automation, but ultimately human operators make the final choices when identifying and responding to attacks. When cyber security experts working with security software such as intrusion detection systems (IDS) successfully prevent attacks, organizations save directly by preventing loss of integrity, confidentiality, and availability, as well as indirectly by preventing future attacks that breach the system through the same vulnerability (Iheagwara, Blyth, Kevin, & Kinn, 2004). Improved understanding of conditions that foster appropriate operators' use of security software, including IDSs, is crucial for protecting companies from financial losses.

IDSs function similarly to burglar alarms, with the purpose of preventing security breaches. They compare the log files of events in the network with "normal events," and produce alerts when anomalies are detected. An IDS produces alerts but does not prevent

breaches without the attention, knowledge, and skills of a human operator. The human must oversee the IDS in a supervisory role and periodically must manually check log files to determine if anomalies identified by the IDS constitute threats.

**Trust in automation.** Trust has been an important topic in the literature because of its role in allowing for cooperation among humans and automation (Lee & See, 2002; Parasuraman & Riley, 1997), such as IDSs (Cain & Schuster, 2014), and because of its relationship with appropriate use (de Vries, Midden, & Bouwhuis, 2003; Dzindolet, Peterson, Pomranky, Pierce, & Beck, 2003; Lee & Moray, 1994; Riley, 1994). In the literature, researchers have postulated disparate definitions of trust, although it is generally agreed among researchers that trust is an affective and motivational psychological state (Bromiley & Cummings, 1996; Kramer, 1996; Lewis & Weigert, 1985; McAllister, 1995; Tyler & Degoey, 1996). Commonly, trust is interpreted as an intention to act and become vulnerable (Johns, 1996; Mayor, Davis, & Schoorman, 1995; Moorman, Deshpande, & Zaltman, 1993). Elaborating on this definition, trust has also been defined as the result of uncertainty that makes one vulnerable (Deutsch, 1960; Kramer, 1999; Meyer, 2001). Finally, researchers define trust as an expectation of beneficial outcomes (Barber, 1983; Rotter, 1967; Rempel, Holmes, & Zanna, 1985). Specifically, trust with automation has been defined as "the attitude that an agent [automation] will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability" (Lee & See, 2004). Synthesizing the elements of uncertainty and benefits from these definitions, the rational perspective provides a useful definition of trust (Hardin, 1992). It explains that trust is a rational choice made in

uncertain circumstances that aims to increase benefits and decrease costs; the trustor makes a decision that the trustee will act towards their benefit, or at least will not hinder their progress towards a goal.

This perspective provides a useful framework for understanding trust, especially in work-related relationships (as between humans and automation). However, it overstates our abilities to make cost/benefit calculations in uncertain situations (Crossman, 1974; Klein, 1989; Kramer 1999). While trust aims to increase benefits and decrease losses in uncertain interactions (Hardin, 1992), inappropriate trust that results in misuse (overutilizing faulty automation) or disuse (underutilizing capable automation) can occur due to humans' limited abilities to make cost benefit calculations (Crossman, 1974; Klein, 1989; Kramer, 1999). While trust precedes use of automation (de Vries et al., 2003; Dzindolet et al., 2003; Lee & Moray, 1994; Riley, 1994) and thereby aids collaboration and supports performance, sometimes the decision to trust a human or automated teammate can be inappropriate for the situation.

**Trust and complacency.** Complacency, the "insufficient monitoring and checking of automation functions" (Manzey, Bahner, & Hueper, 2006, p. 59), is a subcategory of misuse (over-relying on faulty automation; Manzey, Bahner, & Hueper, 2006). The avoidance of complacency is another precondition for appropriate use of automation (Bagheri & Jamieson, 2004; Bahner, Hüper, & Manzey, 2008; Muir, 1987) such as IDSs, which inevitably miss some attacks in order to avoid overly frequent false alarms. When human operators complacently oversee automation, they are less prepared

to manually take control when their intervention is needed. Complacency may be related to the development of inappropriate trust.

Because IDSs are a form of automation, research about interactions with this software can be informed by research about other forms of automation. Previous research has identified inappropriate trust, misuse, and complacency as issues in other supervisory tasks, including aircraft (Billings, 1991) and ships (Dekker & Lutzhoft, 2004; Parasuraman & Miller, 2004). Similar to overseeing an IDS, these other tasks require high vigilance while the human operator processes many environmental cues in a frequently passive role. It has not been experimentally verified that inappropriate trust and misuse lead to complacency when supervising IDSs, but it is likely that they do due to the monotonousness yet high workload that is common to supervisory roles that are at risk for complacency (Prinzel III, DeVries, Freeman, & Mikulka, 2001).

Cyber security experts are certainly trained to be analytical, skeptical, and vigilant. However, in reference to security software vendors and system administrators, Risto Siilasmaa, the founder, chairman, and former CEO of F-Secure stated that "the danger provided by viruses is in direct proportion to the complacency that seems so prevalent today" (Armstrong, 2001, cited in Arief and Besnard, 2003, p. 11). When working with process control and supervisory control and data acquisition systems, security experts have been described as complacent and implicated for "letting hackers take advantage of the control industry's ignorance" (Byres & Lowe, 2004, p. 1).

However, cyber security experts should not necessarily be blamed for missing threats, as task factors make poor human performance likely. According to the

conditions that encourage complacency, including monotony or boredom and high workload during a supervisory task (Prinzel III et al., 2001), overseeing IDSs and checking log files in a large database is another cyber security context in which administrators are at risk of complacency. Monotony and high workload are two preconditions for complacency that put human operators of IDSs in cyber security at particularly high risk of complacency, but complacency might not be an inevitable problem unless a third precondition also occurs. Without the presence of trust as a mediator, high workload and monotonous supervisory roles may not necessarily lead to complacency (Bagheri & Jamieson, 2004). High operator trust may be a crucial predictor of complacency in the context of IDSs.

**Existing Approaches**

Inappropriate trust and subsequent miscalibrated reliance hinder performance in human-automation teams (Dzindolet et al., 2003). When human operators are complacent, misuse is more likely to occur, and performance suffers due to over-reliance on imperfect automation (Bagheri & Jamieson, 2004; Bahner et al., 2008; Parasuraman, Molloy, & Singh, 1993; Prinzel III et al., 2001). Early studies about complacency operationalized the construct based on its effect on performance by measuring the human's detection of errors in the automation (Bailey & Scerbo, 2007; Parasuraman et al., 1993). In order to measure complacency more precisely and differentiate it from performance, researchers have operationalized complacency as insufficient information sampling behaviors (Bagheri & Jamieson, 2004; Bahner et al., 2008; Manzey et al, 2006). Researchers have measured complacency as the time between eye fixations (Bagheri &

Jamieson, 2004) and mouse clicks and keystrokes (Bahner et al., 2008). While complacency has been measured directly and indirectly, previous research showed that complacency is an issue in tracking, system-monitoring, fuel-management, and air-quality tasks in planes and spacecraft, because these are supervisory tasks in which the human departs from a manual role (Bagheri & Jamieson, 2004; Bahner et al., 2008; Bailey & Scerbo, 2007; Parasuraman et al., 1993; Prinzel III et al., 2001).

There is tenuous support for trust's effect on complacency (Bagheri & Jamieson, 2004; Singh, Molloy, & Parasuraman, 1993). However, it is evident that trust affects use of automation in general, such as operators' decisions to rely on it (de Vries et al., 2003; Lee & Moray, 1992, 1994; Riley, 1994; Dzindolet et al., 2003). In industrial semi-automatic control, perceptual classification and decision, and route planning tasks, humans are more likely to agree with decisions made by the automation when trust is high. Because it facilitates collaboration, such as between humans and automation, trust is inherently adaptive. However, when trust is miscalibrated, it becomes problematic. It can lead to misuse when operators' trust is high and they continue to rely on faulty automation (Lee & See, 2002; Parasuraman & Riley, 1997), especially under conditions of high workload (Parasuraman & Riley, 1997). Misuse results in deficient monitoring behaviors and decision biases (Parasuraman & Riley, 1997), which manifest as errors of omission and commission; human operators might ignore problems that the automation does not alert them to (omission) or might accept notifications from the automation without cross-checking them with the available information (commission; Mosier & Skitka, 1996). Complacency describes this deficient monitoring and is a specific type of

misuse (Manzey et al., 2006, p. 59). Complacency is a precise construct that fits within the broader umbrella of misuse. Complacency has been shown to be related to trust in two studies, which include the contexts of everyday use of automation, such as when using ATMs, shopping online (Singh, Molloy, & Parasuraman, 1993), and flying simulated aircraft (Bagheri & Jamieson, 2004); trust predicts self-report of complacent attitudes (Singh et al., 1993) and is related to less information sampling behavior (Bagheri & Jamieson, 2004).

**Deficiencies in Past Literature**

Although complacency has been shown to be an issue in other contexts in which humans adopt a supervisory role, complacency has not been studied in the context of cyber security, except for on the part of the end user; end users tend to be weak links in security processes due to complacency issues (Sasse, Brostoff, & Weirich, 2001). Given the substantial research showing problems associated with complacency, it is likely to be an issue in the use of IDSs. However, trust may mediate this relationship. Research has repeatedly shown that trust affects humans' reliance on general automation. However, there is limited research on trust's effect on complacency, which may be the intermediary through which trust hinders reliance. Researchers have linked trust and complacency without providing empirical support for the relationship (Bahner et al., 2008; Danaher, 1980; Endsley, 1996; Inagaki, Furukawa, & Itoh, 2005; Moray & Inagaki, 2000; Parasuraman & Manzey, 2010; Parasuraman & Miller, 2004; Wiener, 1985; Prinzel III et al., 2001). Four studies have provided evidence that trust is a predictor of complacency in contexts outside of cyber security (Bailey & Scerbo, 2007; Ho, Wheatley, & Scialfa,

2005; Singh, Molloy, & Parasuraman, 1993), but only one of these studies used objective measures of information sampling (Bagheri & Jamieson, 2004). No studies have empirically tested the relationship between trust and complacency in the context of cyber security. Possibly, when cyber security operators' trust levels are high, there would be fewer information sampling behaviors as well, which would reflect increased complacency in this condition.

**Research Needs Addressed by the Current Study**

The current experiment addresses a deficiency of empirical evidence about trust's relationship with complacency, as measured by information sampling behavior. The study validates findings that high trust relates to complacency and extends them to the domain of cyber security. The hypothesis was that a lack of information sampling behavior when operating IDSs would correspond to higher self-report of trust. Observing trust as a possible antecedent of complacency will help to increase understanding about the processes that lead to security breaches and the loss of information or confidentiality at organizations. Identifying whether trust levels correlate with complacency will provide guidance for procedure and design; if trust, based on reliability, affects complacency, then IDSs should be designed in such a way and procedures should be implemented that interrupt this causal sequence. Human operators may become complacent when working with a reliable IDS; however, the solution may likely not be to lower reliability. Instead, we may be able to have high reliability and low complacency if we implement designs and procedures that calibrate trust.

**Purpose of the Current Study**

In the context of cyber security, for the purpose of avoiding errors, professionals may benefit from a certain amount of distrust, inasmuch as it decreases complacency. Too much trust leads to misuse, while too little leads to disuse. To explore the possibility that operators can avoid complacency by developing appropriate, moderate trust levels, participants received a brief training and then interacted with simulated IDSs. Participants received warnings from the IDSs, with varying levels of reliability, which required them to decide to block or allow someone who is attempting to access the network. They could best make these decisions by examining the log files to determine if the log files are suspicious. The researcher measured trust using a subjective questionnaire, and she measured complacency by the number of keystrokes and mouse clicks involved in information sampling from the log files. It was hypothesized that appropriate trust would help operators avoid misuse and complacency. While reliable automation may lead to complacency, this causal relationship may be mediated by trust. The researcher aimed to establish this mediation through three hypothesis tests.

**Hypothesis 1.** Automation reliability predicts trust such that higher reliability leads to higher trust.

**Hypothesis 2.** Reliability predicts complacency such that higher reliability leads to more complacency.

**Hypothesis 3.** Trust mediates the relationship between reliability and complacency (See figure 1).

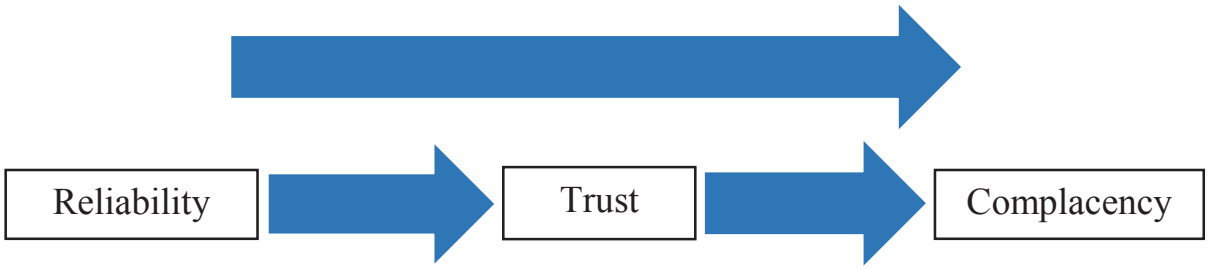


*Figure 1*. Trust as a mediator

## Method

### Participants

A power analysis using a medium effect size of .15 according to Cohen revealed a sample size of 64 per group. Participants were selected from the subject pool of first year psychology students and were compensated with class credit. There were 59 women and 42 men. Ages ranged from 18 to 31 ($M$ = 19.31, $SD$ = 2.35). All of the participants had normal or corrected-to-normal vision. None of the participants reported prior experience with IDSs.

### Materials

The experiment was run using a Python script, a Python created graphic user interface, and a low fidelity IDS. A list of log files was displayed on a desktop computer (See figure 2). The Python script recorded the total number of clicks that participants used to drill down for security-related information about each log file. The IDS was composed of a list of alerts that were printed on paper for convenience. In the two conditions, the IDS was 97.25% or 60% reliable with a base rate of anomalous log events

that was 13% of the total log events, meaning that the IDS failed to identify anomalous log events either 2.75% or 40% of the time. The researcher selected these reliability levels because 60% reliability is the lowest level of reliability at which automation is still useful (Wickens & Dixon, 2007), and 97.25% reliability represents a high reliability level while accounting for the fact that automation is imperfect. The researcher manipulated sensitivity while holding the criterion constant, so $d' = .88$ for the high reliability and $d' = .57$ for the low reliability condition; criterion $c = 1.65$ for both conditions. The two levels of reliability constitute the independent variable, which was manipulated between subjects.

*Figure 2.* List of log events. Highlighted logs have been clicked.

## Measures

**Baseline for trust.** The dimension of trust from Singh and colleague's Automation-Induced "Complacency" scale (1993) was used to establish a baseline for trust with general automation. This dimension includes three weighted items, which were assessed with a five-point Likert scale. For example, participants reported their degree of agreement with the statement "Bank transactions have become safer with the introduction of computer technology for the transfer of funds." One indicated "not at all," and five indicated "extremely." The researcher summed responses to create a baseline trust score. This measure of trust was included as a possible covariate with the final trust measure.

**Trust.** The experiment used Jian, Bisantz, and Drury's (2000) empirically derived trust scale to measure the construct of trust between humans and automation. The trust scale was developed based on the results of three studies exploring trust and distrust in a word elicitation task, a questionnaire, and a paired comparison task. This measure had twelve total items, each with a seven-point Likert type scale. One indicated "not at all," and seven indicated "extremely." A sample question from the scale is, "The system has integrity" (Jian et al., 2000).

**Complacency.** Complacency was measured by participants' information sampling behaviors from the list of log files. Clicking on each log file opened a small window that contained more information about each event. The Python script counted the total number of clicks a participant made in the list of log files, and the total clicks were reverse coded to compose a measure of complacency.

**Performance.** Performance was measures as *d'*, the participants' sensitivity for detecting attacks. This measure was computed by subtracting z of false alarms from z of hits.

**Workload.** To check that workload was high when using the IDS, the researcher measured workload using the NASA-TLX (task load index; Hart & Staveland, 1988). This questionnaire measures workload as a subjective experience rather than as an objective outcome of the demands of the task. Participants were instructed to place a mark on the line to represent the magnitude of each of the six items, for example mental demand. Lines reflected opinions of "low" to "high" or "good" to "poor."

**Boredom.** As a measure of boredom experience in monotonous situations, the researcher used Drory's (1982) questionnaire for boredom, which was designed for the context of truck driving but can be adapted to cyber security supervisory tasks. The scale consists of six items. Participants put a check next to any item with which they agreed. As a whole, Drory found the items accounted for 83% of variance in boredom, thereby providing evidence of validity. The scale was also found to be reliable, with a Cronbach's alpha coefficient of .86. Examples of items include, "Feeling bored," "Feeling of monotony," and "Feeling that time goes very slowly."

**Demographic Questionnaire.** The researcher included a demographic questionnaire to gain an understanding of characteristics in the sample. Basic demographic questions were included about age, gender, and English fluency (whether English is their first language). Participants were also asked if they had normal or corrected-to-normal vision, which was a requirement for the study.

**Procedure**

Participants from Introduction to Psychology courses signed up for the study through SONA. After reviewing and signing consent forms and completing a demographic questionnaire, participants filled out the trust questionnaire to establish a baseline for trust with automation (Singh et al., 1993). Next, participants had a brief training about identifying anomalies in log files and how to use the IDS. The training slides also conveyed the level of reliability participants could expect from the automation, for example, "Your IDS attack alerts are 60% reliable… If you rely on the IDS alerts only, you will correctly identify 387 attacks but will miss 39 attacks." Then they interacted with a low fidelity IDS. Throughout the trials, software recorded the frequency of participants' mouse clicks and keyboard strokes that allowed participants to drill down for security-related information about log files. Participants wrote a list of every attack they detected in the network with or without the aid of the IDS. This was a signal detection task. Participants either detected a signal (an attack) or did not detect a signal. Responses were coded as hits (correctly identifying an attack), misses (not detecting an attack that was present), false alarms (detecting an attack that was not present), or correct rejections (not detecting an attack that was not present). Lastly, participants filled out questionnaires about their level of trust based on their experience with the automation (Jian et al., 2000), workload (Hart & Staveland, 1988), and boredom (Drory, 1982). The researcher measured workload and boredom, because they have been shown to covary with complacency (Prinzel III et al., 2001).

## Results

A series of multiple regression analyses was used to determine if trust mediated the relationship between reliability and complacency. Descriptive statistics are presented in Table 1. Higher trust scores indicated more trust. The number of clicks were reverse scored to compose complacency, because more information sampling translated to less complacency. The number of clicks was subtracted from 1000 (e.g., 50 clicks would compose a high complacency score of 950). Examination of histograms for trust ratings and number of clicks showed that the assumption of normality was met for trust for high and low reliability conditions, and the assumption was met for complacency for the low reliability condition. Because the histogram did not fit a normal bell curve and was negatively skewed (ratio of skew and standard error = -2.36), the assumption of normality was not met for complacency at high reliability due to the nature of the experiment; there is a floor to the amount of information that a participant cannot sample (See figure 3 for histograms of measures). There were no significant correlations among baseline trust, boredom, workload, trust, and performance. See Table 2 for correlation matrix. Random assignment was verified by a t-test comparing scores on baseline trust between the two reliability condition. Non-significance indicated that the groups were randomly assigned ($t(98) = 0.22$, $p = .827$, $d = .05$). Boredom scores indicated that there were not significant differences in motivation between the conditions ($F(1, 98) = 1.39$, $p = .241$, partial $\eta^2 =$ 014). There was high internal reliability among individual trust items on Jian et al.'s (2002) trust questionnaire, Cronbach's $\alpha = .91$. Cronbach's $\alpha$ for the baseline trust

measure was .05, for the workload measure was .66, and for the boredom measure was .50.

**Test of Mediation Model**

Following the procedure described by Baron and Kenney (1968), the mediation was tested using a hierarchical regression within three steps. The baseline trust measure was not included as a covariate, because it did not correlate with the dependent variable trust scores. Hypothesis one was that reliability would predict trust. In the first step of the regression, reliability was a significant predictor of trust, predicting 7% of the variance, $R^2 = .08$, $R^2_{adjusted} = .07$, $F(1, 98) = 0.84$, $p = .005$. The standardized coefficient for reliability was $\beta = -.28$, $t(98) = -2.89$, $p = .005$. The direction of this finding was counterintuitive and contrary to previous literature, with high reliability leading to low trust. Hypothesis two was that reliability would predict complacency. In the second regression model, reliability significantly predicted 21% of the variance in complacency, $R^2_{adjusted} = .21$, $F(1, 98) = 26.73$, $p < .001$. The standardized Beta coefficient for reliability was $\beta = .46$, $t(98) = 5.17$, $p < .001$. When reliability was high, trust was low, and complacency was high. Hypothesis three was that reliability's effect on complacency would diminish when trust was entered into the analysis. In the third step, both reliability and trust were included as predictors of complacency and significantly predicted 22% of the variance, $R^2 = .22$, $R^2_{adjusted} = .21$, $F(2, 97) = 13.56$, $p < .001$. The standardized Beta coefficient for reliability was $\beta = .44$, $t = 4.75(97)$, $p < .001$, and the coefficient for trust was $\beta = -.07$, $t = -0.73(97)$, $p < .469$. Reliability's predictive strength did not decrease when trust was considered, $\Delta R^2 = .01$, $F(1, 97) = 1.37$, $p = .245$. By

comparing the significance of the direct effect (reliability predicting complacency) and the indirect effect (reliability predicting trust, and trust predicting complacency), a SOBEL test (Sobel, 1982) confirmed that the mediation was not supported, $p = .481$. Overall, this finding did not provide support for the existence of a mediated relationship.

Table 1

*Descriptive Statistics for Reliability on Trust (Subjective Ratings) and on Complacency (Reverse Coded Number of Clicks)*

| Variable | | *n* | *M* | *SD* | *Range* | *Empirical Range* | α |
|---|---|---|---|---|---|---|---|
| Low Reliability | Trust | 51 | 18.78 | 6.81 | 0-84 | 5-35 | .86 |
| | Complacency | 51 | 602.86 | 196.08 | 0-1000 | 96-889 | |
| | Trust Baseline | 50 | 9.3 | 2.26 | 0-15 | 0-13 | .26 |
| | Performance | 51 | .33 | 1.22 | | -1.38-.25 | |
| | Workload | 51 | 18.71 | 5.64 | 0-42 | 8-31 | .64 |
| | Boredom | 51 | 2.39 | 1.73 | 0-6 | 0-6 | .56 |
| High Reliability | Trust | 49 | 14.31 | 6.56 | 0-84 | 5-30 | .92 |
| | Complacency | 50 | 811.74 | 201.54 | 0-1000 | 120-974 | |
| | Trust Baseline | 49 | 9.02 | 1.76 | 1-15 | 4-12 | -.31 |
| | Performance | 49 | 0.71 | 1.35 | | -2.31-2.25 | |
| | Workload | 49 | 19.17 | 5.17 | 1-42 | 0-33 | .68 |
| | Boredom | 49 | 2.02 | 1.39 | 0-6 | 0-4 | .41 |

Table 2

*Pearson Correlation Results*

| Variable | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1. Baseline Trust | --- | | | | | |
| 2. Trust | .13 | --- | | | | |
| 3. Workload | -.13 | -.17 | --- | | | |
| 4. Boredom | -.15 | -.16 | -.06 | --- | | |
| 5. False Alarms | -.19 | .10 | .08 | .17 | --- | |
| 6. Misses | -.08 | .05 | -.04 | .16 | .49** | --- |

*Note.* $N$= 101.
* = p<.05 ** = p<.01.

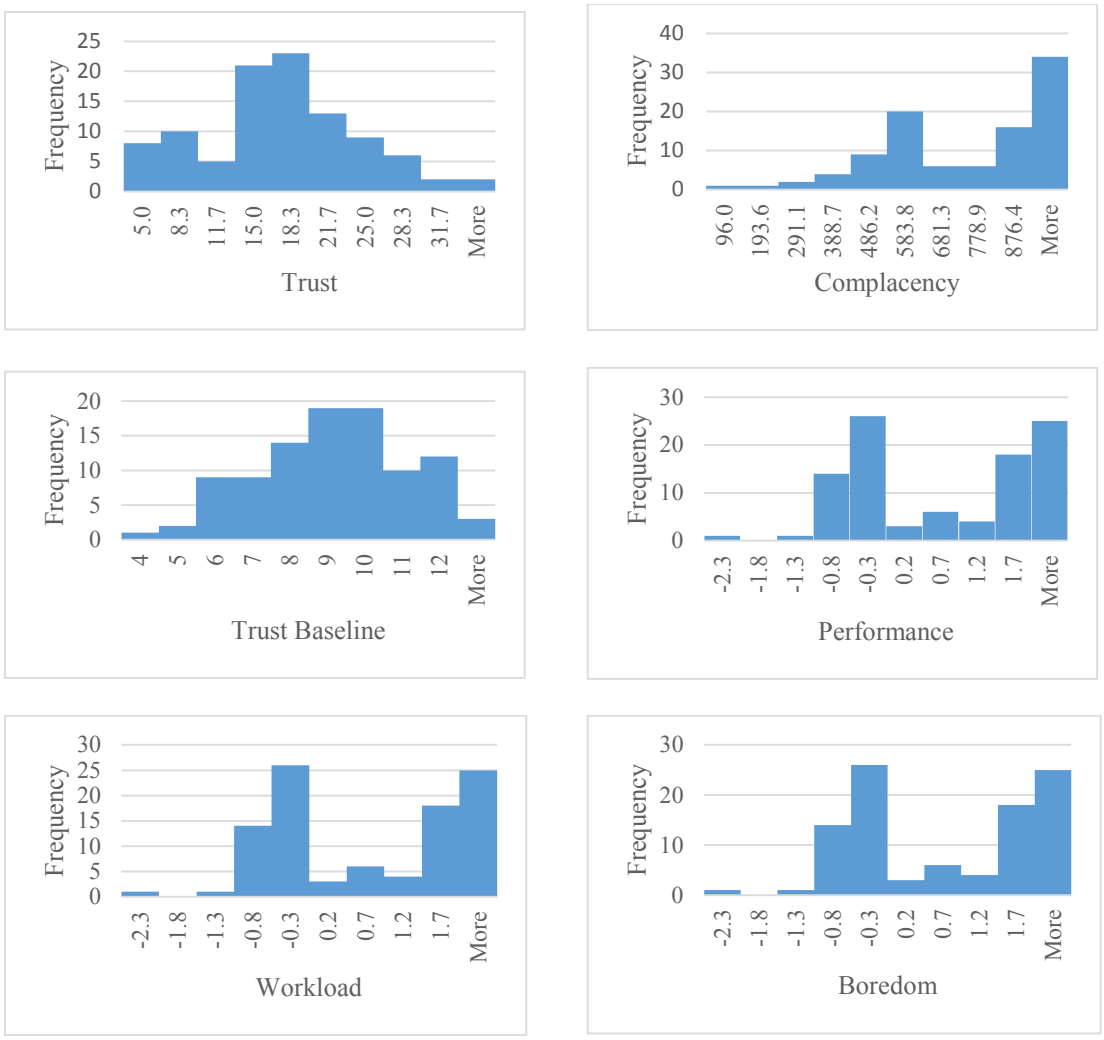


*Figure 3*. Histograms of measures.

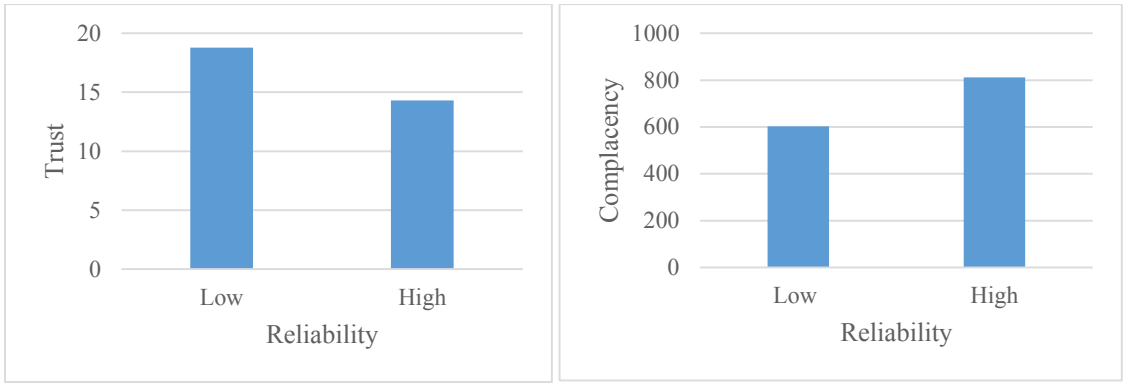


*Figure 4*. Trust and complacency plots.

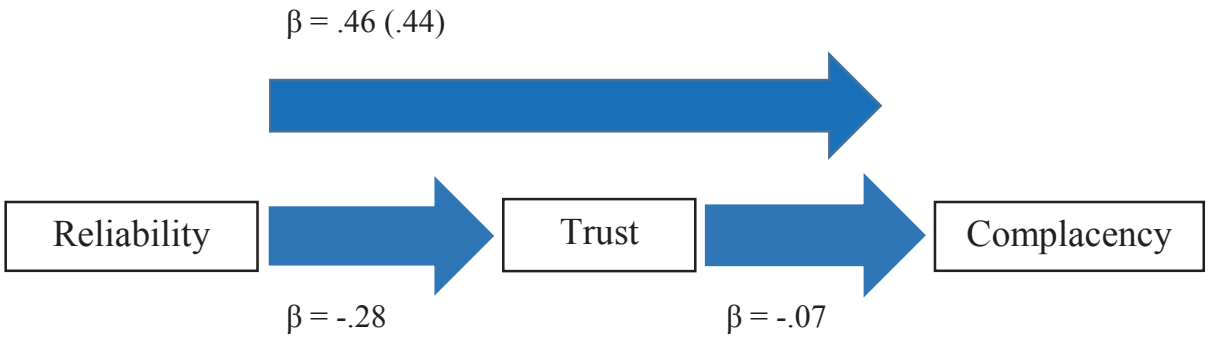


*Figure 5*. Mediation results.

**Test of Moderated Model**

Next, to explore an alternate model, the researcher explored whether trust moderated complacency. See Table 3 for regression results of the moderation test. In block 1, reliability did not predict complacency, accounting for only 3% of the variance, $R^2 = .05$, $R^2_{adjusted} = .03$, $F(2, 97) = 2.71$, $p = .071$. The standardized Beta coefficient for reliability was β = -.22, $t(97) = -2.26$, $p = .026$. In block 2, the researcher added a reliability by trust interaction term. Reliability's standardized Beta coefficient was β = -.06, $t(96) = -0.22$, $p = .827$, and trust's standardized Beta coefficient was β = -.06, $t(96) = -0.58$, $p = .561$. The standardized Beta coefficient for the interaction term was β = -.18, $t(96) = -0.72$, $p = .473$. $\Delta R^2$ was not significant, $\Delta R^2 = .01$, $F(1, 96) = 0.52$, $p = .473$. In all, the results provide no support for trust moderating or mediating the relationship between reliability and complacency.

Table 3

*Regression Results for Moderation Test*

| Variable | Beta | $R^2$ | $\Delta R^2$ |
|---|---|---|---|
| Block 1 | | .05 | |
| Reliability | -.22 | | |
| Block 2 | | .05 | .01 |
| Reliability | -.06 | | |
| Trust | -.06 | | |
| Reliability by Trust | -.18 | | |

**Effects on Performance**

The performance of the participant, as measured by sensitivity for signal detection (*d*') was higher for the high reliability condition ($M$ = .71) than the low reliability condition ($M$ = .33). This result mirrors the performance of the IDS, which was also higher for the high reliability condition ($M$ = .88) than the low reliability condition ($M$ = .57). False alarm rates were $M$ = 7.6 for the low reliability condition and $M$ = 3.96 for high reliability. The researcher used Baron and Kenney's (1968) method to test whether trust mediated the relationship between reliability and performance. The first step tested whether reliability predicted trust. Reliability significantly predicted 7% of the variance in trust, $R^2$ = .08, $R^2_{adjusted}$ = .07, $F(1, 98) = 0.84$, $p$ = .005. The second regression model tested whether reliability predicted *d'*. Reliability did not significantly predict performance, accounting for only 1% of the variance in sensitivity, $R^2$ = .02, $R^2_{adjusted}$ = .01, $F(1, 98) = 2.19$, $p$ = .142. The standardized Beta coefficient for reliability was β = .15, $t(98) = 1.48$, $p$ = .142. In the third step, reliability and trust were entered as

predictors of performance but only predicted 3% of the variance, $R^2 = .05$, $R^2_{adjusted} = .03$, $F(2, 97) = 2.37$, $p = .099$. The standardized Beta coefficient for reliability was $\beta = .13$, $t(97) = 1.31$, $p = .193$. As performance was not predicted by either reliability or trust with reliability, this mediation was not supported.

Last, the researcher explored whether trust is a moderator of performance. Reliability and trust did not predict performance in block 1, as they accounted for only 3% of the variance, $R^2 = .05$, $R^2_{adjusted} = .03$, $F(2, 97) = 2.37$, $p = .099$. The standardized Beta coefficient for trust and reliability was $\beta = .13$, $t(97) = 1.31$, $p = .193$. The reliability by trust interaction term was added in block 2. The standardized Beta coefficient the interaction term was $\beta = .08$, $t(96) = -0.70$, $p = .485$. $\Delta R^2$ was not significant, $\Delta R^2 = .01$, $F(1, 96) = 0.49$, $p = .485$, and neither was the reliability by trust interaction coefficient, $F(3, 96) = 1.74$, $p = .165$. Trust as a mediator of performance was not supported.

## Discussion

Reliability was found to have a causal relationship with complacency, such that higher reliability led to increased complacency. The high reliability condition led to higher complacency, possibly because the participants in this condition frequently relied on the automation exclusively. The cost of making a mistake may have been minimal for undergraduates who were protecting a simulated network and had no experience with the cost of misses in the real world. They frequently preferred to accept the guidance of the automation exclusively, even though it was 97.25% reliable, and this strategy led to misses, because that reliability level and the cost of a few misses in a simulated network

was acceptable to them. However, the mediation as well as a moderation were not found likely due to the lack of incentives for good performance by the undergraduate participants. As a result, this research provides limited immediate design recommendations towards calibrating trust to avoid complacency in cyber security professionals. Instead, the discussion will focus on the theoretical implications of this experiment, especially in the applied measurement of trust.

Firstly, the high reliability condition led to an over-reliance on the automation that functioned to simplify the task. For complacent participants in the high reliability condition who were unconcerned with a few misses, the task may have become became easy, routine, and fast. Possibly due to this characteristic of the experimental procedure, while reliability was found to predict trust, the relationship was in the opposite direction from many previous studies (Oakley, Mouloua, & Hancock, 2003; Yeh, & Wickens, 2001). The researcher suggests that trust was low in this condition, because trust attributions may take time to form. Participants in the low reliability condition frequently spent more time and effort during the experiment, allowing more time to form trust. While time and effort may have confounded the trust results, this finding suggests that trust attributions are influenced by multiple factors that can overcome the influence of the reliability of the automation.

The second main limitation was due to the participant population. Undergraduates may not have had accurate mental models of the system, which included log files and an IDS; they may not have accurately understood that the log files comprised the state of the network and the IDS functions as a form of automation to

provide guidance about attacks. The use of the trust questionnaire to measure trust was based on the assumption that the participants understood that the IDS was an entity. However, novice participants may not have understood the difference between the log files and the IDS. Inaccurate mental models that lay the basis for clear interpretation of questions on the trust questionnaire likely led to the lack of support found for the hypothesis that trust predicts complacency and mediates the relationship between reliability and complacency. This mismatch between the wording of the trust questionnaire and the mental models of the participants suggests that a trust questionnaire may not be an appropriate measure of trust when the object of trust is not clear. Participants may not have understood the role of the IDS or may not have thought of it as an agent. While reliability was found to impact complacency, this experiment illustrates that task factors, including time and effort spent during the experiment and the accuracy of participants' mental models, need to be considered by researchers when measuring trust.

In addition to trust's relationship with complacency, we also examined trust's effect on performance. Support for trust as a mediator or moderator of performance was not supported. It was unexpected that automation reliability did not predict performance, as measured by signal detection sensitivity, because one would expect that participants working with a 97.25% reliable IDS would identify attacks more accurately than those working with a 60% reliable IDS. However, there were frequent false alarms in both the high and low reliability groups. Performance may have been low overall due to the novice population. Misses were significantly correlated with false alarms, which

suggests that some participants may have been confused about how to identify an attack. Performance was not a focus of the experiment, because we would not expect performance to suffer greatly when participants are high in trust and complacent unless an unexpected event such as system failure occurs, which did not occur in this experiment. When human operators are complacent and automation fails, they are less prepared to take manual control, but if the automation continues to perform, the automation can support the performance of the human-automation team.

## Conclusion

The current study investigated trust's role in the relationship between reliability and complacency. Based on a limited number of studies from previous literature (Bagheri & Jamieson, 2004; Singh et al., 1993), trust was theorized to be a likely mediator between reliability and complacency, but trust was not found to either mediate or moderate this relationship. Reliability was found to predict both trust and complacency, but the relationship between reliability and trust was found to contradict previous literature and theory that high reliability facilitates the formation of trust. The non-significant mediation suggests that task factors may affect the impact of reliability on trust. Specifically, while previous research established that high reliability is related to high trust (Oakley et al., 2003; Yeh, & Wickens, 2001), trust is also impacted by the time and effort a participant spends interacting with the automation. Participants who rely exclusively on a highly reliable automated aid and who do not sample adequate information from the environment may incidentally simplify the task, and as a result, trust attributions may not be formed. In addition, when measuring trust in novices, the

accuracy of their mental models needs to be carefully considered when using self-report measures. Novices may not interpret the questions in the same way that experienced cyber security professionals do, even though the experimental task was simplified.

The results of the study have implications for measuring trust that can be generalized to the research community. Findings suggest that task factors influence trust. When measuring trust, it is important to control for time and effort spent on a task. In addition, in order to manipulate trust, time and effort as well as reliability can possibly be targeted. Secondly, findings of this study bring the consideration that subjective measures of trust may be influenced by the accuracy of participant's mental models and awarenesses of the automation's agency in a system.

Future research should investigate the impact of multiple task factors on trust. Trust may mediate the relationship between reliability and complacency in cyber security, but trust may be influenced by specific methodologies that need to be considered in addition to reliability. Specifically, future studies should examine whether time and effort spent on a task influence the development of trust and how these task factors interact with reliability. Further study could verify that trust can be attributed to reliable automation but only if there is sufficient time and effort spent on a task. Future studies should also examine whether the results of a subjective trust questionnaire are a factor of the accuracy of participants' mental models. Possibly, the reliability of a trust questionnaire depends on accurate conceptions of the system and the object of trust in a system.

# References

2013 cost of data breach study: Global analysis. (2013). *Phonemon Institute Research Report*. Retrieved from https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

Arief, B., & Besnard, D. (2003). Technical and human issues in computer-based systems security. *Technical Report Series-University of Newcastle upon Tyne Computing Science*. Report No. CS-TR 790, University of Newcastle, UK.

Barber, B. (1983). *The Logic and Limits of Trust*. New Brunswick, NJ: Rutgers University Press.

Bagheri, N., & Jamieson, G. A. (2004). Considering subjective trust and monitoring behavior in assessing automation-induced "complacency." In D. A. Vicenzi, M. Mouloua, & P. A. Hancock (Eds.), *Human Performance, Situation Awareness, and Automation* (HPSAA II, pp. 54–59). Mahwah, NJ: Erlbaum.

Bahner, J. E., Hüper, A. D., & Manzey, D. (2008). Misuse of automated decision aids: Complacency, automation bias and the impact of training experience. *International Journal of Human-Computer Studies*, *66*(9), 688-699.

Bailey, N. R., & Scerbo, M. W. (2007). Automation-induced complacency for monitoring highly reliable systems: The role of task complexity, system experience, and operator trust. *Theoretical Issues in Ergonomics Science*, *8*(4), 321-348.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173.

Billings, C. E. (1991). Human-centered aircraft automation: A concept and guidelines. (NASA Technical Memorandum 103885). Moffett Field, CA: NASA-Ames Research Center.

Bromiley P. & Cummings, L. L. (1996). Transaction costs in organizations with trust. In R. Bies, R. Lewicki, and B. Sheppard (Eds.), *Research on Negotiation in Organizations* (Vol. 5, pp. 219-247). Greenwich, CT: JAI.

Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress,* (Vol. 116, pp. 213-218).

Cain, A. A., & Schuster, D. (2014, March). Measurement of situation awareness among diverse agents in cyber security. In *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2014 IEEE International Inter-Disciplinary Conference on* (pp. 124-129). IEEE.

Crossman, E. R. F. W. (1974). Automation and skill. In E. Edwards & F. P. Lees (Eds.), *The Human Operator in Process Control* (pp. 1-24). London: Taylor & Francis.

Danaher, J. W. (1980). Human error in ATC system operations. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *22*(5), 535-545.

Dekker, S., & Lützhöft, M. (2004). Correspondence, cognition and sensemaking: A radical empiricist view of situation awareness. In S. Banbury & S. Tremblay (Eds.), *A Cognitive Approach to Situation Awareness: Theory and Application* (pp. 22–41). Aldershot, UK: Ashgate.

Deutsch, M. (1960). The effect of motivational orientation upon trust and suspicion. *Human Relations*, *13*, 123-139.

de Vries, P., Midden, C., & Bouwhuis, D. (2003). The effects of errors on system trust, self-confidence, and the allocation of control in route planning. *International Journal of Human-Computer Studies*, *58*(6), 719-735.

Drory, A. (1982). Individual differences in boredom proneness and task effectiveness at work. *Personnel Psychology*, *35*(1), 141-151.

Dzindolet, M. T., Peterson, S. A., Pomranky, R. A., Pierce, L. G., & Beck, H. P. (2003). The role of trust in automation reliance. *International Journal of Human-Computer Studies*, *58*(6), 697-718.

Grossman, A. (2014, June 3). Authorities break up hijacked computer network. *Wall Street Journal*, p. B5. Retrieved from http://www.wsj.com/articles/hijacked-computer-network-broken-up-by-law-enforcement-1401738851

Hardin, R. (1992). The street-level epistemology of trust. *Analyse & Kritik*, *14*(2), 152-176.

Hart, S. G., & Staveland, L. E. (1988). Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. *Advances in Psychology*, *52*, 139-183.

Ho, G., Wheatley, D., & Scialfa, C. T. (2005). Age differences in trust and reliance of a

medication management system. *Interacting with Computers*, *17*(6), 690-710.

Iheagwara, C., Blyth, A., Kevin, T., & Kinn, D. (2004). Cost effective management frameworks: The impact of IDS deployment technique on threat mitigation. *Information and Software Technology*, *46*(10), 651-664.

Inagaki, T., Furukawa, H., & Itoh, M. (2005). Human interaction with adaptive automation: Strategies for trading of control under possibility of over-trust and complacency. In *Proceedings 1st International Conference on Augmented Cognition* CD-ROM*,* 1-10.

Jian, J. Y., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics*, *4*(1), 53-71.

Johns, J. L. (1996). A concept analysis of trust. *Journal of Advanced Nursing*, *24*(1), 76-83.

Johnson, S. (2014, May 22). Shoring up cybersecurity tied to bottom-line losses. *San Jose Mercury News*. Retrieved from http://www.mercurynews.com/business/ci_25818380/shoring-up-cyber-security-tied-bottom-line-losses

Klein, G. A. (1989). Recognition-primed decisions. In W. B. Rouse (Ed.), *Advances in Man-Machine System Research* (Vol. 5, pp. 47-92). Greenwich, CT: JAI.

Kramer, R. M. (1996). Divergent realities and convergent disappointments in the hierarchic relation: The intuitive auditor at work. In Kramer and Tyler (Eds.), *Trust in Organizations* (pp. 216-245). Thousand Oaks, CA: Sage.

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology*, *50*(1), 569-598. Palo Alto, CA: Annual Reviews.

Lee, J. D., & Moray, N. (1994). Trust, self-confidence, and operators' adaptation to automation. *International Journal of Human-Computer Studies*, *40*(1), 153-184.

Lee, J. D., & See, K. A. (2002). Trust in computer technology and the implications for design and evaluation. In C. Miller (Ed.), *Etiquette for Human-Computer Work: Technical Report* FS-02-02 (pp. 20-25). Menlo Park, CA: American Association for Artificial Intelligence.

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *46*(1), 50-80.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social forces*, *63*(4), 967-985.

Manzey, D., Bahner, J. E., & Hueper, A. D. (2006, October). Misuse of automated aids in process control: Complacency, automation bias and possible training interventions. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 50, No. 3, pp. 220-224). Sage Publications.

Meyer, J. (2001). Effects of warning validity and proximity on responses to warnings. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *43*(4), 563-572.

McAllister, D. J. (1995). Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, *38*(1), 24-59.

Moorman, C., Deshpande, R., & Zaltman, G. (1993). Factors affecting trust in market research relationships. *The Journal of Marketing*, *57*, 81-101.

Moray, N., & Inagaki, T. (2000). Attention and complacency. *Theoretical Issues in Ergonomics Science*, *1*(4), 354-365.

Mosier, K. L., & Skitka, L. J. (1996). Human decision makers and automated decision aids: Made for each other? In R. Parasuraman & M. Mouloua (Eds.), *Automation and Human Performance: Theory and Application* (pp. 201–220). Mahwah, NJ: Erlbaum.

Muir, B. M. (1987). Trust between humans and machines, and the design of decision aids. *International Journal of Man-Machine Studies*, *27*(5), 527-539.

Oakley, B., Mouloua, M., & Hancock, P. (2003). Effects of automation reliability on human monitoring performance. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 47, No. 1, pp. 188-190). SAGE Publications.

Parasuraman, R., & Manzey, D. H. (2010). Complacency and bias in human use of automation: An attentional integration. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *52*(3), 381-410.

Parasuraman, R., & Miller, C. A. (2004). Trust and etiquette in high-criticality automated systems. *Communications of the ACM*, *47*(4), 51-55.

Parasuraman, R., Molloy, R., & Singh, I. L. (1993). Performance consequences of automation-induced 'complacency'. *The International Journal of Aviation Psychology*, *3*(1), 1-23.

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *39*(2), 230-253.

Prinzel III, L. J., DeVries, H., Freeman, F. G., & Mikulka, P. (2001). Examination of automation-induced complacency and individual difference variates (Technical Memorandum No. TM-2001-211413). Hampton, VA: National Aeronautics and Space Administration Langley Research Center.

Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Journal of Personality and Social Psychology*, *49*(1), 95-112.

Riley, V. A. (1994). *Human use of automation*. Unpublished doctoral dissertation, University of Minnesota, Minneapolis.

Rotter, B. J. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, *35*(4), 651-665.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122-131.

Sheridan, P. M. (2014, May 5). Target breach: How things stand. *CNN Money*. Retrieved from http://money.cnn.com/2014/05/05/news/companies/target-breach/

Singh, I. L., Molloy, R., & Parasuraman, R. (1993). Automation-induced "complacency": Development of the complacency-potential rating scale. *The International Journal of Aviation Psychology*, *3*(2), 111-122.

Sobel, M. E. (1982). Asymptotic confidence intervals for indirect effects in structural equations models. In S. Leinhart (Ed.), *Sociological Methodology 1982* (pp. 290-312). San Francisco: Jossey-Bass.

Tyler, T. R., & Degoey, P. (1996). Trust in organizational authorities: The influence of motive attributions on willingness to accept decisions. *Trust in Organizations: Frontiers of Theory and Research* (pp. 331–356). Thousand Oaks, CA: Sage.

Wickens, C. D., & Dixon, S. R. (2007). The benefits of imperfect diagnostic automation: A synthesis of the literature. *Theoretical Issues in Ergonomics Science*, *8*(3), 201-212.

Wiener, E.L. (1985). Cockpit automation: In need of a philosophy. In *Proceedings of the 1985 Behavioral Engineering Conference* (pp. 369-375). Warrendale, PA: Society of Automotive Engineers.

Yeh, M., & Wickens, C. D. (2001). Display signaling in augmented reality: Effects of cue reliability and image realism on attention allocation and trust calibration. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *43*(3), 355-365.

## Appendix A

**Consent Form**

# INFORMED CONSENT DOCUMENT

OLD DOMINION UNIVERSITY

**PROJECT TITLE:** Trust as a Predictor of Complacency on Cyber Security

## INTRODUCTION

Please take your time in deciding if you would like to participate in this research study by reading this document carefully. This document will record your consent to participate in this study, "Trust as a Predictor of Complacency on Cyber Security," in either MGB 331 or ECS 2100.

## RESEARCHERS

RESPONSIBLE PRINCIPAL INVESTIGATOR:
Jeremiah Still, PhD
Assistant Professor
Department of Psychology
College of Sciences

INVESTIGATOR:
Ashley Cain
Graduate Student
Department of Psychology
College of Sciences

## DESCRIPTION OF RESEARCH STUDY

The purpose of this study is to learn about processes that lead to cyber security breaches. You will be asked to monitor a computer server for incoming security threats. You will be provided with cyber security software to help you do this task. The results of this study will be used to improve cyber security tools and generate knowledge of how people perform cyber security tasks.

The study will last no more than 1 hour. You will interact with a computer throughout the experiment. In the first part of the study you will be asked to complete biographical questionnaires and a trust questionnaire. Next, you will be asked to complete several cyber security tasks. In each task, you will monitor a server for incoming security threats. Last, you will compete a second trust questionnaire, a boredom questionnaire, and a workload questionnaire.

## EXCLUSIONARY CRITERIA

You must be at least 18 years old to participate in this study.

**RISKS AND BENEFITS**

RISKS: There are no known risks to participating in this study beyond those risks you would encounter using a computer.

BENEFITS: We cannot promise any benefits to you or others from your taking part in this research. Participants will be immersed in an environment of scholarly research, which may help to augment their research education.

**COSTS AND PAYMENTS**

Your decision to participate in this study must be voluntary. And, we recognize that your participation, although educational, may pose some inconveniences. Therefore, you will receive course credit as designated by your instructor for your participation. We are unable to provide you with any monetary payment for participating.

**NEW INFORMATION**

Because this study may span several months, new information may emerge. If we found new information during this study that would reasonably change your decision to participate, we would provide it now.

**CONFIDENTIALITY**

The results of the study will not be associated with you in any way. We are required to keep a copy of this informed consent document, but it will be kept separate from the study results. No records are kept that allow your name to be associated with your responses in the study or on the survey. Your responses will be anonymous. The outcome of this research may be used in reports, presentations, and publications. But, again we will not identify you personally. Of course, your records may be subpoenaed by court order or inspected by government bodies with oversight authority.

**WITHDRAWAL PRIVILEGE**

Your participation in this study is completely voluntary and you may refuse to participate. If you agree to participate, you have the right to stop at any time with no penalty. You also have the right to skip any survey question that you do not wish to answer.

**COMPENSATION FOR ILLNESS AND INJURY**

If you say agree to participate, then your consent in this document does not waive any of your legal rights. However, in the event of any harm arising from this study, neither Old Dominion University nor the researchers are able to give you any money, insurance coverage, free medical care, or any other compensation for such harm. In the event that you suffer some type of harm as a result of participation in any research project, you may contact Dr. Jeremiah Still at 757-683-4051, Dr. George Maihafer the current IRB chair at 757-683-4520 at Old Dominion University, or the Old Dominion University Office of Research at 757-683-3460 who will be glad to review the matter with you.

**VOLUNTARY CONSENT**

By signing this form, you are saying several things. You are saying that you have read this form or have had it read to you, that you are satisfied that you understand this form, the research study, and its risks and benefits. The researchers should have answered any questions you may have had about the research. If you have any questions later on, then the researchers should be able to answer them: Dr. Jeremiah Still at 757-683-4051 or Dr. Mary Still at 757-683-4439.

If at any time you feel pressured to participate, or if you have any questions about your rights or this form, then you should call Dr. George Maihafer, the current IRB chair, at 757-683-4520, or the Old Dominion University Office of Research, at 757-683-3460.

And importantly, by signing below, you are telling the researcher that you DO agree to participate in this study. The researcher should give you a copy of this form for your records.

| | |
|---|---|
| **Print Your Name & Provide Signature** | **Date** |

**INVESTIGATOR'S STATEMENT**

I certify that I have explained to this participant the nature and purpose of this study, including benefits, risks, costs, and any experimental procedures. I have described the rights and protections afforded to human subjects and have done nothing to pressure, coerce, or falsely entice this subject into participating. I am aware of my obligations under state and federal laws, and promise compliance. I have answered the participant's

questions and have encouraged him/her to ask additional questions at any time during the course of this study. I have witnessed the above signature(s) on this consent form.

| | |
|---|---|
| **Investigator's Printed Name & Signature** | **Date** |

## Appendix B

## Automation-Induced "Complacency" Scale

Below is a list of statements for evaluation trust between people and general automation. Please mark an "x" on each line at the point that best describes your feeling or your impression.

(Note: not at all = 1; extremely = 5)

1 Manually sorting through card catalogues is more reliable than computer-aided searches for finding items in a library.

_____

1 2 3 4 5

2 I would rather purchase an item using a computer than have to deal with a sales representative on the phone, because my order is more likely to be correct using the computer.

_____

1 2 3 4 5

3 Bank transactions have become safer with the introduction of computer technology for the transfer of funds.

_____

1 2 3 4 5

## Appendix C
## Checklist for Trust between People and Automation

Below is a list of statements for evaluation trust between people and automation. There are several scales for you to rate the intensity of your feelings of trust, or your impression of the system while operating the IDS. Please mark an "x" on each line at the point that best describes your feeling or your impression.

(Note: not at all = 1; extremely = 7)

1 The system is deceptive

_____

1 2 3 4 5 6 7

2 The system behaves in an underhanded manner

_____

1 2 3 4 5 6 7

3 I am suspicious of the system's intent, action, or outputs

_____

1 2 3 4 5 6 7

4 I am wary of the system

_____

1 2 3 4 5 6 7

5 The system's actions will have a harmful or injurious outcome

_____

1 2 3 4 5 6 7

6 I am confident in the system

_____

1 2 3 4 5 6 7

7 The system provides security

1 2 3 4 5 6 7

8 The system has integrity

1 2 3 4 5 6 7

9 The system is dependable

1 2 3 4 5 6 7

10 The system is reliable

1 2 3 4 5 6 7

11 I can trust the system

1 2 3 4 5 6 7

12 I am familiar with the system

1 2 3 4 5 6 7

## Appendix D

**Demographic Questionnaire**

1 What is your age? ____

2 What is your gender? Male ____ Female ____

3 Are you a native English speaker? Yes ____ No ____

4 (If no) What is/are you're your native language(s)? _____

5 Do you wear prescriptive glasses or corrective contact lenses? Yes ____ No ____

6 (If yes) Are you wearing your glasses or contacts now? Yes ____ No ____

## Appendix E

**Boredom Measure**

Check any that apply.

1 Feeling bored ____

2 Feeling that I wish to do something else now ____

3 Feeling of monotony ____

4 Feeling that time goes very slowly ____

5 Feeling that nothing happens ____

6 Feeling that I wish to be at the end of the road now ____

## Appendix F

**NASA-TLX**

Put an "x" on the line to express your experience with the automation.

1 How much mental and perceptual activity was required (e.g. thinking, deciding, calculating, remembering, looking, searching, etc.)? Was the task easy or demanding, simple or complex, exacting or forgiving?

_____

Low High

2 How much physical activity was required (e.g. pushing, pulling, turning, controlling, activating, etc.)? Was the task easy or demanding, slow or brisk, slack or strenuous, restful or laborious?

_____

Low High

3 How much time pressure did you feel due to the rate or pace at which the tasks or task elements occurred? Was the pace slow and leisurely or rapid and frantic?

_____

Low High

4 How successful do you think you were in accomplishing the goals of the task set by the experimenter (or yourself)? How satisfied were you with your performance in accomplishing these goals?

_____

Good Poor

5 How hard did you have to work (mentally and physically) to accomplish your level of performance?

_____

Low High

6 How insecure, discouraged, irritated, stressed and annoyed versus secure, gratified, content, relaxed and complacent did you feel during the task?

_____

Low High

## Appendix G

**IRB Approval**

SJSU SAN JOSÉ STATE UNIVERSITY

Office of Research
Division of
Academic Affairs

San José State University
One Washington Square
San José, CA 95192-0025

TEL: 408 924-2272
sjsu.edu/research

To: Ashley Cain

From: Pamela C. Stacks, Ph.D.
Associate Vice President
Office of Research

Pamela C Stacks

Date: July 6, 2015

The Human Subjects-Institutional Review Board has approved your request to use human subjects in the study entitled:

"Trust as a Predictor of Complacency in Cyber Security"

This approval is contingent upon the subjects participating in your research project being appropriately protected from risk. This includes the protection of the confidentiality of the subjects' identity when they participate in your research project, and with regard to all data that may be collected from the subjects. The approval includes continued monitoring of your research by the Board to assure that the subjects are being adequately and properly protected from such risks. If at any time a subject becomes injured or complains of injury, you must notify Dr. Pamela Stacks immediately. Injury includes but is not limited to bodily harm, psychological trauma, and release of potentially damaging personal information. This approval for the human subject's portion of your project is in effect for one year, and data collection beyond July 6, 2016 requires an extension request.

Please also be advised that all subjects need to be fully informed and aware that their participation in your research project is voluntary, and that he or she may withdraw from the project at any time. Further, a subject's participation, refusal to participate, or withdrawal will not affect any services that the subject is receiving or will receive at the institution in which the research is being conducted.

If you have any questions, please contact me at (408) 924-2479.

Protocol # S15102

cc. David Schuster 0120