3-9-2009

The Development of IT Suspicion as a Construct and Subsequent Measure

Matthew T. Olson

THE DEVELOPMENT OF IT SUSPICION AS A CONSTRUCT AND SUBSEQUENT MEASURE

THESIS

Matthew T. Olson, Captain, USAF

AFIT/GEM/ENV/09-M15

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GEM/ENV/09-M15

THE DEVELOPMENT OF IT SUSPICION AS A CONSTRUCT AND SUBSEQUENT MEASURE

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Engineering Management

Matthew T. Olson, BS

Captain, USAF

March 2009

AFIT/GEM/ENV/09-M015

THE DEVELOPMENT OF IT SUSPICION AS A CONSTRUCT AND SUBSEQUENT MEASURE

Matthew T. Olson, B.S.
Captain, USAF

Approved:

Alexander J. Barelka, Lt Col, USAF (Chairman) Date

Daniel T. Holt, Lt Col, USAF (Member) Date

Michael R. Grimaila, (Member) Date

AFIT/GEM/ENV/09-M15

Abstract

Suspicion has not been studied in great depth; however, a conceptual understanding of suspicion is no less important than many of the other highly studied constructs related to healthy working relationships. Information technology (IT) is one area where suspicion study is lacking, and this research effort was a study into the specific domain of IT suspicion.

An extensive study of the suspicion literature and the suspicion nomological net as well as informal surveys of the general populous and subject matter experts were used to create an IT suspicion conceptual definition and measure. In order to test IT suspicion's relationships with other more established constructs a survey was created. The final pilot study consisted of two measures from suspicions nomological net, locus of control and disposition to trust, a trait IT suspicion measure, a manipulation exercise on a laptop computer intended to induce suspicion, and finally a state suspicion measure.

Analysis indicated IT suspicion is a multi-dimensional construct, with independent state and trait properties. It also has separate dimensions within the state and trait components. Comparisons between the components of the IT suspicion construct and related measures indicated a negative correlation between state suspicion and locus of control.

Acknowledgments

I would like to thank my family, classmates, and committee, without whom this thesis would not have been possible.

Matthew T. Olson

Table of Contents

List of Figures

Page

List of Tables

THE DEVELOPMENT OF IT SUSPICION AS A CONSTRUCT AND SUBSEQUENT MEASURE

I. Introduction

The idea of suspicion is one that is common in everyday conversation. Most people intuitively have a conceptualization of suspicion in their minds, but would have a hard time expressing it in terms of a definable construct that can be studied. Similarly, suspicion is a concept that is often loosely identified or undefined by researchers because, as is often the case, they assume the reader knows the definition of the construct under investigation. In most cases, suspicion is tangentially mentioned in an attempt to describe the real target of the research. Such literature is full of nebulous or assumed definitions for suspicion, not conceptualizing it in a way that makes it truly valuable to research on its own. This effort attempts to fill the void by creating conceptual definition and measure for a domain of suspicion.

While suspicion is briefly mentioned in many organizational behavior studies, there are few examples of research focused specifically on the different domains of suspicion. Most that do exist center on generic communication-related suspicion. Another (Levine and McCornack, 1991) focused on suspicion in criminology and prisons rather than suspicion in productive working relationships. Based on this, there appears to be some conceptualizations for suspicion that would inform the domain, if researched.

In addition to minimal domain-specific suspicion research, an even smaller number of validated measures for suspicion exist. When some forms of suspicion are defined and researched, manipulation checks (Caso et al., 2006) and validation are often incomplete. A lack of proper validation makes a small list of domain-specific suspicion research even smaller. Few suspicion studies combined with inconsistent validation creates a deficiency in the suspicion literature.

Taking a high-level view of suspicion and creating a research topic out of it requires focusing suspicion within an overarching context, such as a jury's suspicion of guilt or innocence of a criminal on trial. Once a context has been determined, thorough research of the context can be accomplished and a focused definition of suspicion within that context can be created. Framing suspicion in such a way is necessary to make it testable.

One viable context for researching suspicion is the area of information technology (IT).   The information systems and computer technology that make up IT are important to nearly every individual in the modern world, and this is a fertile area, full of weakly defined concepts (Barki, 2008) that could be developed into constructs. Research into cognitive, attitudinal, and behavioral constructs set within a reference of IT will provide valuable results; therefore IT is the context of this suspicion research.

IT is a primary tool used to perform work, communicate, and store information by nearly every company today. For the purposes of this research, information technology will be defined as the computer systems, software, and networks used for the processing, distribution and storage of data. Computer hardware and software and the global communication network have become the backbone for obtaining, processing, storing, and interpreting data and information for the execution of daily operations in nearly every organization.

The practical importance of suspicion in terms of IT is easy to visualize. Security, validity, and authenticity are always of primary concern when dealing with important and sensitive information, and requirements for protecting and disseminating this type of information abound in today's organizations. For obvious reasons, security of IT systems is crucial. The information and IT infrastructure must be protected to ensure smooth organizational operations. The perceived validity of any information delivered using IT is also important, and it would seem natural that questioning the validity of IT delivered information could have a negative impact on organizational activities. Uncertainty of information authenticity (who it came from) could also lead to hesitation and work failure. This uncertainty can arise from not trusting the human source of the information in the IT system or not trusting the computer-mediated communication infrastructure that replaces face-to-face communication. This concept should be measured in some manner, and a construct of IT suspicion seems to be a natural way of doing that. This leads to the problem statement of this research.

What is Information Technology suspicion and how can it be measured?

Research Objectives

The objectives of this research effort are to (1) define a construct for IT suspicion, (2) create a subjective measure for this construct, (3) acquire a mobile lab for administering the construct measure and for future research, and (4) execute a pilot study of the measure to guide future research.

Methodology

The first step in creating and measuring a construct is the theoretical activity of generating a conceptual definition. A conceptual definition of the IT suspicion construct cannot be created without a review of the existing suspicion related research. The existing literatures must be used to clearly define the concept of IT suspicion and identify dimensions for the construct. Once complete, the nomological network of IT suspicion can then be explored, examining convergent and discriminate validity (Judge et al., 2003) of the new IT suspicion construct. The sum of these activities is a validated theoretical IT suspicion construct.

Once an IT construct has been created, the empirical activity of producing a corresponding subjective measure is required for data gathering and future hypothesis testing. Multiple items are generated using information gathered from measures of existing related constructs and subject matter expert input. Items are then validated and analyzed using appropriate statistical methods.

In order to administer the suspicion measure and collect data, a mobile test lab was procured. Computers with a manipulation exercise were used to induce suspicion in the test subjects. The equipment will also be used as a platform allowing for further research in the area of IT suspicion, including further sampling and revised measures incorporating team activities.

The final step in this research was administering a pilot study of the IT suspicion measure. Results were analyzed to further validate measure items and outline areas of possible future research.

Implications

Measuring IT suspicion is a very important concept as it relates to both industry and the DoD. When dealing with IT, there is a delicate balance between system security and availability. The greater the level of security required, the greater the tendency to reduce ease of use (Pipkin, 2000). This carries over well into the concept of IT suspicion. Ensuring critical military data and information is maintained in a way that ensures authentication, integrity, and confidentially is important, but it must not be so buried in security procedures as to make it unavailable to all allied combatants who need it. IT suspicion mirrors security's relationship to capability, too little or too much can lead to disaster.

The absence of IT suspicion can be disastrous for corporate or national security. The United States has many enemies home and abroad, and these enemies are constantly attempting to probe, hack, and disrupt the IT systems and infrastructure of the United States government or major corporations. One hacker group alone, Javaphile, has launched over 200 attacks on the US government and other NATO allies (Henderson, 2007). An employee ignoring the possibility of these attacks leaves the United States far more vulnerable. Ignoring the possibility of attack through lack of suspicion can lead to theft or destruction of classified information or trade secrets, denial of production or critical war fighting services, and loss or intercept of sensitive organizational communication.

A second, less obvious reason to characterize the level of IT suspicion is that too much suspicion can have a negative impact on productivity. Every day more and more communications and collaboration are electronic instead of face to face, so it is crucial that IT systems in different organizations communicate securely and effectively. High levels of suspicion can negatively impact communication and productivity in an inter- or intra-organizational context.

High levels of suspicion lead to guarded, competitive behavior which has a negative impact on common goal seeking, positive compromise, and collaboration (Heretick, 1984). In a DoD environment driven by the Goldwater-Nichols Act and the Global War on Terror to a more joint arena, overly suspicious attitudes can create tension and conflict between the armed services and their organizations, negatively impacting mission accomplishment. The commercial sector can also be damaged by suspicion levels that are too high. Business strategies now include more collaborations than ever with increased outsourcing and business partnerships (Pipkin, 2000). Suspicion above a healthy level could affect the taking of action and the bottom line.

In addition to damaging inter-organizational relationships, high suspicion levels also negatively impact intra-organizational activities within the Air Force. The exact relationship between trust and suspicion depends upon how each is defined, but Hoffman states that suspicion negatively affects a trusting relationship (Hoffman, 2007). This means high suspicion leads to a relationship lacking trust, creating a chain of command that lacks trust in superiors and subordinates. In such an organization, poor trust would lead to poor delegation and communication. In addition, suspicion makes individuals less likely to conform to procedures (Stricker et al., 1967) that are healthy and required for organizational success. Poor delegation and communication lead to inefficient use of resources. Poor communication also leads to lower productivity through incorrect explanation of expectations, poor feedback, and numerous other problems. The negative impact of lack of trust and high suspicion in a work environment is summed up best by Hoffman when he said trusting takes less effort (Hoffman, 2007).

With all the implications of too much or too little IT suspicion, it is apparent that knowledge about what causes it to increase and decrease is important. Creating and testing a measure for IT suspicion is the first steps in a stream of study that will allow the researchers to characterize these antecedents and what scenarios and technologies create healthy and unhealthy levels of suspicion.

II. Literature Review

IT Suspicion Definition Methodology

Research into the area of IT suspicion cannot proceed without formally defining IT suspicion. If there is indeed an abundance of opportunities to develop validated IT constructs in order to provide a better understanding of IT relationships (Barki, 2008), it starts with a clearly defined concept of IT suspicion since "a valid definition for a concept is a prerequisite to a valid measurement" (Locke, 2003, p. 417). Choosing techniques for creating, testing, and refining a construct that promote thoroughness and validity are the most important steps in this research effort. Numerous methodologies exist to produce a well-bounded and sound definition for IT suspicion. Several approaches are outlined in Barki (2008) and a few of those seem particularly relevant and are used in this research.

Intuitively, defining a construct would appear to be as simple as looking it up in a dictionary. However, constructs are abstract (Bacharach, 1989), and such simple one dimension conclusions do not provide the required level of rigor necessary to adequately conceptualize such an abstraction. As previously stated, suspicion is a concept mentioned sometimes in the literature but with few conceptual definitions offered, and none that relate to IT. Consequently, a testable definition of IT suspicion simply does not exist.

Generating a proper conceptualization of IT suspicion is the first step in defining this construct. Exploring how the construct of IT suspicion applies in different contexts and expanding the conceptualization of the construct (Barki, 2008) are important steps. Barki (2008) discusses many approaches in terms of determining new, useful constructs, but it should follow that these methods would also be useful in defining a specific construct under a larger reference umbrella, like IT suspicion under suspicion. Examining IT suspicion in different contexts and trying to relate it to an expanded or altered conceptualization of another suspicion-like construct helped to narrow down the definition and determine which existing construct items may be useful. When generating a conceptual definition of a construct, using other established constructs that are related to the construct being studied can also be useful (Bacharach, 1989). Other validated constructs such as domains of trust are critical to this research effort.

A literature review and completion of the steps listed above provide a list of constructs related to IT suspicion. These constructs make up the nomological network for IT suspicion (Judge et al., 2003) and prove useful in validation and the creation of the IT suspicion measure. The method used to generate IT suspicion measure items from the nomological network defined in this literature review are discussed in Chapter 3.

IT Suspicion Defined

As discussed above, the creation of an IT suspicion construct requires the examination of suspicion constructs in other literatures as well as constructs related to suspicion. Existing suspicion definitions vary in scope, as do their respective constructs, when constructs have been created. The biggest difference in existing suspicion research is the relationship suspicion is examined under, in other words, who is suspicious of what. In addition, some researchers characterize suspicion from a state perspective, only analyzing a current situation. In contrast, others view suspicion from a trait perspective, requiring the long-term observation to determine tendencies. Even the quantification of suspicion varies, with some researchers viewing suspicion as a dichotomy, while others quantify suspicion using a continuous scale.

The existing literature was searched by using the Social Sciences Citation Index of the ISI Web of Knowledge online academic database. The key word “suspicion” yielded an initial set of results containing articles on suspicion and suspicion related constructs. A review of those articles was used to generate a preliminary nomological net for suspicion including trust and locus of control. The literature review was completed by searching under the key words “trust” and “locus of control”, as well as by using references from articles from all three searches. This yielded a collection of works that conceptually define suspicion and its nomological net, characterize the relationships between the concepts in that net, and provide constructs and items to measure these concepts.

Suspicion was the primary focus of the literature review. Heretick researched suspicion and trust as it relates to gender differences. In her research she conceptually defined suspicion as “expectancies that another is self-motivated” (Heretick, 1984, p. 29) and a construct called trust-suspicion (T-S) as “expectancies that others are generally motivated to be supportive and beneficial toward others” (Heretick, 1984, p. 28). While her conceptual definition of suspicion does not address the temporal specifics of the sender/receiver relationship, the T-S conceptual definition does through the phrase “generally motivated”, implying an enduring relationship and a trait construct. In addition, in her conceptual suspicion definition, Heretick did not address whether self-motivation leads to a positive or negative outcome. Self-motivation by the sending party could still lead to positive results for the receiving party.

Fein (1996) also examined suspicion in a purely conceptual manner, specifically as it relates to personal motives. He defined suspicion as “a dynamic state in which the individual actively entertains multiple, plausibly rival hypotheses about the motives or genuineness of a person's behavior” (Fein, 1996, p. 1165). His definition differs from Heretick’s in that it defined suspicion as a state instead of trait characteristic, but he also maintained an outcome-neutral stance about the sender’s potential self-motivation.

Both Heretick and Fein appeared to consider the receiver’s perception of the motivation of the sender’s behavior in their conceptual definitions of suspicion. Motivation can be defined as “a set of energetic forces that originate both within as well as beyond an individual’s being, to initiate work-related behavior and to determine its form, direction, intensity, and duration” (Pinder, 1998). When relating this definition to motivation of IT in an IT suspicion conceptual definition, the form of the behavior could be considered IT. Intensity and duration could also be considered the amount of effect and temporal length of the behavior that would arouse suspicion of IT. For direction, we can examine Burgoon, Buller, Ebesu, White, and Rockwell.

Burgoon et al. examine suspicion in terms of Interpersonal Deception Theory, researching behaviors of two individuals when deception was implanted into their communication. In their research, suspicion was defined as “a receiver variable that refers to doubt about another’s truthfulness or honesty” (Burgoon et al., 1996, p. 243), and the research subject was simply asked to rate their suspicion on a continuous scale. Like Fein, this is another example of a state suspicion concept of a dyadic relationship. Where it differs from the previous two examples is that it is not outcome neutral. “Doubt about another's truthfulness or honesty" definitely carries a negative connotation with it. Therefore, the direction of the outcome is negative.

Levine and McCornack researched the relationship between trust, suspicion, and lie bias, or the "bias toward decoding all incoming messages as deceptive" (Levine and McCornack, 1991, p. 328). In their research, they define generalized communication suspicion (GCS) as a "predisposition toward believing that the messages produced by others are deceptive" and stated that it is a "relatively consistent and enduring tendency" (Levine and McCornack, 1991, p. 328). Their GCS construct measured suspicion as a trait characteristic on a continuous scale. Like Burgoon et al., Levine and McCornack viewed the potential outcome direction as negative, only more directly by stating the "messages produced by others are deceptive". Of note, at the time of their research, Levine and McCornack stated no attempt had been made to develop distinctions between different types of suspicion and no prior attempt had been made to create an instrument for measuring GCS (Levine and McCornack, 1991).

In addition to defining GCS, Levine and McCornack also defined a concept called general state suspicion as "the situation-specific belief that the messages of a particular person may be deceptive. As such, state suspicion can be aroused by a particular event or cue within a context" (Levine and McCornack, 1991, p. 329). Previous examples also demonstrated that suspicion can be a state or trait concept. It follows that if a general trait suspicion can determined and a stimulus applied, a state suspicion of that particular stimulus could be determined.

One final consideration in developing an IT suspicion construct is to ensure survey questions address suspicion related to IT, not toward the method of data gathering.

In their research into suspicion of deception, Stricker, Messick, and Jackson (1967) used different open-ended questionnaires for suspicion of the purpose of the research and suspicion in the method of the research. Results showed differences between suspicion of method and suspicion of the purpose of their research, showing the importance of being specific in IT suspicion survey questions. A subject may not be suspicious of IT at all, but suspicion of the purpose of the research, which can distort results if surveys are not written and administered properly.

As the previously listed suspicion definitions show, suspicion is commonly defined in terms of the individual who is suspicious (the receiver) and the individual who generates the suspicion (the sender). A unique problem encountered in defining IT suspicion is the sender isn't an individual at all; the sender is the information technology used to pass various services and forms of information to receiver. IT does not have hidden emotional motives as a driver of performance and actions. Actions are driven by design, inputs, physics, and logic. Some inputs, however, do come from other individuals, and real people do design, build, and maintain IT systems. Truthfulness and deception from other definitions of suspicion associated with people become accurateness and corruption of data. Individual motives aren't doubted; IT system designs and policies are doubted. So from this, the following motivational and perceived outcome based definition for IT suspicion emerges:

User perceptions that the direction, duration, and intensity of an IT systems behavior will negatively impact their task.

Combining this definition with the definition of IT given in Chapter 1, evidence does exist for the possibility of multiple suspicion dimensions, even within the different contexts of state and trait suspicion. IT can be sub-categorized into the general physical hardware and software that make up a system and the electrons, or data, which are passed around and stored within the system. Items in the subsequent chapter should be written for general system suspicion as well as suspicion of the data contained within.

Correlated and Related Constructs

Trust and suspicion intuitively seem to have a strong relationship, so exploring that relationship helped build an IT suspicion construct. While it can be argued trust and suspicion are related, Levine and McCornack give two strong arguments why suspicion and interpersonal trust are not opposites. First, lack of trust is questioning whether a person will do the right thing while suspicion is questioning if they will do the wrong thing. Second, trust involves belief in a positive outcome while suspicion involves uncertainty about the possibility of a negative outcome (Levine and McCornack, 1991). Lack of trust doesn't mean a bad outcome and lack of suspicion doesn't mean a good outcome. There is, however, a high, negative correlation between the two (Levine & McCornack, 1991) which proves useful in construct assembly and validation. However, since suspicion and trust aren't opposites, the trust constructs must be reviewed very carefully before considering how, or if, components of the trust construct should be integrated into the IT suspicion construct.

There are many definitions of trust in existing literature. One study defined trust as "a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behavior of another" (Rousseau, 1998, p. 395). Another stated "At its core, *trust* refers to an actor's *perception* that it may safely delegate control over its interests to others (that is, potential trustees) under certain circumstances. This perception is rooted in the belief that potential trustees will protect the interests placed in their care even if some of their own interests suffer." (Hoffman, 2007, p. 288). Still another defined a concept called interpersonal trust as "an expectancy held by an individual or a group that the word, promise, verbal, or written statement of another individual or group can be relied upon." (Rotter, 1967, p. 664). One thing to be aware of when comparing trust to suspicion is to ensure that the intent is properly translated from one to the other. As stated previously, all variables associated with a lack of trust are not necessarily caused by the thought of possible deception. It can be caused by a perceived lack of capability of the trustee. The trustor may not be suspicious of the trustee's intent, but they may not be confident in the trustee's ability to complete a task.

Another article defined trust "in terms of confident positive expectations regarding another's conduct, and distrust in terms of confident negative expectations regarding another's conduct" (Lewicki et al., 1998, p. 439). This definition of trust and distrust provides an avenue for examining the relationship between trust and suspicion. The authors' definition of distrust is very similar to the above conceptual definition of suspicion. They go on to say that "low distrust is not the same as high trust" (Lewicki et al., 1998, p. 444) and give examples where low trust and low distrust or high trust and high distrust can exist. This further validates that trust and suspicion are not the same dimension simply reversed. Instead, they are related constructs.

According to Li, Hess, and Valacich, trust has five bases that make up a general trust formation. The five are personality base, cognitive base, calculative base, institutional base, and knowledge base (Li et al., 2008). Personality equates to a tendency or trait, similar to the trait characteristic of GCS. Cognitive and knowledge bases are related to second and first-hand experience with the trustee. The calculative base assumes a trustee will act in their own best interest, so a trustor will logically trust a trustee if it is no benefit to the trustee to deceive the trustor. A situation where there is of no benefit to the trustee to deceive the trustor can potentially create a scenario of lack trust but no suspicion. A trustor will not believe in hidden motives by the trustee, so no suspicion, but the trustor may not trust the institution base. An example of this may be an individual has no need to be suspicious of malicious intent or hidden motives of a news website on the internet but the individual has no reason to trust the validity of the content. This is another instance that demonstrates that trust and suspicion are not exact opposites.

Trust and suspicion are, however, very similar. Since trust is a far more researched construct than suspicion, this makes trust a very useful tool in creating a suspicion construct and in validating it. Care must still be taken to ensure a trust item used in a suspicion construct isn't one of the examples of lack of trust not equaling suspicion.

While IT trust and suspicion are not prevalent topics in existing research, trust related to e-commerce is well researched. For example, McKnight et al. (2002) defined the relationship between the disposition to trust, perception of the internet environment, and trusting beliefs as it relates to influencing trust intentions and trust actions. The simple model illustrated in Figure 1 helps explain how trust and a particular environment shape an individual's attitudes about a specific information technology. Disposition to trust is a representation of trait trust and trusting beliefs and intentions are similar to a state trust or trust of a specific thing or person at a specific time. Both must be measured to obtain a complete picture of a specific domain of trust. It follows that it would be the same for suspicion; measurements of trait suspicion and state suspicion are necessary to obtain a complete understanding of IT suspicion. Validated trust measures can also be used in determining convergent validity.

Figure 1. Trust Model Based on McKnight et al., 2002

Locus of control is defined as the degree to which individuals believe they control their own fate (Robbins and Judge, 2008). Individuals who have a high locus of control tend to be less suspicious while people who don't believe they control their lives are more suspicious because they believe they have no power to change their environment (Robbins and Judge, 2008). Locus of control is a trait attitudinal characteristic which cannot be directly used to generate any type of suspicion construct or measure items because it is a completely different dimension. However, since the two are related, a locus of control measure can be used to determine convergent validity of a suspicion measure.

III. Methods

Measure Generation

Given the presented definition of IT suspicion, a measure for it can now be created. The measure consists of three parts, the trait measures from suspicion's nomological net, the trait suspicion measure for establishing the baseline, and the state suspicion measure. The trait measures from the suspicion nomological net, trust and locus of control, were added to for validity testing in the analysis.

For this research, three areas were mined for input for the measure items. They are the literature, subject matter experts, and the general population. These resources were utilized in two deductive and one inductive approach to determine items for an IT suspicion measure.

Hinkin (1995) outlined two different deductive approaches that are used in this research to collect item information; obtaining items from suspicion's nomological network and extracting items from subject matter expert inputs based a conceptual definition for IT suspicion. This required an understanding of IT suspicion and theoretical definition from a thorough literature review (Hinkin, 1995), which was produced in Chapter 2. Once this was accomplished, the existing research was used to create items and validate possible dimensions. Items used came from the nomological network analysis. Since suspicion constructs with different domains (other than IT) exist, they were fertile ground for suspicion measure items. In addition, constructs for trust were used because the literature showed a strong negative correlation to suspicion. Each trust item used was reviewed and altered to ensure it addressed this research's definition of suspicion. Constructs from IT suspicion's nomological net are shown in Appendix A.

The second method of deductive development used involved the use of subject matter experts. In this method, the researcher again develops a sound conceptual definition of the construct, and then surveys subject matter experts for critical input in developing items (Hinkin, 1995). The Air Force Institute of Technology (AFIT) has experts on staff in the fields of IT and organizational behavior research. Two of the members of this thesis' research committee are organizational behavior research experts and the other is an IT expert.

The inductive method used for this research involved asking a sample of respondents to describe IT suspicion (Hinkin, 1995) and list ways to assess it. The respondents are from the general AFIT student population, and the results assisted the research effort in several ways. First, the results provided more items for use in the final measure. They also provided reinforcement by repeating already determined items. Finally, the provided IT suspicion descriptions guided the exploration of possible IT suspicion construct dimensions and validated the final conceptual definition of IT suspicion. The responses are listed in Appendix B.

Throughout the entire item generation process, content validity was maintained to the greatest extent that was workably feasible. Hinkin stated that there are two primary concerns with item generation. First, some measures lack proper content validity and second, some researchers fails to report their method for items generation (Hinkin, 1995). Using multiple methods for items generation and a thorough review of the existing literature helps strengthen the argument for the validity of the IT suspicion construct.

Once the list of items is compiled and compared, care must be taken to avoid extraneous content but guarantee the measure still captures the IT suspicion domain (Hinkin, 1995).

Hinkin also outlined five important issues that must be addressed in scale development. They are the details of the sample chosen, the use of reverse-scored items, the number of items, the scaling of the items, and the sample size (Hinkin, 1995). The sample came from the AFIT student population. Due to time constraints, this was the most feasible method to obtain volunteers. Hinkin's (1995) research explored 31 different studies that used reverse-scored (negatively worded) items. His examination of those studies showed no discernable pattern of problems in the analysis but the reverse-scored item loading was lower (Hinkin, 1995). Therefore, reverse-scored items were not used because loading was already assumed to be an issue due to a projected small sample size. The number of items used must be enough to define the construct without being too long in order guarantee construct validity and avoid response biases (Hinkin, 1995) respectively. Therefore, eight or nine items were used for each measure. A 5-point Likert scale is used to maximize reliability (Hinkin, 1995). The sample size was based solely on volunteers from the student body, so a low number was an undesirable but ultimately unavoidable result.

Procedure

The trait IT suspicion measure was administered with a disposition to trust and a locus of control measure. The intent was to establish a trait IT suspicion baseline and use other validated constructs from suspicion's nomological network for analyzing validity. Judge et al. used internality (Levenson, 1981) interchangeably with locus of control in a core self-evaluation publication (Judge et al., 2003). The original scale was modified from a 7-point to a 5-point scale for measure consistency. Two dispositional trust scales were also administered using a 5-point scale; one from a relational trust article (Rodgers and Deng, 2004) and the other from a virtual trust article (Riding et al., 2002). Neither of the scales is specific to the domain of IT.

The trait characteristic measure was followed by a simple computer task with a manipulation unknown to test subjects intended to raise a moderate level of suspicion. The task prompted the subject to write a paragraph about that day's work schedule, create a summary spreadsheet, and combine the two documents and save them in a created folder. The control panel was altered from the manufacturer settings in order to induce suspicion. The left and right mouse button functions were reverse, the double-click speed was increased, the pointer format was altered, and the pointer had a trail added to it (appears like multiple shadows). Upon completion of the computer task, the state IT suspicion measure was administered to determine an induced level of state IT suspicion. The entire IT suspicion survey is shown in Appendix C.

Measure Analysis

To further validate the new IT suspicion measure, a factor analysis and internal reliability test was accomplished on the pilot study data. An exploratory factor analysis was accomplished to reduce the set of items to a more parsimonious representation of IT suspicion, to test for multiple dimensions, and to provide evidence of construct validity (Hinkin, 1998). The Statistical Package for the Social Sciences (SPSS) software was used to accomplish this task. After a preliminary comparison of the inter-item correlations was accomplished to eliminate all items with a correlation of less than .4 to all the other items, the Eigenvalues for the potential factors were determined using factor analysis. Any group with a value greater than one was retained for further analysis (Hinkin, 1998). If multiple factors were present with Eigenvalues greater than one, each factor was explored using higher order factor analysis. The process was continued until the uncorrelated factors were identified or only one factor was extracted (Arnau, 1998).

Once an exploratory factor analysis was completed, providing a level of validation and narrowing the list of items, the reliability of the results was checked. SPSS was also used for this analysis. Once uni-dimensionality has been established through factor analysis, reliability can be determined using Cronbach's alpha (Hinkin, 1998). The remaining factors were tested for reliability, with a desired coefficient alpha of at least .7 for a new measure (Hinkin, 1998). Once the reliability was tested and the locus of control and disposition to trust measures were analyzed in the same manner as IT suspicion, the remaining groups were compared to the locus of control and disposition to trust measures using inter-correlation analysis.

IV. Analysis and Results

20 respondents from the Air Force Institute of Technology participated in the IT suspicion survey. There were 18 male and 2 female participants, all active duty Air Force officers. The results were entered into SPSS for the following analysis. Principal component factor analysis was used with all factors (components) retained having Eigenvalues greater than 1.

Analysis of IT suspicion measure

As previously mentioned in Chapters 2 and 3, the created suspicion measure included items to address trait and state suspicion, as well as generalized system questions and data specific questions. The trait IT suspicion general questions (trait-general) are items 1, 2, 3, 4, and 5 of the trait measure, while the trait IT suspicion data related questions (trait-data) are items 6, 7, 8, and 9. The state IT suspicion general questions (state-general) are items 2, 3, 4, 5, 7, 8, and 9 of the state measure, and the data specific questions (state-data) are items 1 and 6.

A first order exploratory factor analysis with orthogonal (Varimax) rotation was accomplished for the entire IT suspicion portion of the measure to begin the analysis. Results shown in Table 1 indicate highly correlated factors, which is consistent with expectations because all items measure some form of suspicion.

Table 1. Entire Construct Component Transformation Matrix

Component	1	2	3	4	5	6
1	0.732	0.225	0.478	0.305	0.265	0.147
2	-0.622	0.599	0.371	0.272	0.147	0.144
3	0.230	0.675	-0.403	-0.058	-0.104	-0.561
4	-0.009	0.064	-0.527	-0.033	0.788	0.310
5	0.067	0.252	0.266	-0.900	0.031	0.226
6	0.139	0.259	-0.350	0.138	-0.525	0.704

After the first order factor analysis with orthogonal rotation, a first order factor analysis with oblique (Oblimin) rotation, shown in Table 2, was accomplished for the entire IT suspicion portion of the measure (Arnau, 1998). Results indicate low correlations (<.2) between factors. What begins to emerge is a pattern between the way items were created for the IT suspicion measure and the way items are loading under components in the factor analysis.

Analysis of the structure matrix shows three of the five trait-general items load under factor 3; items 2 and 3 do not. All four trait-data load under factor 2. Six of the seven state-general load under factor 1; with item 5 being the exception. These are the three factors with the highest Eigenvalues and they explain 60% of the variance. The state data didn't load well under any factor, so it was removed from further analysis.

Table 2. Construct Structure Matrix

	Component					
Item	1	2	3	4	5	6
Trait IT suspicion item 1	0.241	-0.132	-0.870	0.100	-0.243	0.366
Trait IT suspicion item 2	-0.094	-0.067	-0.204	-0.082	-0.108	0.887
Trait IT suspicion item 3	0.164	0.032	-0.187	0.197	-0.921	0.157
Trait IT suspicion item 4	0.122	0.251	-0.858	0.275	-0.089	0.132
Trait IT suspicion item 5	0.121	0.230	-0.628	0.131	-0.659	0.085
Trait IT suspicion item 6	0.191	0.413	-0.802	-0.112	-0.435	0.113
Trait IT suspicion item 7	-0.016	0.716	-0.215	-0.090	-0.608	-0.131
Trait IT suspicion item 8	-0.164	0.879	-0.160	0.211	0.015	-0.017
Trait IT suspicion item 9	-0.208	0.764	-0.381	0.035	-0.003	-0.171
State IT suspicion item 1	0.159	0.154	-0.260	0.628	-0.083	0.728
State IT suspicion item 2	0.899	0.052	-0.215	-0.032	-0.055	-0.121
State IT suspicion item 3	0.855	-0.162	-0.055	0.169	-0.102	0.177
State IT suspicion item 4	0.874	0.024	-0.175	-0.033	-0.072	-0.081
State IT suspicion item 5	-0.250	0.257	-0.101	0.707	-0.433	0.240
State IT suspicion item 6	0.311	0.767	0.039	0.176	-0.339	0.191
State IT suspicion item 7	0.892	-0.151	-0.014	0.255	-0.162	-0.181
State IT suspicion item 8	0.782	0.033	-0.173	0.341	-0.166	0.337
State IT suspicion item 9	0.414	0.115	-0.189	0.827	-0.084	-0.101

A second order factor analysis with orthogonal rotation was then completed on the trait suspicion measure items. Results, shown in Table 3, again indicate highly correlated factors for trait general (component 1) and trait data (component 2), which is also expected due to the fact that they were both trait level suspicion measures.

Table 3. Trait Component Transformation Matrix

Component	1	2	3
1	0.647	0.512	0.565
2	-0.555	0.824	-0.111
3	0.522	0.241	-0.818

As a result, a second order factor analysis with oblique rotation was accomplished on the trait suspicion measure, indicating low correlation between factors (<.3). The structure matrix, Table 4, shows four of the five trait-general items load on factor 1, and all four trait-data items load on factor 2 with some cross-loading with factor 1 for item 6.

Table 4. Trait Structure Matrix

Item	Component 1	2	3
Trait IT suspicion item 1	0.924	-0.012	-0.323
Trait IT suspicion item 2	0.540	-0.205	-0.009
Trait IT suspicion item 3	0.204	-0.068	-0.890
Trait IT suspicion item 4	0.789	0.406	-0.211
Trait IT suspicion item 5	0.568	0.265	-0.722
Trait IT suspicion item 6	0.674	0.480	-0.579
Trait IT suspicion item 7	-0.009	0.650	-0.696
Trait IT suspicion item 8	-0.029	0.880	-0.078
Trait IT suspicion item 9	0.101	0.864	-0.165

A third order factor analysis with orthogonal rotation on the trait general suspicion items shown in Table 5 reflects two significant factors, one with an Eigenvalue of 2.48, but the second with an Eigenvalue of 1.030, so its contribution is questionable. The un-rotated solution indicates items 1, 4, and 5 have loaded properly on factor 1; however items 3 and 4 are problematic and were therefore removed from further analysis.

Table 5. Trait-General Component Matrix

Item	Component 1	2
Trait IT suspicion item 1	0.842	0.301
Trait IT suspicion item 2	0.402	0.685
Trait IT suspicion item 3	0.584	-0.557
Trait IT suspicion item 4	0.776	0.135
Trait IT suspicion item 5	0.819	-0.376

A final factor analysis on items 1, 4, and 5, shown in Table 6, yields one factor with an Eigenvalue of 2.15, representing 71.5% of the variance with a reliability coefficient alpha of .796. Therefore, these three items are retained for the final trait-general portion of the measure.

Table 6. Final Trait-General Component Matrix

	Component
Item	1
Trait IT suspicion item 1	0.853
Trait IT suspicion item 4	0.889
Trait IT suspicion item 5	0.793

A third order factor analysis with orthogonal rotation on the data items of the trait measure, shown in Table 7, reveals one factor with an Eigenvalue of 2.42, representing 60.5% of the variance, and with a coefficient alpha of .774. Therefore, these four items are retained for the final trait-data portion of the measure.

Table 7. Final Trait-Data Component Matrix

	Component
Item	1
Trait IT suspicion item 6	0.694
Trait IT suspicion item 7	0.809
Trait IT suspicion item 8	0.765
Trait IT suspicion item 9	0.836

After completing the exploratory factor analysis for the trait portion of the IT suspicion measure, a second order factor analysis with orthogonal rotation was completed on the general items of the state suspicion measure, shown in Table 8, revealing two uncorrelated factors (<.2). Factor one accounted for 57.3% of the variance.

Table 8. State-General Component Matrix

	Component	
Item	1	2
State IT suspicion item 2	0.887	-0.192
State IT suspicion item 3	0.855	-0.034
State IT suspicion item 4	0.861	-0.170
State IT suspicion item 5	-0.157	0.907
State IT suspicion item 7	0.904	-0.001
State IT suspicion item 8	0.801	0.134
State IT suspicion item 9	0.523	0.730

The second factor, which contained items 5 and 9, was therefore removed and the analysis was accomplished again, shown in Table 9, yielding one factor with an Eigenvalue of 3.75, representing 75.1% of the variance, and with a coefficient alpha of .916. Therefore, these five items were retained for the final state-general portion of the measure. Again, no state-data items were retained in the final analysis.

Table 9. Final State-General Component Matrix

	Component
Item	1
State IT suspicion item 2	0.895
State IT suspicion item 3	0.870
State IT suspicion item 4	0.873
State IT suspicion item 7	0.894
State IT suspicion item 8	0.798

Analysis of locus of control measure

An exploratory factor analysis of the locus of control measure, shown in Table 10, yielded four possible factors. Items 1, 5, 6, 7, and 8 loaded well on the first factor and explained 30.0% of the variance. Factors 2, 3, and 4 did not load well so they were removed from further analysis.

Table 10. Initial Locus of Control Component Matrix

	Component			
Item	1	2	3	4
Locus of control item 1	0.504	-0.686	-0.336	-0.027
Locus of control item 2	0.277	-0.353	0.481	0.615
Locus of control item 3	0.068	0.723	-0.353	0.392
Locus of control item 4	0.174	0.439	0.782	-0.028
Locus of control item 5	0.801	0.071	-0.034	-0.435
Locus of control item 6	0.682	-0.290	0.008	0.375
Locus of control item 7	0.537	0.495	-0.383	0.278
Locus of control item 8	0.799	0.240	0.189	-0.294

A second order factor analysis on the first component, shown in Table 11, yields one strong and one weak component. The strong component includes items 1, 5, 6, 7, and 8 and explained 46.7% of the variance. There was cross-loading between components for item 1 so it was removed from further analysis.

Table 11. Interim Locus of Control Component Matrix

	Component	
Item	1	2
Locus of control item 1	0.548	0.720
Locus of control item 5	0.823	-0.193
Locus of control item 6	0.665	0.428
Locus of control item 7	0.547	-0.337
Locus of control item 8	0.787	-0.427

A third order factor analysis on items 5, 6, 7, and 8, shown in Table 12, lists all four items loading under one factor with an Eigenvalue of 2.147, representing 53.7% of the variance, and a reliability coefficient alpha of .706. These four items were retained for the final analysis.

Table 12. Final Locus of Control Component Matrix

	Component
Item	1
Locus of control item 5	0.828
Locus of control item 6	0.606
Locus of control item 7	0.604
Locus of control item 8	0.854

Analysis of disposition to trust measure

As explained in Chapter 3, the disposition to trust measure was composed of two separate instruments that were intended to measure the same target construct. An exploratory factor analysis of the items, shown in Table 13, from these measures indicates two components, item numbers 1, 2, 3, 4, 5, 6, and 8 loading under one and item 7 on the second. Component one had an Eigenvalue of 4.949 and accounted for 61.8% of the variance, therefore item 7 was removed.

Table 13. Intial Disposition to Trust Component Matrix

	Component	
Item	1	2
Disposition to trust item 1	0.769	-0.559
Disposition to trust item 2	0.871	0.181
Disposition to trust item 3	0.790	-0.242
Disposition to trust item 4	0.848	0.235
Disposition to trust item 5	0.899	-0.101
Disposition to trust item 6	0.802	0.309
Disposition to trust item 7	0.610	0.648
Disposition to trust item 8	0.656	-0.439

A secondary factor analysis was accomplished on the remaining seven items. The results in Table 14 show one component representing 66.1% of the variance with an Eigenvalue of 4.631 and a coefficient alpha .911. Therefore, the seven items were retained for the final analysis.

Table 14. Final Disposition to Trust Component Matrix

	Component
Item	1
Disposition to trust item 1	0.817
Disposition to trust item 2	0.859
Disposition to trust item 3	0.808
Disposition to trust item 4	0.825
Disposition to trust item 5	0.903
Disposition to trust item 6	0.784
Disposition to trust item 8	0.678

Inter-measure correlations

Once the factor analysis and reliability testing were completed, the remaining items from the trait general, trait data, and state general portions of the IT suspicion measure were compared to the revised locus of control and disposition to trust measures. Results are shown in Table 15. Due to the low sample size, most of the analysis was insignificant. The correlation table does show one significant relationship, between revised locus of control and the general portion of the state suspicion measure, with a p-value of .0078. The -.576 correlation mirrors the multicollinearity expected in the literature review, without being so large as to indicate the locus of control and state-general measures represent the same phenomena. No other correlations had a p-value less than .05. However, another result of interest is the lack of a substantial correlation between disposition to trust and any of the remaining suspicion measures, reinforcing the literature review statement that lack of trust and suspicion are indeed different.

Table 15. Inter-Measure Correlations

Measure	Revised trait general suspicion	Trait data suspcion	Revised state general suspicion	Revised locus of control	Revised disposition to trust
Revised trait general suspicion	α=.796				
Trait data suspicion	0.412	α=.774			
Revised state general suspicion	0.227	-0.044	α=.916		
Revised LOC	0.064	0.323	-0.576**	α=.706	
Revised disposition to trust	0.167	0.279	-0.169	0.222	α=.911

N=20 ** denotes correlation is significant at p<0.01 level.

V. Discussion and Conclusions

Discussion

The results of the IT suspicion factor analysis show the state and trait portions of the measure load on different factors, providing a level of confirmation that suspicion is composed of a state and trait component. This result provides strong validation that the literature review was correct in stating that suspicion has an enduring trait component as well as a situation-based state component that can be manipulated by outside factors. In addition, the analysis shows state and trait IT suspicion themselves are not single dimension constructs. The loading of general IT system and data specific items under different components in the factor analysis indicate suspicion of IT as a whole may be too broad an area to research. Suspicion of infrastructure, stored data, software, and other specific areas of IT and IT output may require more focused research. In addition, there are other factors that may contribute to IT suspicion, including knowledge of other individuals using the IT system, programming it, and supplying data. In order to gain a fuller understanding of the underlying mechanisms of IT suspicion, it appears more focused and bounded research is required to narrow IT suspicion down to more simplistic relationships then build it back up in a more complex, all-encompassing model with multiple dimensions. This analysis would require more factors and a much larger sample size in order to accomplish confirmatory factor analysis.

The factor analysis of the locus of control and disposition to trust measures had mixed results. The locus of control measure did not load as well as expected, although item reduction through factor analysis did yield a four item measure that met the requirements of the research methodology. A different locus of control measure may lead to better results in follow-on research. The combination of two disposition to trust measures yielded excellent results in the factor analysis. Only one item was removed because of cross-loading, and it still loaded well on the first factor.

With a sample size of 20, it was unrealistic to expect significant results from a correlation analysis of the individual measures in the IT suspicion survey. However, even though the sample size was small, analysis revealed a significant negative correlation between the state-general items and locus of control. Based on the literature review, this is an expected result. If locus of control is indeed defined as the degree to which individuals believe they control their own fate (Robbins and Judge, 2008) and those who have a high locus of control tend to be less suspicious (Robbins and Judge, 2008), one might expect a negative correlation between locus of control and all suspicion. However, the sample size is small, and it would take a very strong relationship for this to surface in this analysis. Individuals who don't believe they control their lives (low locus of control) tend to be more suspicious (Robbins and Judge, 2008) and should therefore be more sensitive to changes in normal activities and procedures. Since the state suspicion measure was primed with a manipulation of computer control panel presets used by most individuals, the strongest correlation for locus of control should theoretically be with state suspicion, and it should be negative.

There were no significant correlations between the different suspicion components of the IT suspicion measure. The final state-general suspicion had almost no correlation with either of the trait suspicion components. However, the two trait components were correlated (.412). These relationships were not significant but they do provide additional evidence to support a fundamental difference between state and trait suspicion. As state in Chapter 4, the lack of correlation between any of the suspicion measures and disposition to trust also provides validation to the assertion that suspicion and trust do indeed measure different phenomena.

There does appear to be an oversight in the literature review. The definition of IT suspicion states that an IT system's behavior will negatively impact the user's desired task. However, basic security measures can impede a user's task and not arouse suspicion. They are, in fact, expected. A revised definition might read:

User perceptions that the direction, duration, and intensity of an IT system's unexpected behavior will negatively impact their task.

Implications

There are many potential uses for a validated IT suspicion measure. It can be used by human resources in a couple of different ways to determine the proper job fit for a particular employee. It can also be used to IT systems and software before implementation. Proper use of the IT suspicion measure comes down to pre-determining the appropriate level of suspicion desired for a particular situation.

Determining the best personality for a job ahead of time could be one of the uses of an IT suspicion measure. A locus of control and trait IT suspicion measure or a locus of control and state measure with a job specific manipulation could be administered prior to job placement in career fields that are heavily reliant on information technology. Examples of use could be when hiring IT related equipment operators or network security employees. It would be desirable that the IT equipment operator (a pilot, for instance) have low suspicion of the IT systems the job required, especially since this research's definition of suspicion is based on expectation of negative task impact. It may, however, be more desirable for someone in information and network security to be more suspicious. The level of IT suspicion should fit the IT related job.

Not only can an IT suspicion measure be used to fit an employee to an IT system, it can be used to test a new IT system with existing employees. If a company wanted to run a test on a database management system or something else IT related that would be shared between multiple organizations, an IT suspicion measure could prove to be a valuable part of the testing process. Possibly administered with a satisfaction survey, an IT suspicion measure tailored to the particular IT system could be used to determine the suspicion of that IT system. If it is too high, the employees may be hesitant to use the system and it could affect productivity. This could also be an analysis technique of existing technology, created to determine why an IT system isn't used to its maximum capability. Specific suspicions could be determined in order to facilitate system improvement or training efforts that would increase system usage, security, or efficiency.

Limitations

There are several limitations that may have affected the results of this research effort. The small sample size clearly affected the significance of the analysis, although one major relationship, locus of control and state suspicion, was still observed. A much larger sample size would definitely expose the presence of weaker but still significant relationships between state suspicion, trait suspicion, locus of control, and disposition to trust. It would also allow for confirmatory factor analysis as part of a more thorough validation process.

Another dominant limitation to this analysis was the test subjects were aware that IT suspicion was the general topic of the research. This creates demand characteristics that possibly biased the results. Test subjects should be unaware of the topic in the future to avoid demand characteristics.

The delays and problems associated with the computer procurement and a fixed end-date to the research effort led to the third limitation. A complex and effective yet subtle manipulation intended to induce a level of suspicion that was real but undetectable to the test subject was not created. The timeline did not allow for one to be generated using outside help. The manipulation substituted in its place included simplistic alterations to the control panel presets to the mouse and cursor, which would impede use. This did achieve a level doubt in computer performance, but it was also overt in nature.

Lack of equalization of treatments was the final significant limitation. The measure was administered to different size groups in different locations. While they were instructed not to talk to each other while taking the IT suspicion measure, test subject group members new each other and the groups were as large as five participants. There was limited talking and other non-verbal forms of communication that could have biased results. In an ideal situation, the test subjects would have participated in a controlled environment, by themselves so as to be isolated from outside influence.

Future research

As the analysis explains, there appears to be multiple dimensions to IT suspicion, and further research could help explain the multiple relationships within the construct of IT suspicion. Further review of the literatures of suspicion, trust, locus of control, and IT will help to better define the mechanisms behind these constructs. Once complete, a methodology of study for these more focused relationships can be created and tested. All future analysis should contain an adequate sample size with preliminary testing before factor analysis on the measure is accomplished. The testing should indicate if the data is adequate for factor analysis and include: inter-item correlation matrix review similar to the analysis of this research; off-diagonal review of the anti-image covariance matrix searching for low correlations; Bartlett’s test of sphericity; and Kaiser-Meyer-Olkin measure of sampling adequacy (Hair et al., 1995).

For example, the analysis shows a strong relationship between locus of control and IT state suspicion and the literature supports a relationship between both IT trait and state suspicion and locus of control. Creating a model of the relationship between the three concepts when a stimulus is introduced appears to be a valid avenue of research. A revised measure could be created to test the model, using a much larger sample size than this research in order to achieve significant results.

A revised version of the existing measure could also be tested across different cultures. This would allow researchers to test and see the level of IT suspicion structural invariance. Testing nationalities outside of the United States would provide interesting results for use in areas such as psychological operations and information warfare, or something as simple as advertising. Comparing civilian and military subjects may help aid in the study and understanding of military culture and assist in recruitment and retention.

In addition to adding greater depth into the previously explored areas of suspicion literature, adding breadth to the literature review by researching social engineering could provide vital understanding of the mechanisms of IT suspicion. This research viewed IT as a stand-alone domain, disregarding what specific part of the IT system made the user suspicious. That was intentional, in order to achieve a high-level picture of IT suspicion. The social engineering literature may provide a better understanding of what a user is suspicious of and what mechanisms activate a detectable level of suspicion. This could assist in creating a holistic, multi-dimensional view of IT suspicion, specifically as it relates to refining the concepts of data and general IT suspicion under the state and trait domains. The system user’s focus of suspicion needs to be determined, whether it is at the software, at the hardware, or at the idea that an individual is maliciously manipulating the IT system.

A main factor in any future research should be increasing the sample size and number of items. This will help increase the significance. The test subjects should also come from a less focused group (Air Force company grade officers) in order to increase generalizability of the resulting construct.

Appendix A: Existing Construct Measures

Generalized Communication Suspicion (Levine and McCornack, 1991)

1. Everyone lies, the person who says they don't is the biggest liar of all.
2. I often feel as if people aren't being completely truthful with me.
3. Most often people only tell you what they think you want to hear.
4. When I am in a conversation with someone, I frequently wonder whether they are really telling me the truth.
5. People rarely tell you what they're really thinking.
6. The best policy is to trust people until proven wrong.
7. Dishonesty is part of human nature.
8. When I first meet someone, I assume they are probably lying to me about some things.
9. Most people are basically honest.
10. Anyone who completely trusts someone else is asking for trouble.
11. When I ask a stranger for directions, I frequently wonder whether they are being truthful.
12. When I am talking to others, I tend to believe what they say.
13. People seldom lie to me.
14. Most people follow the saying "honesty is the best policy."

Trust-Suspicion (Heretick, 1981)

1. I think most people would lie to get ahead.
2. Most people will use somewhat unfair means to gain a profit or an advantage rather than lose the advantage.
3. I commonly wonder what hidden reasons another person may have for doing something nice for me.
4. It is safer to trust nobody.
5. Most people inwardly dislike putting themselves out to help other people.
6. I tend to place a great deal of trust in other people and have seldom been disappointed.

Five questions of the suspiciousness index (Edelman, 1970)

1. What was the purpose of this experiment?
2. Did you notice anything unusual about this experiment? If so, what?
3. Do you feel this experiment was deceptive (involved lying) in any way? If so, how?
4. Do you have any reservations or doubts about the intelligence test you took? If so, what?
5. Do you think the experimenter was lying to you about the average scores on the intelligence test?

Two question perceived suspicion measure (Stiff et al, 1992)

1. I was highly concerned about whether my interview partner was responding truthfully.
2. I was very suspicious about what my partner was saying during the interview.

Appendix B: Student Responses to Item Request

Respondent 1
I personally know the source of the message.
I am confident that the sender is who he/she says they are.
I believe that the message was tampered with between sender and receiver.
I believe that the message is in the proper (or intended) graphical format.

Respondent 2
1) Do you ever notice anything unfamiliar about your desktop or the way a plug-n-play device is acting?
2) If there is a patch pushed out during the evening (i.e. Windows or DoD update), do you ever notice any changes in normal operability from the day before? Do you notice a change in your desktop or toolbar?
3) Are there ever times when your internet communications slows to the point where you feel something might be effecting you computer?
4) How many times a week do you avoid certain programs/files/e-mails because you aren't sure of what they will do to your computer?

Respondent 3
On a scale of 1 to 5 where 1 = always distrust, 2 = usually distrust, 3 = neither trust nor distrust, 4 = usually trust, and 5 = always trust, please respond to the following statements:

1. I _______________ that my email messages are received by the intended recipients.
2. I _______________ that I can access all my documents that are stored on my computer whenever I need to.
3. I _______________ that I can access all my files that are stored on the network whenever I need to.
4. I _______________ that my password is protected when I use it to access various websites (i.e. MyPay, online banking, etc).
5. I _______________ that no one has access to my email except for me and those I give permission to have access (i.e. USAF monitoring policy).

Respondent 4
Is my private information being shared when I am unaware?
Is it going to the wrong people?
Is my IP being stored to track my movement through the web?
Am I going to get spam mail if they ask for my e-mail address or do I even need to input it to get spam?
How do I know I won't get a virus from this?

Appendix C: IT Suspicion Survey

SURVEY NUMBER _____

①	②	③	④	⑤
Disagree Very Much	**Disagree Slightly**	**Neither Agree or Disagree**	**Agree Slightly**	**Agree Very Much**

1.	Whether or not I get to be a leader depends mostly on my ability.	①	②	③	④	⑤
2.	Whether or not I get into a car accident depends mostly on how good a driver I am.	①	②	③	④	⑤
3.	When I make plans, I am almost certain to make them work.	①	②	③	④	⑤
4.	How many friends I have depends on how nice a person I am.	①	②	③	④	⑤
5.	I can pretty much determine what will happen in my life.	①	②	③	④	⑤
6.	I am usually able to protect my personal interests.	①	②	③	④	⑤
7.	When I get what I want, it’s usually because I worked hard for it.	①	②	③	④	⑤
8.	My life is determined by my own actions.	①	②	③	④	⑤
9.	I am the sort of person who generally tends to trust others.	①	②	③	④	⑤
10.	I am the sort of person who generally tends to believe that others have good intentions.	①	②	③	④	⑤
11.	I am the sort of person who generally tends to trust what people say.	①	②	③	④	⑤
12.	I am the sort of person who generally tends to believe that people are basically moral.	①	②	③	④	⑤
13.	I am the sort of person who generally tends to believe in human goodness.	①	②	③	④	⑤
14.	I generally have faith in humanity.	①	②	③	④	⑤
15.	I feel that people are generally reliable.	①	②	③	④	⑤
16.	I generally trust other people unless they give me reason not to.	①	②	③	④	⑤

SURVEY NUMBER _____

①	②	③	④	⑤
Disagree Very Much	**Disagree Slightly**	**Neither Agree or Disagree**	**Agree Slightly**	**Agree Very Much**

1.	I feel that IT systems I use provide valid information.	①	②	③	④	⑤
2.	Computers never lie.	①	②	③	④	⑤
3.	The best policy is to trust an IT system until proven wrong.	①	②	③	④	⑤
4.	When using my IT system, I always believe what is presented.	①	②	③	④	⑤
5.	The output of most IT systems is valid.	①	②	③	④	⑤
6.	I always trust the data that my IT systems provide.	①	②	③	④	⑤
7.	I believe I have full access to all data stored locally on my computer.	①	②	③	④	⑤
8.	I believe I have full access to all data stored on the network.	①	②	③	④	⑤
9.	I always have complete confidence in the integrity of my computer data.	①	②	③	④	⑤

STOP! WAIT FOR INSTRUCTIONS

Next, complete the following exercise.

Step 1. Open Microsoft Word on the laptop provided to you and write a paragraph explaining your entire work schedule for today, briefly summarizing all planned activities. Once complete, please run spell check. Create a folder on the desktop named the 2-digit number on your survey and save the document as your 2-digit number*.doc.*

Step 2. Open Microsoft Excel and create a table summarizing your entire duty day schedule to embed at the end of the word document. Save as your 2-digit number.xls or xlsx in the same folder and insert the table into the Word file, resaving the Word file.

Note: AFIT/SC has certified that each of these machines is running correctly. No changes to the computers attributes are necessary or allowed.

STOP! WAIT FOR INSTRUCTIONS

SURVEY NUMBER _____

① **Disagree Very Much**	② **Disagree Slightly**	③ **Neither Agree or Disagree**	④ **Agree Slightly**	⑤ **Agree Very Much**

1.	I have complete confidence in the integrity of the data stored on this computer.	①	②	③	④	⑤
2.	I noticed no unusual behaviors.	①	②	③	④	⑤
3.	I was never concerned about whether my computer was working properly.	①	②	③	④	⑤
4.	I noticed no unfamiliar behaviors.	①	②	③	④	⑤
5.	The output of the computer was valid.	①	②	③	④	⑤
6.	I believe I have full access to all data stored locally on this computer.	①	②	③	④	⑤
7.	My computer was acting normally.	①	②	③	④	⑤
8.	The software on this computer is operated the way I expected.	①	②	③	④	⑤
9.	I was not suspicions about what my computer was presenting to me.	①	②	③	④	⑤

References

Arnau, R. C. Second-order factor analysis: Methods and interpretation. New Orleans, LA April 11, 1998.

Bacharach, S. (1989). Organizational theories: Some criteria for evaluation. *Acadamy of Management Review*, *14*(4), 496-515.

Barki, H. (2008). Thar's gold in them thar constructs. *The DATA BASE for Advancements in Information Systems*, *39*(3), 9-20.

Burgoon, J. K., Buller, D. B., Ebesu, A. S., White, C. H., & Rockwell, P. A. (1996). Testing interpersonal deception theory: Effects of suspicion on communication behaviors and perceptions. *Communication Theory, 6*(3), 243-267.

Caso, L., Maricchiolo, F., Bonaiuto, M., Vrij, A., & Mann, S. (2006). The impact of deception and suspicion on different hand movements. *Journal of Nonverbal Behavior, 30*(1), 1-19.

Edelman, R. I. (1970). Some variables affecting suspicion of deception. *Journal of Personality and Social Psychology, 15*(4), 333-&.

Fein, S. (1996). Effects of suspicion on attributional thinking and the correspondence bias. *Journal of Personality and Social Psychology, 70*(6), 1164-1184.

Hair, J. F.; Anderson, R. E.; Tatham, R. L.; and William C. Black, W. C. *Multivariate Analysis*, 5th ed., Prentice-Hall, Englewood Cliffs, NJ, 1998.

Henderson, S. J. (2007). *The dark visitor: Inside the world of chinese hackers* Lulu.

Heretick, D. M. L. (1984). Trust-suspicion and gender differences in interpersonal functioning. *Journal of Research in Personality, 18*(1), 27-40.

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questions. In *Organizational research methods, vol. 1, no. 1* (pp. 104-121). Thousand Oaks, CA: Sage Publications, Inc.

Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. *Journal of Management, 21*(5), 967-998.

Hoffman, A. M. (2007). The structural causes of trusting relationships: Why rivals do not overcome suspicion step by step. *Political Science Quarterly, 122*(2), 287-312.

Judge, T. A., Erez, A., Bono, J. E., & & Thoresen, C. J. (2003). The core self-evaluations scale: Development of a measure. *Personnel Psychology, 56*, 303-331.

Levenson, H. (1981). Differentiating among internality, powerful others and chance. In H. M. Lefcourt (Ed.), *Research with the locus of control* (pp. 15-63). New York: Acedemic Press, Inc.

Levine, T. R., & & McCornack, S. A. (1991). The dark side of trust: Conceptualizing and measuring types of communicative suspicion. *Communication Quarterly, 39*(4), 325-340.

Lewicki, R. J., McAllister, D. J., & & Bies, R. J. (1998). Trust and distrust: New relationships and realities. *Acadamy of Management Review, 23*(3), 438-458.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *Journal of Strategic Information Systems, 17*(1), 39-71.

Locke, E. A. (2003). Good definitions: The epistemological foundation of scientific progress. In J. Greenberg (Ed.), *Organizational behavior: The state of the science* (pp. 415-444). Manwah, NJ: Lawrence Erlbaum.

McKnight, H. D., Choudhury, V., & & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *Journal of Strategic Information Systems, 11*, 297-323.

Pinder, C. C. (1998). *Work motivation in organizational behavior*. Upper Saddle River, NJ: Prentice-Hall.

Pipkin, D. L. (2000). *Information security*. Upper Saddle River, NJ: Prentice-Hall.

Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antcedents and effects of trust in virtual communities. *Journal of Strategic Information Systems, 11*, 271-295.

Robbins, S., & & Judge, T. (2008). *Essentials of organizational behavior* (9th ed.). NJ: Pearson/Prentice-Hall.

Rodgers, R., & Deng, M. The role of trust in the reciprocal exchange process: Evidence from china. New Orleans, LA August 6-11, 2004.

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

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & & Camerer, C. (1998). Not so different after all: A crossdiscipline view of trust. *Acadamy of Management Review, 23*(3), 393-404.

Stiff, J. B., Kim, H. J., & Ramesh, C. N. (1992). Truth biases and aroused suspicion in relational deception. *Communication Research, 19*(3), 326-345.

Stricker, L. J., Messick, S., & Jackson, D. N. (1967). Suspicion of deception - implications for conformity research. *Journal of Personality and Social Psychology, 5*(4), 379-&.

Vita

Biographical Sketch

Capt Matthew T. Olson is a 1995 graduate of Moline High School in Moline Illinois. After attaining a Bachelor of Science degree in Mechanical Engineering from the University of Illinois at Urbana/Champaign in 2000, he attended Air Force Officer Training School at Maxwell AFB, AL and commissioned as a Second Lieutenant in May of 2001.

Capt Olson's Air Force assignments include Whiteman AFB, MO and Seymour Johnson AFB, NC where he worked as Deputy Chief of Environmental, Chief of Plans and Programs, Chief of Maintenance Engineering, and Readiness Flight Officer. He also served in two deployments, one each to Kuwait and Qatar, working as Chief of Maintenance Engineering and Design Engineer. In August of 2007 he entered the Graduate School of Engineering and Management at the Air Force Institute of Technology. Upon graduation he will be assigned to the 62nd Civil Engineer Squadron at McChord AFB, WA as the Operations Flight Chief.

Education

Master of Science, Engineering Management, Air Force Institute of Technology, Wright-Patterson AFB, OH. Master's Thesis: The Development of IT Suspicion as a Construct and Subsequent Measure. Chair: Lt Col. Alex Barelka. In progress. Expected graduation date: March 2009.

Bachelor of Science, Mechanical Engineering, The University of Illinois at Urbana/Champaign, May 2000.

SF 298

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)* March 2009	2. REPORT TYPE Master's Thesis	3. DATES COVERED *(From – To)* July 2008-March2009

4. TITLE AND SUBTITLE The Development of IT Suspicion as a Construct and Subsequent Measure	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Olson, Matthew T., Capt, USAF	5d. PROJECT NUMBER JON#09-150
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765	8. PERFORMING ORGANIZATION REPORT NUMBER AFIT/GEM/ENV/09-M15
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

Suspicion has not been studied in great depth; however, a conceptual understanding of suspicion is no less important than many of the other highly studied constructs related to healthy working relationships. Information technology (IT) is one area where suspicion study is lacking, and this research effort was a study into the specific domain of IT suspicion.

An extensive study of the suspicion literature and the suspicion nomological net as well as informal surveys of the general populous and subject matter experts were used to create an IT suspicion conceptual definition and measure. In order to test IT suspicion's relationships with other more established constructs a survey was created. The final pilot study consisted of two measures from suspicions nomological net, locus of control and disposition to trust, a trait IT suspicion measure, a manipulation exercise on a laptop computer intended to induce suspicion, and finally a state suspicion measure.

Analysis indicated IT suspicion is a multi-dimensional construct, with independent state and trait properties. It also has separate dimensions within the state and trait components. Comparisons between the components of the IT suspicion construct and related measures indicated a negative correlation between state suspicion and locus of control.

15. SUBJECT TERMS
Suspicion, Information technology, Trust, Construct

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Alexander J. Barelka , AFIT/ENV
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U	UU	61	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636 (Ext 7404)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18

	Form Approved *OMB No. 074-0188*