Proceedings of the 2015 Winter Simulation Conference
L. Yilmaz, W. K. V. Chan, I. Moon, T. M. K. Roeder, C. Macal, and M. D. Rossetti, eds.

AGENT IMPLEMENTATION FOR MODELING INSIDER THREAT

John A. Sokolowski
Catherine M. Banks

Virginia Modeling, Analysis, and Simulation Center
Old Dominion University
1030 University Boulevard
Suffolk, VA 23435, USA

ABSTRACT

Insider threat modeling focuses primarily on the individual and the prediction of an insider threat incident. The majority of these models are statistical that tend toward trend-projections using various regression models. The modeling presented in this paper engages an agent-based paradigm that is designed to explore how an agent interacts with other employees and the organization in an environment that grants the agent opportunity and access. This paper continues our research with a discussion of the implementation of the agent's decision-making in the context of emotional, rational, and social factors affecting agent disposition. We proffer that once the agent's disposition reaches or exceeds a personal threshold, the agent is disposed to become an active threat. Our refinement of the agent facilitates continued and more rounded discussion to our original research question: "How and when does a pre-disposed insider make the decision to become an active insider threat?"

1 INTRODUCTION

A widely accepted definition of an "insider threat" describes a legitimate user of data who abuses his or her access and, given one's proximity to, and familiarity with, an environment, can cause significant damage or loss (Chinchani, 2005). Insider threat detection tends to occur when the insider exceeds his rights or alters his behavior with respect to one of three inter-related aspects (access, proximity, familiarity). Insider threat research focuses on the individual; as such, the models derived from this research is dedicated to predicting insider threat. These predictions are primarily drawn from statistical models whose analyses generally lean toward trend-projections using various regression models. A significant concern with statistical modeling is that while such approaches can present a valid representation of past activity, it does not focus on understanding the complexity and impact of dynamic changes to the system. Additionally, low base-rates of insider offending and small research populations make the derivation of offending probabilities questionable at best. Thus, statistical methods tend to provide unsatisfactory indications and probabilities of future insider threat behavior. Thus, we engage agent-based modeling.

Central to our insider threat modeling is the aspect of decision-making on the part of the agent (employee). The agents in our model are designed to make the decision to become an active insider threat based on a combination of emotional, rational, and social factors affecting their disposition. These variables are influenced by how much they are impacted by their organization's culture and by the risk and reward they perceive. Our research suggests that when an agent's disposition reaches or exceeds a personal threshold, that agent is prime to becoming an active insider threat. Given the importance of disposition in the decision-making process, we deemed it useful to further investigate the agents' emotional, rational, and social factors in the context of ethics.

This paper is a continuation of the research presented at SpringSim 2015, *An Agent-based Approach for Modeling Insider Threat.* The paper moves from the broader discussion on agent-based modeling of insider threat to a closer look at the implementation of the agent. More specifically, the agent's decision-making in the context of emotional, rational, and social factors affecting agent disposition. Our

preliminary conclusions indicate that when an insider's disposition nears the threshold it can transition to active threat mode. Our refinement of the agent facilitates continued and more rounded discussion to our original research question: "How and when does a pre-disposed insider make the decision to become an active insider threat?"

The general discussion begins in Part 2 by reviewing current approaches used to analyze insider threat. Included in this section are the conceptual underpinnings of "disposition" and the tipping-point between ideation and action. Part 3 introduces the agent-based model we have implemented for this research. A review of model outputs and validation are included. Part 4 concludes by suggesting the usefulness of this approach in the overall assessment of insider threat.

2 SIGNIFICANT THEORETICAL AND BEHAVIORAL APPROACHES

The theoretical and computational models we reviewed suffer some deficiencies in comprehensively representing and characterizing the problem of insider threat. In short, the leading theoretical approaches to the insider threat problem tend to:

- emphasize the organization, rather than individual
- concentrate on organizational defense
- center on IT vulnerabilities
- focus on monitoring and profiling technical actions
- neglect human behavioral, psychological, social aspects as a result of focusing on technical elements or center on human factors (behavior) while omitting technological elements
- examine an insider threat's behavior in a vacuum focusing on ONLINE or OFFLINE computer activity
- focus on the actions an insider threat can take (alteration, distribution, snooping)
- use a tiered-approach to prediction which lacks flexibility
- use attack trees for defense decision-making

The theoretical literature speaks to incident assessments and opportunity while the behavioral literature tended toward motive. Included in this brief literature review is Joshua Epstein's research on the notion of agent disposition.

2.1 Incident Assessments and Opportunity

For purposes of our model development, we adhere to the Chinchani definition mentioned in the introduction: a legitimate user who abuses access and capable o causing significant damage or loss (Chinchani 2005) with potential detection occurring when the insider exceeds legitimate use or changes behavior relative to access, proximity, familiarity. Recognition of anomalous behavior (when compared to the insider's baseline of activities) is a key to initiating an exploratory investigation to assess and characterize the insider's potential threat.

Chinchani (2005) conducted a thorough review of the literature to compile a general consensus of the insider threat problem and identify the areas in need of further examination. This research describes the difficulty in perceiving, detecting, and predicting insider threat on three levels: a low-base problem because these individuals have authorization (thus, it is difficult to predict or protect against these attacks; as such security officers view these attacks as unpreventable, resulting in inaction); a misperceived problem because security audits are in place focusing on external attacks; a high-impact problem because

unlike an external threat, insider threat tends to go undetected and can involve long-term malicious access. This three-level challenge has left modeling in a lurch because generally, the insider remains within his or her privilege levels.

Legg (2012) proffered an intriguing approach to anticipating threat by modeling a reasoning structure. This conceptual model allows analysts to construct hypotheses regarding a potential insider threat. The

structure emphasizes the need to represent the complete scenario beginning with why an insider may initiate an incident, to noting the indicative elements along an attack chain. As such, this model includes behavioral elements, conditions, and actions. Legg and his colleagues acknowledge that the nature of the insider threat circumvents traditional protective and detective measures of an organization. They proffer this framework to facilitate incident recognition and response discussions.

The definitive report on insider threat incident assessments is the Carnegie Mellon's Computer Emergency Response Team (CERT) Guide to Insider Threats which focuses on types of incidents: information technology sabotage, theft of intellectual property, and fraud (Capelli et al. 2012). The report drew multiple profiles of the insider per the incident type. CERT has developed a catalogue of case studies with behavior mapping. This data proved insightful for our agent-based model because it provided useful information for agent and environment development.

Munshi et al. (2012) also investigated the at-large body of literature on the subject in an effort to compile a comprehensive set of factors associated with insider threats. These factors were critiqued using empirical evidence from incidents as a means of supporting or not supporting the theoretical perspectives. A few of the conclusions drawn from their review include:

- malicious insiders do not need privileged access if they have physical access,
- theoretical literature suggests organizational/cultural factors are important, but the reported empirical evidence did not support this,
- insiders come from diverse cultures,
- over 70% of the insiders broke through system vulnerabilities in processes, procedures, and policies,
- 61% of the insiders exploited inherent weaknesses in hardware, software, or network design, and
- many incidents occurred due to the lack of physical and technical access controls despite a known need for these measures.

2.2 Motive

A 2004 Secret Service National Threat Assessment Center Report deemed financial gain as the primary motivating factor behind insiders becoming insider threats; this report concluded that to the insider, other motives are not worth the risk. Conversely, other studies indicate no single motive serves as impetus for developing into a threat (Deloitte 2012) while still others (Greitzer et al. 2012) cite greed, revenge, stress, and espionage (sabotage) as significant factors. Retaliation in light of a negative event or experience ranked also high among reported incidents: 84 percent.

Perhaps the best way to generalize motive for an insider becoming an insider threat is to note that the transition tends to be associated with "gain" that is financial or personal in nature. To a motivated insider threat, these rewards can be anticipated as any (or all) of three outputs: (1) asset loss for the institution; or (2) financial gain for the insider; (3) or a sense of retaliation for an aggrieved insider. It is also important to note that "motivation" itself is difficult to establish. This is due in part to determinations about "motivation" that are based on circumstantial inferences and, in other cases, reliance on potentially self-serving statements made by offenders such as, "I deserve to be recognized for my work; this company is cheating its constituents and I'm the only one who can fix that; I can be a hero for exposing what is happening here." Additionally, much traditional criminological research tends to regard "motivation" as static.

Yet, motivation is not static and it may, in fact, over the course of time develop or change. Recent modeling of the offending process has begun to look at motivation as a "dynamic purpose" that can, itself emerge from compounding activities not only as a driving force of behavior, but also as the result of adaptation to un-anticipated events (Dover 2010).

For example, while the insider's initial "motivation" may be driven by financial gain or excitement, it may quickly change to a desire for retribution if during early stages of the threat activity the offender is identified, sanctioned and embarrassed. Thus, threat activity may have started as a relatively covert and

unobtrusive siphoning of organizational assets but may quickly become a destructive and maliciously executed logic bomb or virus given a changing set of circumstances.

2.3 Disposition

Epstein (2013) explains disposition as the emotional, cognitive, social factors that shape the behavior of individuals, which in turn shapes the emergence of important social dynamics. His agent_zero possesses interacting emotional (affective), cognitive (deliberative), and social modules. The agent's cognitive component reflects well-documented biases and heuristics in the estimation of probabilities. As agents tend toward social networks, the social component exhibits contagion effects. Disposition is manifest as an explicit function of the agent's emotion and cognition (passion and reason) and other agent's affective and deliberative states (social). The sum of emotion, cognition, and social components equates to an agent's disposition towards action. Interestingly, action is binary and it is triggered when an agent's disposition exceeds a threshold. Epstein has developed an explicit model of individual behavior in groups that includes representations of emotion, cognition, and social influence. Our insider threat model engages and incorporates aspects of Epstein's holistic approach to representing agent behavior.

There is a plethora of matrices listing characteristics and behaviors of the insider threat. These lists include technical skills (advanced, ordinary, novice) to idiosyncrasies (impulsive, unable to assume responsibility, complacent) to sociopathic behaviors (frustrated, ethical lapses, sense of entitlement) to ethno-cultural (Caucasian, African-American, Asian) to gender (Kowalski 2008, Spooner 2013, Keeney 2005, Deloitte 2012). Wood (2000) crafted a combined approach to characterizing an insider threat by citing attributes ranging from access and knowledge, to risks and tactics, to motivation and process. The problem with this inclusive approach to representing the insider threat is that it requires the insider to follow a basic, predictable process. Unfortunately, at this point no basic, predictable process exists.

There are also models of the insiders' perception of risk and endogenous characteristics that are unique to insiders. In fact, Farahmand and Spafford (2013) uncovered an interesting paradox of risk behavior: there is an inverse relationship between perceived risk and benefit by insiders. They also note that existent traditional modeling is unable to adequately explain this paradox, especially with regard to risk analysis and expected utility.

Of great interest to our model development are the two behavioral approaches proposed by Eldardiry et al. (2013). This research distinguishes between two types of insider activities: blending anomalies wherein the insider threat tries to behave similarly to a group they do not belong to (non-threats); and unusual change anomalies wherein the insider exhibits changes in his behavior that are dissimilar to behavioral changes in (non-threat) peers. Eldardiry and his colleagues used discrete and hybrid models to compute predictability of anomalous insiders in order to craft detection techniques and Markov modeling for detection of insiders as unusual change anomalies. This thought provoking assessment of insider behavior makes it clear that some insiders, those deemed malicious, are willing to risk departure of the norm to achieve a malicious goal.

These theoretical and behavioral models highlight the need to characterize the insider threat and as such, they provide the foundation for subjective factors and hypotheses that can shape computational models. The computational models typically used, Bayesian network predictions and system dynamics, tend to take a holistic look at the complexity of insider threat, but suffer the constraint of static representation. These paradigms are, thus, useful for understanding and communicating the problem, but not predicting it. Conversely, game theory models are unable to capture the level of complexity needed to represent insider threat relative to the dynamism of human behavior in an adaptive environment. Still, it is useful to cull aspects of these models that can contribute to our agent-based model.

3 AGENT-BASED MODELING APPROACH

The strength of agent-based modeling (ABM) is that it provides a means to represent complex adaptive behavior by focusing on the attributes of individual (heterogeneous) entities (agents) and how they interact within the larger system. This is in sharp contrast to other modeling methods which tend to either

focus on the variables of the system as a whole, or focus on attributes of homogeneous entities without robust and dynamic interactions.

In our ABM implementation we assume that an organization is made up of a certain number of heterogeneous employees. Those employees have the potential to become an active insider threat based on a combination of emotional, rational, and social factors affecting their disposition. Their disposition is influenced by how much they are impacted by their organization's culture and by the risk and reward they perceive. Once their disposition reaches or exceeds a personal threshold, the employee is disposed to become an active threat.

3.1 Implementation

We implement insider disposition using Epstein's Agent_zero ABM structure (Epstein 2013). Agent_zero consists of three behavioral components: emotional, rational, and social. These three components combine to provide an overall disposition towards a particular decision or action. Agent_zero treats disposition as a binary condition. Either the agent is disposed or not disposed to take some action or make some decision. This behavioral structure was used to represent each insider in an organization.

Implementation of the emotional component of agent_zero is represented as the difference between an insider's expectations and fulfillment of those expectations. In our insider threat model, expectations are related to an insider's anticipated level of fulfillment within a particular organizational culture. How the insider interprets the organization's actual ability or failure to meet expectations represents the insider's fulfillment.

An insider's expectations change based on initial, current, and historical fulfillment of those expectations. We represent expectations with the following equation.

$$E_{j+1} = \frac{(F_1 p + ((\sum_{i=1}^{j} F_i)/j)c + F_j r)}{(p + c + r)} \tag{1}$$

$E_{j+1}$is the expectation for the next time step of the simulation, F is actual fulfillment at various times throughout the simulation, p is the primacy weight, i.e. how much weight the employee places on his or her initial fulfillment, c is a consistency weight for how much emphasis is placed on the average fulfillment over time, and r is the recency weight for the emphasis on the most current fulfillment. The agent's interpretation of fulfillment deficit is then computed using Equation (2).

$$d_j = \big(E_j - F_j\big)a \tag{2}$$

Here d_j is distance of expectation from fulfillment d at time j given the insider's interpretation. In Equation (2) a is essentially an agent-specific affective weight.

The rational component of the agent_zero concept is usually implemented as a probability associated with classical decision theory and bounded rationality. For our implementation we treat the rational component as a payoff probability measured by the difference between assessed risks vs. expected reward.

The social component is a sum of weighted dispositions of the other agents in the model. These weighted dispositions represent how much the employee in question is influenced by his or her fellow employees.

Mathematically an agent's disposition is represented by Equation (3).

$$D_i^{tot}(t) = d_i(t) + P_i(t) + \sum_{j \neq i} \omega_{ji} D_j^{solo}(t) \tag{3}$$

$D_i^{tot}(t)$ represents an employee's disposition to become an insider threat, $d_i(t)$ is the employee's interpretation of fulfillment deficit from Equation (2), $P_i(t)$ is the employee's risk versus reward payoff

probability, and $\sum_{j \neq i} \omega_{ji} D_j^{solo}(t)$ is the weighted dispositions of all other employees. This insider threat ABM is implemented with a specified number of employees, each represented by an agent_zero model. The organization is also modeled as an agent; however it is not represented by an agent_zero model.

The emotional aspect of the employee is related to the insider's interpretation of his ability or inability to derive the expected level of fulfillment from the organizational environment. The organizational environment is characterized by two factors: *organizational_culture* and *organizational_impact*. *Organizational_culture* is the sum of three user editable parameters: *employee_support*, *it_policy*, and *organization_ethic*. Each of these three parameters is scored as a number between zero and one. A score of zero indicates that the organizational parameter adversely impacts expectations. A score of one indicates that the organizational parameter favorably impacts expectations.

At the start of the simulation each employee is initialized with values for their insider threat threshold and their risk and reward values. An initial value for *organizational_impact* is then computed. *Organizational_impact* is a random normal variable with a mean based on the *organizational_culture* value. Thus, while *organizational culture* gives a general sense of the organizational environment, *organizational_impact* represents the current organizational environment with dynamic variations. This variation defines how each insider perceives fulfillment and thus has a direct bearing on the insider's fulfillment deficit and resulting disposition.

Additionally, each insider is influenced (to some degree) by other employees in the organization. The "degree" of influence is characterized by a weighting factor assigned to each employee. This factor can be positive or negative (negative value represents a mitigating influence). Each employee is, therefore, influenced by the average view of all the other employees combined. Keep in mind that an employee may not be influence by every employee because weighting factors could be zero or very nearly zero for a given employee relationship.

Variation in fulfillment deficit for each insider occurs over time. Given enough of a deficit, an insider may exceed his or her personal threat threshold and become an active insider threat. It is also possible that an active insider threat's fulfillment deficit can be reduced over time and his active threat disposition can drop back below his threshold. In this case, a previously active insider threat can cease to be an active insider threat. We capture the number of insiders that become an active threat, as well as the insiders who transition from active threat to inactive threat as an indicator of possible threat generation and threat status.

The model was initially implemented in NetLogo Version 5.0.5 (Welinsky 1999). However to gain computational efficiency it was recoded in C++. The simulation explores the percentage of employees that develop an insider threat disposition for a given set of conditions. Parameters include the number of employees, the organizational environment (as outlined above), the number of days to evaluate the organization, and the number of iterations for each set of parameters to develop a statistical output.

Each iteration (or step) in the model represents a single day. The simulation uses these parameters to explore the result of various insider-specific characteristics that include affective weight, risk tolerance level, reward level, and threat threshold. Organizational characteristics are also allowed to vary to simulate changes in organizational culture over time.

3.2 Preliminary Results

Various combinations of employee characteristics and organizational change can thus be evaluated and compared to see which combinations provide for greater likelihood of insider threats developing over time. Significant parameters used in the initial parameter sweeps for were: *affective-weight*, *risk-tolerance*, *threat-threshold*, *reward-value*, and *organizational-change*.

Affective-weight, *risk-tolerance*, and *threat threshold* are insider specific parameters. *Affective-weight* is directly involved in the calculation of fulfillment deficit (a in Equation (2)) and represents the affective impact of lack of fulfillment. *Risk-tolerance* is involved in the calculation of the cognitive aspect of the

Agent_zero structure and represents the insider's ability to tolerate risk. Threat-threshold provides the individual insider's threshold beyond which his threat disposition becomes active.

Reward-value and organizational-change are specific to the organizational environment. Reward-value represents the potential value of becoming an insider threat and is involved in the cognitive aspect of the agent-zero structure. *Organizational_change* represents the propensity for organizational shifts independent of culture. A lower value (0.01) indicates gradual shifts and a larger value (0.05) indicates potentially more dramatic shifts. This parameter is used in the calculation of organizational fulfillment and is implemented as the standard deviation in determining the over-all impact of the organizational culture.

The model was set up and tested using an organization size of three hundred employees. The p, c, and r weights of Equation 1 were all set to a value of one. Parameter sweeps were run across all five of the following parameters using three parameter-specific values to represent high (H), medium (M), and low (L) values. All possible combinations of these parameters were run. This method was chosen as a computationally efficient way to evaluate model response over the range of these parameters. These values were:

affective-weight	(H=1.5, M=1.0, L=0.5)
risk-tolerance	(H=0.3, M=0.2, L=0.1)
threat-threshold	(H=2.0, M=1.5, L=1.0)
reward-value	(H=0.3, M=0.2, L=0.1)
organizational-change	(H=0.05, M=0.03, L=0.01)

The number of *active* insider threats, *inactive* (but previously active) insider threats, and *total number of threats* (*active* + *inactive*) for a twenty year-period (7,305 steps) were collected and averaged over 100 runs for each of the 243, or 3^5, parameter combinations. One hundred runs were chosen to provide a meaningful statistical sample size. Table 1 shows the results of the 20 combinations of factors that produced the highest total of threats.

Table 1: Sample simulation output showing low, medium, and high indicators.

Affective Weight	Risk Tolerance Value	Reward Value	Threat Threshold	Organization Change	Previous Threat Count	Threat Count	Total
H	H	H	L	H	86	75	161
H	H	M	L	H	80	69	149
H	M	H	L	H	81	66	147
H	M	M	L	H	74	64	138
H	L	H	L	H	74	61	135
H	H	L	L	H	74	61	135
H	M	L	L	H	66	58	124
H	L	M	L	H	67	56	123
H	L	L	L	H	61	51	112
H	H	H	M	H	55	45	100
H	M	H	M	H	51	39	90
H	H	M	M	H	51	38	89
M	H	H	L	H	47	36	83
H	L	H	M	H	45	36	81
H	M	M	M	H	45	36	81
H	H	L	M	H	46	35	81
H	M	L	M	H	44	33	77

H	L	M	M	H	40	32	72
M	M	H	L	H	40	30	70
M	H	M	L	H	38	31	69

3.3 Model Validation and Discussion of Results

Validation of human behavior and social models poses a challenge because of the truly random nature of the system being simulated and the difficulty of gathering empirical evidence because of this variability. However there are accepted techniques that can be used to address this issue (Petty 2010). From a theoretical validity standpoint, we started with behavioral theory grounded in published research. Epstein provides a review of the relevant theories employed in this model. From an empirical validation standpoint given the acceptance that insider threat is a rare event we next checked the reasonableness of our model results and looked for any noticeable or dramatic artifacts that would indicate unreasonable behavior.

An example of "unreasonable behavior" would be a large number of employees becoming insider threats under an organization with a favorable culture or no employees tending towards insider threat status in a very unfavorable culture. None of these cases were observed. As noted in the National Business Ethics Survey (Ethics Resource Center 2013) forty-one percent of workers surveyed said they observed misconduct by fellow workers while on the job. While it does not directly correlate to insider threat, this level of worker misconduct resembles the average prediction of our top ten parameter combinations of 132.4 previous and current insider threat totals (44%). Further empirical validation could involve comparing simulation results to actual cases. This approach may be explored as we further develop this model.

4 CONCLUSION

Our model and its yielded results are a promising exploration of the insider threat issue from an agent-based model paradigm. Agent-based models provide a platform to observe complex adaptive behavior of employees in an organization and study how insider threats can evolve within an organization. This paper presents the second iteration of our model's execution. Its aim is to capture the development of insider threat behavior given the set of assumptions we have outlined that govern the agents' behavior. This model will serve as a platform for further investigation of insider threats. Future plans include developing a more detailed dissatisfaction model governing emotional response and to explore ways the model may be used to develop detection schemes for such threats. Next steps will be to conduct sensitivity analysis of the parameters to better gauge their influence on the behavior and to assist in further validation of the model.

REFERENCES

Capelli, D.M., A.G. Desai, A.P. Moore, T.J. Shimeall, E.A. Weaver, B.J. Willke. 2008. *Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System*. Pittsburgh: Software Engineering Institute.

Cappelli, D.M., A.P. Moore, R.F. Trzeciak. 2012. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Boston: Addison-Wesley.

Chinchani, R., et al. 2005. "Towards a Theory of Insider Threat Assessment. Dependable Systems and Networks". In *IEEE Proceedings of the International Conference on Dependable Systems and Networks,*108 – 117. Yokohama, Japan: Institute of Electrical and Electronics Engineers, Inc.

Deloitte Consulting. 2012. "Mitigating the Insider Threat Building a Secure Workforce." Accessed July 7. http://csrc.nist.gov/organizations/fissea/2012-conference/presentations/fissea-conference-2012_mahoutchian-and-gelles.pdf

Dover, T. J. 2010. "The Offender Interaction Process Model." *The Forensic Examiner*. 19(3):28 – 40.

Eldardiry, H., B. L. Evgeniy, L. Juan, J. Hanley, B. Price, O. Brdiczka. 2013. "Multi-Domain Information Fusion for Insider Threat Detection". In *Proceedings for the IEEE CS Security and Privacy Workshops (SPW2013)*, 45 – 51. San Francisco: Institute of Electrical and Electronics Engineers, Inc.

Epstein, J. M. 2013. *Agent Zero: Toward Neurocognitive Foundations for Generative Social Science*. Princeton: Princeton University Press.

Ethics Resource Center. 2013. *National Business Ethics Survey of the U. S. Workforce*. Arlington: Ethics Resource Center.

Farahmand, F.; E.H. Spafford. 2013. "Understanding Insiders: An Analysis of Risk-taking Behavior". *Information Systems Frontiers*. 15(1):5 – 15.

Greitzer, F.L.; L.J. Kangas, C.F. Noonan, A.C. Dalton, R.E. Hohimer. 2012. "Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats." In *Proceedings for the 2012 45th Hawaii International Conference on System Science*, edited by R. H. Sprague, Jr., 2392 – 2401. Maui, Hawaii: Institute of Electrical and Electronics Engineers, Inc.

Keeney, M.D., et al. 2005. "Insider Threat Study: Computer Sabotage in Critical Infrastructure Sectors." CERT Program and Software Engineering Institute, Pittsburgh, Pennsylvania.

Kowalski, E.T., et al. 2008. "Insider Threat Study: Illicit Cyber Activity in the Government Sector.": U.S. Secret Service and CERT/SEI, Washington, DC.

Munshi, A., P. Dell, H. Armstrong. 2012. "Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents." In *Proceedings of the 45th Hawaii International Conference on System Science*, edited by R. H. Sprague, Jr., 2402 – 2411. Maui, Hawaii: Institute of Electrical and Electronics Engineers, Inc.

Petty, M. D. 2010. "Verification, Validation, and Accreditation." In *Modeling and Simulation Fundamentals: Theoretical Underpinnings and Practical Domains*, edited by J. A. Sokolowski and C. M. Banks, 325 – 372. Hoboken: John Wiley and Sons, Inc.

Spooner, D; et al. 2013. "Spotlight On Insider Theft of Intellectual Property Inside the U.S. Involving Foreign Governments or Organizations." Technical Note CMU/SEI-2013-TN-009, CERT Program, Software Engineering Institute, Pittsburgh, Pennsylvania.

United States Secret Service-National Threat Assessment Center. 2004. Insider Threat Study: Illicit Cyber-Activity in the Banking and Finance Sector. Accessed July 7. http://www.secretservice.gov/ntac/its_report_040820.pdf

Welinsky, U. 1999. NetLogo. http://ccl.northwestern.edu/netlogo/. Center for Connected Learning and Computer-Based Modeling, Northwestern University. Evanston, IL.

Wood, B.J. 2000. "An Insider Threat Model for Adversary Simulation." In *Research on Mitigating the Insider Threat to Information Systems – #2*, edited by R. H. Anderson, T. Bozek, T. Longstaff, W. Meitzler, M. Skroch, and K. Van Wyk, 41 – 48. Santa Monica: RAND Publications.

AUTHOR BIOGRAPHIES

JOHN A. SOKOLOWSKI is the Executive Director for the Virginia Modeling, Analysis, and Simulation Center (VMASC) and Associate Professor of Modeling, Simulation, and Visualization Engineering both at Old Dominion University. He oversees 40 researchers and staff with an annual funded research budget of $3 million. He administers research and development in Transportation, Homeland Security, Defense, Medical M&S, Decision Support, Business & Supply Chain, and Social Science M&S applications. He is contributor and co-editor of Principles of Modeling and Simulation (Wiley, 2011) and Modeling and Simulation: A Multidisciplinary Approach (Wiley 2009). His email address is jsokolow@odu.edu.

CATHERINE M. BANKS is Research Associate Professor at VMASC. Her focus is on qualitative research among the social science disciplines to serve as inputs into various modeling paradigms: game

theoretical, agent-based, social network, and system dynamics. Dr. Banks' research includes models representing humans and human behavior to include the translating / mapping of data for quantitative representations, modeling states and their varied histories of revolution and insurgency, political economy and state volatility, and medical simulation. She has authored and edited books and journal articles on these topics and is co-author of Modeling and Simulation for Analyzing Global Events (Wiley 2008). Her email address is cmbanks@odu.edu.