Modeling Insider Threat Types in Cyber Organizations

Eunice E. Santos[a,c], Eugene Santos Jr. [b,d], John Korah [a,e], Jeremy E. Thompson [b], Vairavan Murugappan[a], Suresh Subramanian[a], Yan Zhao[b]

[c]Ron Hochsprung Endowed Chair & Professor
[e]Research Assistant Professor
[a]Department of Computer Science,
Illinois Institute of Technology, Chicago, IL, USA
Phone: (312) 567-5150 Fax: (312) 567-5067
Email: {eunice.santos, john.korah}@iit.edu, {vmuruga1, ssubra20}@hawk.iit.edu

[d]Professor of Engineering
[b]Thayer School of Engineering
Dartmouth College, Hanover, NH, USA
Phone: (603) 646-6490 Fax: (603) 646-2277
Email: {eugene.santos.jr, jeremy.e.thompson.th, yan.zhao.th}@dartmouth.edu

***Abstract*— Insider threats can cause immense damage to organizations of different types, including government, corporate, and non-profit organizations. Being an insider, however, does not necessarily equate to being a threat. Effectively identifying valid threats, and assessing the type of threat an insider presents, remain difficult challenges. In this work, we propose a novel breakdown of eight insider threat types, identified by using three insider traits: predictability, susceptibility, and awareness. In addition to presenting this framework for insider threat types, we implement a computational model to demonstrate the viability of our framework with synthetic scenarios devised after reviewing real world insider threat case studies. The results yield useful insights into how further investigation might proceed to reveal how best to gauge predictability, susceptibility, and awareness, and precisely how they relate to the eight insider types.**

Keywords— Bayesian knowledge bases (BKBs); insider threat; computational modeling; behavioral modeling; social modeling; trust; manipulation; cyber security

I. Introduction

Immense damage can be caused by individuals who are an integral part of an organization but work against its interests, commonly known as insider threats. Such insider threats can cause enormous damage, as they typically have access to critical and confidential information. They may also have access to information about security precautions taken by the organization and therefore are more adept at circumventing them. However, not all insiders, defined as "a person who belongs to a group or organization and has special knowledge about it,"[1] become actual insider threats. Thus, striking a balance between allowing insiders sufficient freedom to function efficiently while providing adequate protections for the organization is a challenge.

In this paper, we present a computational framework to model insiders using relevant social, cultural, emotional, and other behavioral factors, along with technological factors, with the goal of categorizing them based on the type of threat they are likely to present to the organization. It is our view that establishing trust and avoiding suspicion are essential to insider exploitation and manipulation, and thus guide our focus for understanding the insider threat. Our primary objective is therefore to develop a modeling framework for insider behavior that accounts for and explains the social, cultural, and emotional basis for trust and suspicion, and especially its impacts on the insider threat. An insider is subject to influences, motivations, abilities, beliefs, strengths, and weaknesses. Understanding what factors affect an insider, and how they can be exploited, is essential for identifying potential insider threats within our organizations. By placing ourselves in the roles of outsiders desiring to find insiders who might be manipulated into betraying their organization, even unwittingly, we strove to identify factors which would indicate potential insider threats. We hypothesize that there exist eight distinct insider threat types, and that those types may be identified through the measurement of three important individual qualities: predictability, susceptibility, and awareness (PSA). In this paper, we discuss our initial efforts to translate that hypothesis into a computational model of insider threat types. In the following sections, we provide a brief introduction to the PSA modeling framework, as well as present its relevancy to insider behavior. We also describe our efforts to computationally model the three components of PSA using an initial set of factors and behaviors.

II. PSA MODELING FRAMEWORK

Using the PSA computational modeling framework, we propose to evaluate insiders to determine their potential threat types, to better inform what conditions and possible manipulations might trigger malicious behaviors, and then also to factor in dynamic information which could sway the type assessment as situations evolve. In our framework, insiders are categorized based on three key qualities which were found to be particularly relevant for identifying types of insider threat. These qualities, namely predictability, susceptibility and awareness, are defined as follows:

[1] Source: *Merriam-Webster.com*

This work is sponsored by the US Air Force Office of Scientific Research under grant #FA9550-12-1-0457. Opinions, interpretations, recommendations and conclusions are those of the authors and are not necessarily endorsed by the United States Government.

- An insider's predictability is based on the ability to foretell that insider's reactions to events, and to other stimuli, to which he or she is exposed.
- An insider's susceptibility is the quality or tendency of that insider to become involved in an action that either directly or indirectly affects the organization, due to external or internal manipulative influence.
- An insider's awareness is the insider's ability to detect manipulative intent behind false and/or partial information.

We suggest that these qualities represent aspects that are relatively static and unchanging for an individual—the insider's character or nature, which predisposes them towards different levels of PSA, and therefore towards a potential insider threat type. This aspect we believe can be captured through the measure of certain traits and behaviors. For example, someone with a methodical personality might prove to be predictable, while another with a predilection for addictive substances, such as alcohol, might have susceptibilities which could be exploited. We further recognized, though, that there are more dynamic aspects of PSA affected by less constant factors, e.g. emotion, context, and significant events. For instance, emotions could affect predictability, susceptibility, or awareness. We created synthetic scenarios reflective of realistic situations to study how the different aspects of PSA might present themselves in real-world situations, and how an insider type could potentially be determined. The objectives here were twofold: 1) to better understand the proposed PSA framework to insider type correlation, and 2) to determine if it is reasonable to expect to detect such a correlation in insider scenarios.

In order to accomplish this, a study of known instances of insider behaviors was undertaken. Related to this study of insider cases, an examination of the common indicators found in these cases was conducted. Additionally, a survey of existing measurement tools for personality and indicators was initiated. Finally, initial definitions of PSA and each insider type were drafted, and then related to the synthetic scenarios.

Note that the PSA profile of an insider may change over time, as more information is gathered and as the insider is exposed to new events and circumstances. It is important to note that the PSA framework is hypothesized to be an indicator of potential insider threat type. The emphasis on the term potential is critical, as it is not suggested that insiders with a particular PSA profile will necessarily commit destructive insider actions, but only that if they do at some point become malicious insiders, they are likely to exhibit behaviors according to their PSA type. While the linkage between PSA and insider types is hypothesized (indicated in Table I), details such as the exact nature of those connections, the ability to measure the PSA of subjects, how identifiable is each type of insider, and even the extent to which these connections actually exist, remain to be determined. In this initial foray, the PSA concept's existence and measurability are assumed, while making deductions and inferences about the PSA of individuals in synthetic scenarios is explored, with the aim of determining the viability of PSA as a means for establishing potential insider types.

TABLE I: THE THREE DIMENSIONS OF AN INSIDER BEHAVIOR AND POTENTIAL INSIDER THREAT TYPE

Predictable?	Susceptible?	Aware?	Potential Insider Threat Type
No	No	No	Manipulatable (m)
Yes	No	No	Anticipated + (m)
No	Yes	No	Compromised + (m)
Yes	Yes	No	Marionette
No	No	Yes	Safe/Trusted
Yes	No	Yes	Co-opted*
No	Yes	Yes	Disinformed*
Yes	Yes	Yes	Traitor*
			(*) denotes exceptional cases especially with aware insiders

III. MODELING PREDICTABILITY, SUSCEPTIBILITY AND AWARENESS

To formulate the initial models for measuring the predictability, susceptibility, and awareness of insiders, we leveraged our previous work in socio-cultural modeling [1], [2], including our work on infusing cultural and behavioral factors in social network models [3].

A. Bayesian Knowledge Bases

In order to overcome the data challenges in this domain, that is, the incompleteness of available data and the inherent uncertainty of human behaviors, we employ a probabilistic reasoning networks called Bayesian Knowledge Bases (BKBs) [4]. BKBs provide the ability to represent the uncertainty of behaviors in the form of if-then rules, using conditional probabilities. We can represent fine-grained behaviors of individuals and groups in a cyber organization by breaking them down into three types of components, those being the beliefs, goals, and actions of the insider(s). These components can be represented as random variables in BKBs. Multiple BKBs, where each BKB represent a specific behavior of an insider, can be combined using a fusing algorithm [5] to represent the overall complex behaviors of the insider. BKBs also allow for posterior analysis, which we leverage to provide quantitative measures for an insider's predictability, susceptibility, and awareness. In this work, we validated the PSA modeling framework by developing initial models (described in the subsection below) that also demonstrate how relevant complex insider behaviors can be modeled using BKBs. The probabilities used within the BKBs were derived from multiple sources by graduate students acting in the capacity of subject matter experts. While the precise results derived from the BKBs are of course sensitive to the probabilities found within, the analysis and trends exemplify the capabilities of such a model, and would only improve with more accurate probability determination. Sample BKBs can be found in Fig. 1, Fig. 2, and Fig. 3.

B. Initial Models for Predictability, Susceptibility and Awareness

In order to devise a general method to measure an individual's predictability, we investigated the prospect of using bias as an indicator of predictability. Bias can be described as an inclination or prejudice towards or against a

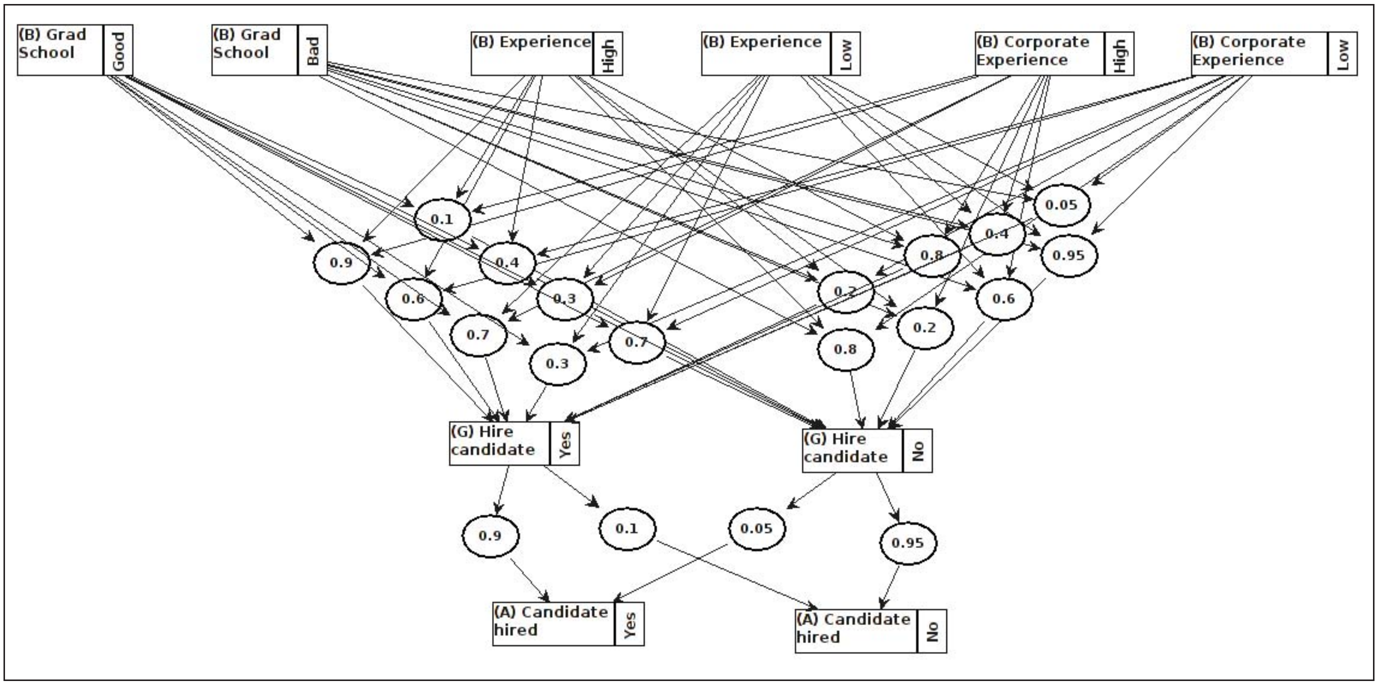

Fig. 1: Predictability baseline BKB

person, entity, or idea [6]. For the initial model of insider predictability, we examined the following four categories of biases. Socio-cultural biases are inherent biases that arise from personal attributes such as age, gender, education, etc. Biases that are based on the emotional state of the insider, such as being happy, sad, or anxious, are classified as emotional biases. Situational biases are those invoked by external events or stimuli. Social network based biases are those invoked by the insider's preference towards certain groups or organizations. The factors relevant to the above-mentioned biases are represented using Bayesian knowledge bases (BKBs). See Fig. 1 for an example BKB used in the predictability model. A measure for predictability was defined using posterior analysis obtained from belief updating and related standard deviations. We theorize that the larger the deviation, the greater the predictability of the outcome. Intuitively, decisions with a small deviation in the possible outcomes are more difficult to predict, as a small change in conditions can quickly alter the likely outcome. Decisions with a larger deviation could indicate a more reliable ability to distinguish between possible outcomes.

For susceptibility, we focused on factors based on an insider's vulnerabilities to bribery and deception [7]. These two vulnerabilities were selected due to their frequent appearance in our survey of case studies [8]. Manipulated insiders were frequently either overtly persuaded to perform malicious acts

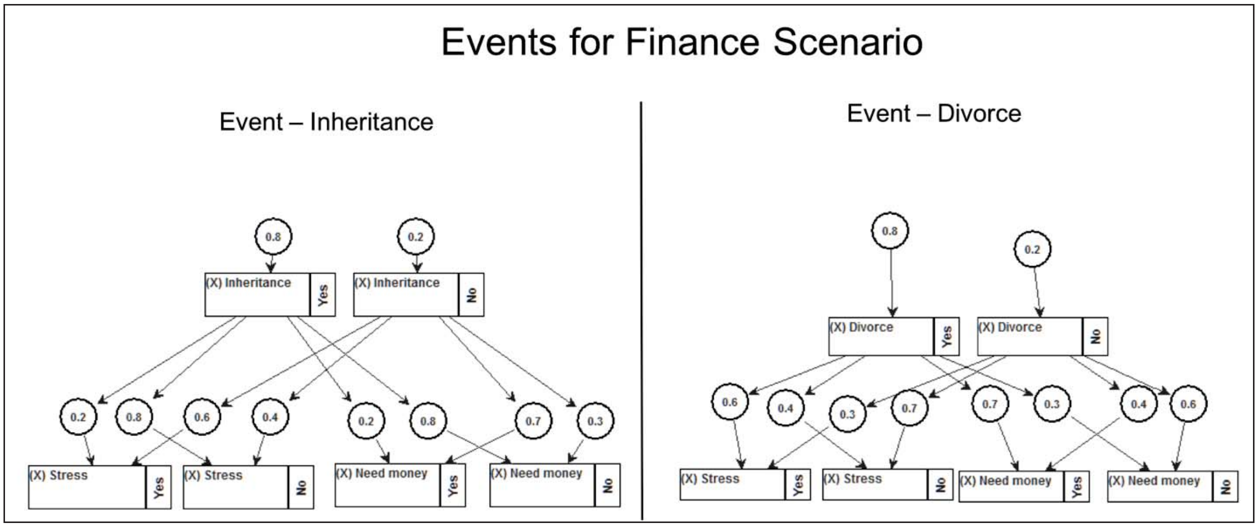

Fig. 2: Susceptibility event BKBs

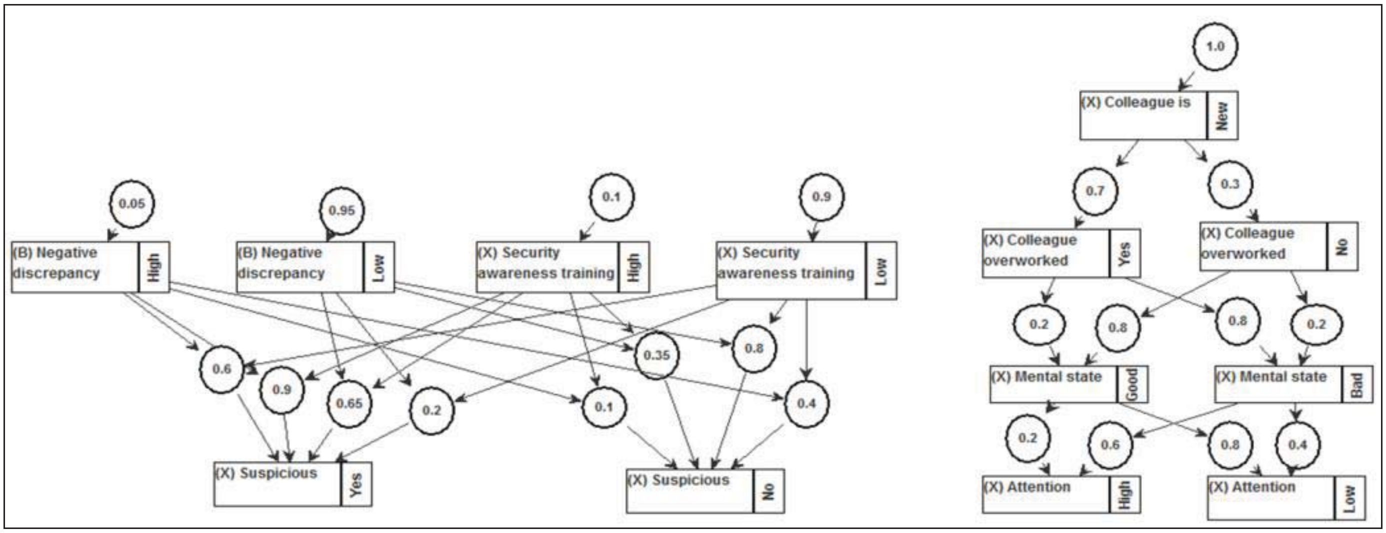

Fig. 3: Awareness Scenario 2 Event BKBs

through outright bribery[2], or were rather innocently co-opted into betrayal through deceit which they did not detect [9][3]. We formulated a method to generate quantitative measures of an insider's susceptibility to manipulation tactics using posterior analysis and provide insights into how the insider's susceptibility changes due to the influence of events. Some example event BKBs from the susceptibility model can be viewed in Fig. 2.

Finally, we concentrated on the variation in awareness of an insider under the influence of three manipulation techniques [10], specifically trust-based manipulation [11], empathy-based manipulation, and false identity-based manipulation [12]. Trust-based manipulation occurs between individuals who have close relationships, such as colleagues, family members, and friends. Due to this closeness, it is extremely difficult for victims to realize they are being manipulated. On the other hand, empathy-based manipulation typically targets strangers. The manipulator may invent a delicate situation and guilt the victim into helping. False identity-based manipulation commonly occurs during online interactions [13], where the manipulator's true identity is easily concealed. The manipulator may even masquerade as the victim's acquaintance by forging a false online profile [14]. The insiders' awareness of manipulation was represented in the model using BKBs (e.g. Fig. 3). Posterior analysis was then used to measure the three types of awareness, corresponding to the manipulation strategies described above.

IV. EXPERIMENTAL RESULTS

For experimental validation of the PSA framework, we designed synthetic scenarios to test the models for representing and measuring insider predictability, susceptibility, and awareness. We made use of synthetic scenarios so that we could better control for unknown factors and influences during this early stage of model development, with the expectation that more complex and realistic scenarios will be explored in the future. In order to investigate the efficacy of our modeling techniques in the cyber security domain, we utilized a three-level evaluation process, with increasing degrees of complexity to allow for better separation of influences and identification of trends. In Level 1, the models were tested against a single scenario, with analysis centered around a single random variable, designated as the target variable. Level 2 evaluation consisted of multiple scenarios and single target variable analysis, and single scenario and multiple target variable analysis. Level 3 evaluation provided more in-depth analysis by utilizing multiple target variables across multiple scenarios. Quantitative measures were calculated for each of the models described above to indicate the levels of predictability, susceptibility, and awareness.

A. Predictability

For predictability, due to the scarcity of real world data linking various forms of bias with insider behaviors, we formulated a generic scenario. This scenario focused on biases during job recruitment, to test our hypothesis that measurements of bias are reliable indicators of predictability as a character trait.

Specifically, we modeled a job recruiter's hiring bias based on candidates' schooling. Towards this end, we produced two synthetic scenarios to demonstrate our approach. The predictability levels for the scenario are described in *TABLE II*. In the BKBs constructed for this scenario, a random variable

TABLE II: PREDICTABILITY SCENARIO LEVELS

Level	Target 1 - Goal Hire Candidate (unbiased)	Target 2 - Action Candidate Hired (biased)
1	Scenario I: Grad of hiring official's alma mater	Scenario I: Grad of hiring official's alma mater
2a	Scenario I: Alma mater Scenario II: Not alma mater	Scenario I: Alma mater Scenario II: Not alma mater
2b	Scenario I: Alma mater	
3	Scenario I: Alma mater Scenario II: Not Alma mater	

[2] E.g. https://www.fbi.gov/history/famous-cases/aldrich-ames and https://www.fbi.gov/history/famous-cases/robert-hanssen

[3] E.g. https://archives.fbi.gov/archives/honolulu/press-releases/2013/defense-contractor-charged-in-hawaii-with-communicating-classified-information-to-person-not-entitled-to-receive-such-information

TABLE III: PREDICTABILITY RESULTS

Level	Scenario	Predictability Measure	
		Hire Goal (unbiased)	***Hired Action (biased)***
1	***I** (bias for)*	0.04668	0.004893
1	***II** (bias against)*	0.1600	0.01950
2a	***I & II***	0.1179	0.01421
2b	***I***	0.03319	
2b	***II***	0.1140	
3	***I & II***	0.08394	

representing the goal to hire a candidate represents the unbiased output of the hiring process, while an action random variable reflects the actual outcome of the situation, hired or not, once bias has been considered.

We hypothesized that bias introduces an unknown influence which results in less predictability, and thus would serve as a baseline measurement for predictability. After applying the calculations for predictability, Scenario I's results (*TABLE III*) revealed that the outcome was more predictable without bias, as we expected.

The Scenario II Level 1 calculations yielded markedly larger predictability scores when compared to Scenario I, though the biased variable predictability in Scenario II was indeed smaller than the unbiased variable. These mixed results caused us to realize that bias can indeed decrease predictability, when the bias is unknown and the outcome of the situation is otherwise predictable. Alternatively, when the outcome is borderline or unclear, and a known bias exists, an increase in predictability is possible. Thus, while our method for computing predictability remains promising, bias does not seem to be the consistent predictability indicator for which we were searching, but merely a complicating factor in predicting outcomes.

Level 3 results reinforced the previous observation. Based on these mixed results, we recognized that bias can either contribute to, or detract from, predictability, depending on the level of uncertainty of other factors, and the level of uncertainty with regards to the bias. We must therefore conclude that bias cannot be serve as a gauge for the predictability of a potential insider. Further study is required to isolate a measurable indicator of predictability as a character trait.

TABLE IV: SUSCEPTIBILITY SCENARIO LEVELS

Level	Target 1 - Susceptibility to bribery	Target 2 - Susceptibility to deception
1	***<u>Scenario 1: Finance</u>*** ***Event1***: Buys expensive car ***Event2***: Divorce ***Event3***: Inheritance	***<u>Scenario 2: Alcoholism</u>*** ***Event1***: Demoted (Long lunches and working while intoxicated) ***Event2***: Paranoid (Misconception and argument in social meeting) ***Event3***: Rehab
2a	***<u>Scenario 1 & 2: Finance & Alcoholism</u>*** (Events identical to Level 3)	***<u>Scenario 1 & 2: Finance & Alcoholism</u>*** (Events identical to Level 3)
2b	***<u>Scenario 1: Alcoholism</u>*** ***Event1***: Demoted ***Event2***: Paranoid ***Event3***: Rehab	
3	***<u>Scenario 1 & 2: Finance & Alcoholism</u>*** ***Event1***: Buys expensive car ***Event2***: Demoted ***Event3***: Divorce	***Event4***: Paranoid ***Event5***: Rehab ***Event6***: Inheritance

TABLE V: SUSCEPTIBILITY LEVEL 2A - MULTIPLE SCENARIOS AND SINGLE TARGET

Scenario – Finance and Alcoholism; Target – Susceptible to bribery or deception					
		Susceptible to bribery		**Susceptible to deception**	
	Events	***Yes***	***No***	***No***	***Yes***
1	***Buys Expensive Car***	0.4651	0.5349	0.5988	0.4012
2	***Demoted***	0.4893	0.5107	0.6229	0.3771
3	***Divorce***	0.5116	0.4884	0.6357	0.3643
4	***Paranoid***	0.5161	0.4839	0.6402	0.3598
5	***Rehab***	0.5151	0.4849	0.5906	0.4094
6	***Inheritance***	0.4838	0.5162	0.5895	0.4105

B. Susceptibility

In evaluating the susceptibility model, we developed a synthetic scenario, influenced by the Aldrich Ames episode[4], with a focus on susceptibilities exploited through bribery and deception (see *TABLE IV*). Overall, the susceptibility results were positive. In Level 1, in which we used a single scenario to model a single target outcome, we found that the Finance Scenario revealed that Events 1 and 2 heightened the subject's need for money, and thus increased his "*Susceptibility to bribery"*. In contrast, the inheritance in Event 3 decreased his need for money and therefore reduced his susceptibility. In the Alcoholism Scenario of Level 1, Events 1 and 2 increased the insider's "*Susceptibility to deception"* because of his alcoholism and threat indicators, while Event 3 decreased his alcohol dependency, and therefore reduced his susceptibility.

TABLE V provides the results of Level 2a, where multiple scenarios (Finance and Alcoholism) are modeled together to predict a single outcome (bribery or deception), while *TABLE VI* contains Level 2b results, modeling a single scenario (Alcoholism) to predict the outcome of multiple targets. Though these events do not contribute directly towards the "*Susceptibility to bribery"*, they influence the insider's threat level [15] due to Event 1 (demotion causing disgruntlement towards the organization), which in turn affects his "*Susceptibility to bribery"*. Hence the trend is common for both susceptibility values.

TABLE VI: SUSCEPTIBILITY LEVEL 2B - SINGLE SCENARIO AND MULTIPLE TARGETS

Scenario – Alcoholism; Target – Susceptible to bribery and deception					
		Susceptible to bribery		**Susceptible to deception**	
	Events	***Yes***	***No***	***Yes***	***No***
1	***Demoted***	0.4959	0.5041	0.6229	0.3771
2	***Paranoid***	0.5091	0.4909	0.6361	0.3639
3	***Rehab***	0.5091	0.4909	0.5864	0.4136

[4] http://fas.org/irp/congress/1994_rpt/ssci_ames.htm

TABLE VII: SUSCEPTIBILITY LEVEL 3 - MULTIPLE SCENARIOS AND MULTIPLE TARGETS

Scenario – Finance and Alcoholism; Target – Susceptible to bribery and deception					
		Susceptible to bribery		**Susceptible to deception**	
	Events	***Yes***	***No***	***Yes***	***No***
1	***Buys Expensive Car***	0.4651	0.5349	0.5988	0.4012
2	***Demoted***	0.4893	0.5107	0.6229	0.3771
3	***Divorce***	0.5116	0.4884	0.6357	0.3643
4	***Paranoid***	0.5161	0.4839	0.6402	0.3598
5	***Rehab***	0.5151	0.4849	0.5906	0.4094
6	***Inheritance***	0.4838	0.5162	0.5895	0.4105

TABLE VII provides the Level 3 analysis of the susceptibility of an insider. In the table, Events 1, 3, and 6 are from the *Finance Scenario*, and Events 2, 4, and 5 are from *Alcoholism Scenario*. Events 1 to 4 increase the insider's threat and *Susceptibility*, because of his increased need for money and alcohol dependencies. Events 4 and 5 reduce both those factors, as the values in the table show. This level shows how interactions between different layers of the model can be captured. The Level 3 results demonstrate how multiple scenarios can interact and subsequently influence multiple targets. This level shows the complete trend in the *Susceptibility* values across all scenarios whereas previous levels show a more fine-grained and selective view of the expected outcome.

C. *Awareness*

For evaluating the awareness model, we constructed scenarios (*TABLE VIII*) where an insider is exposed to trust-based manipulation by a romantic interest and is then subjected to a phishing attack. Using BKB posterior probability analysis, we analyzed the changes in the insider's awareness due to these manipulation strategies.

The awareness calculation results (*TABLE IX*) indicated that, for Scenario I, the victim's experience of being cheated on increased awareness to possible future manipulation, as would be expected. In Scenario II, due to a bad mental state and lack of training, the individual's awareness was decreased when compared with the average information technology worker, thus demonstrating the deleterious effect distractions can have on awareness. These results are in accordance with expectations, and encourage continued investigation of awareness as a factor in insider threat type.

TABLE VIII: AWARENESS SCENARIO DESCRIPTIONS

Scenario	Brief Description
I (trust)	– Dating a new flame, first online, then later in person – He spends a lot of money on her – Girlfriend deceives him and leaves him – He becomes more careful about online dating
II (identity)	– Hacker copies victim's Facebook profile – Hacker phishes victim's colleagues using victim's name – Hacker requests proprietary documents from colleagues – Hacker sells documents to other company

TABLE IX: AWARENESS SCENARIO RESULTS

Scenario	Baseline Awareness	Scenario Awareness	Net Awareness
I (trust)	0.4689	0.4899	+0.0210
II (identity)	0.5909	0.4304	-0.1605

V. Conclusion and Future Directions

Several case studies on insider threat scenarios reveal that many insiders show early threat indicators which can go unnoticed, or at least not acted upon. Initial results farom our model show how these threat indicators and emotions can be effectively utilized for gauging an insider's susceptibility. Moreover, our experiment revealed that an insider can be manipulated through several tactics based on those vulnerabilities. Our results show that having multiple levels of scope in the model aids predicting an insider's susceptibility to multiple tactics, in this case, susceptibility to bribery and deception. In general, we have gained insights into insider vulnerabilities, and how they could potentially be used for manipulation. Awareness of manipulation is determined by both long term and short term factors. Long term factors include experience, training, comprehension, communication skill, and personality, while short term factors consist of information overload, recent experience, and mental state. The same person usually has various levels of awareness to different types of manipulations, and this variation is influenced by social, economic, and cultural factors. Therefore, to improve a person's overall awareness of manipulation, it is recommended to identify his/her vulnerability to these factors. The proposed method provides an efficient relative measure of each person's awareness for different types of manipulations, and it captures both long term and short term factors impacting his or her awareness.

While not every experiment was fully successful, every experiment did yield important insights into how further research might best proceed. For example, the key insight gained from the predictability scenario analysis is that bias can both increase and decrease predictability and therefore is not a consistent indicator of predictability. This finding has led us to consider other factors, such as impulsivity, for future study.

Beyond these individual lessons and future objectives, the next steps for the PSA model include further refinements to the definitions of the eight insider threat types, and investigations into their relationships to observable malicious insider behavior.

References

[1] E. E. Santos *et al.*, "Incorporating social theories in computational behavioral models," in *Proceedings of the Seventh International Conferences on Social Computing, Behavioral-Cultural Modeling and Prediction*, 2014, pp. 341–349.

[2] E. E. Santos *et al.*, "Modeling complex social scenarios using culturally infused social networks," in *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*, 2011, pp. 3009–3016.

[3] E. E. Santos, E. Santos Jr., L. Pan, J. T. Wilkinson, J. E. Thompson, and J. Korah, "Infusing social networks with culture," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 44, no. 1, pp. 1–17, 2014.

[4] E. Santos Jr. and E. S. Santos, “A framework for building knowledge-bases under uncertainty,” *J. Exp. Theor. Artif. Intell.*, vol. 11, no. 2, 1999.

[5] E. Santos Jr., J. T. Wilkinson, and E. E. Santos, “Fusing multiple Bayesian knowledge sources,” *Int. J. Approx. Reason.*, vol. 52, no. 7, pp. 935–947, 2011.

[6] A. Tversky and D. Kahneman, “Judgment under Uncertainty: Heuristics and Biases,” in *Utility, Probability, and Human Decision Making: Selected Proceedings of an Interdisciplinary Research Conference, Rome, 3--6 September, 1973*, D. Wendt and C. Vlek, Eds. Dordrecht: Springer Netherlands, 1975, pp. 141–162.

[7] J. Heron, “Catharsis in human development,” *Hum. Potential Res. Proj.*, 1998.

[8] S. R. Band, D. M. Cappelli, L. Fischer, A. P. Moore, E. D. Shaw, and R. Trzeciak, “Comparing insider IT sabotage and espionage: A model-based analysis,” *Technical Report: CERT Program*. Carnegie Mellon University, p. 107, 2006.

[9] F. L. Greitzer, L. J. Kangas, C. F. Noonan, A. C. Dalton, and R. E. Hohimer, “Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats,” in *45th Hawaii International Conference on System Science (HICSS 2012)*, 2012, pp. 2392–2401.

[10] N. Nwiabu, I. Allison, P. Holt, P. Lowit, and B. Oyeneyin, “Case-Based Situation Awareness,” in *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012 IEEE International Multi-Disciplinary Conference on*, 2012, pp. 22–29.

[11] J. M. McNamara, P. A. Stephens, S. R. X. Dall, and A. I. Houston, “Evolution of trust and trustworthiness: social awareness favours personality differences.,” *Proc. Biol. Sci.*, vol. 276, no. 1657, pp. 605–13, 2009.

[12] T. Thornburgh, “Social engineering: the dark art,” *Proc. 1st Annu. Conf. Inf. Secur. Curric. Dev.*, pp. 133–135, 2004.

[13] M. Hesse and N. Pohlmann, *Internet Situation Awareness*. 2008.

[14] L. Jin, H. Takabi, and J. B. D. Joshi, “Towards active detection of identity clone attacks on online social networks,” *Inf. Sci. (Ny).*, pp. 27–38, 2011.

[15] A. P. Moore, D. M. Cappelli, and R. F. Trzeciak, “The ‘Big Picture’ of Insider IT Sabotage Across U.S. Critical Infrastructures,” in *Insider Attack and Cyber Security: Beyond the Hacker*, S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith, and S. Sinclair, Eds. Boston, MA: Springer US, 2008, pp. 17–52.