Introduction to the special issue on insider threat modeling and simulation

Andrew P. Moore¹ · Kirk A. Kennedy² · Thomas J. Dover²

Published online: 9 March 2016
© Springer Science+Business Media New York 2016

1 Introduction to the insider threat problem

Despite the high impact of insider attacks, findings show that many organizations have no insider threat program in place, and most programs that do exist have serious deficiencies (INSA 2013). Mandates for U.S. Government organizations and their contractors to build such programs attest to their importance (Office of the Press Secretary 2011), but determining how insider threat countermeasures reduce organizational risk is difficult to ascertain (U.S. GAO 2015).

Negative unintended consequences of controls have the potential to exacerbate rather than mitigate the problem (Moore et al. 2015a, b). Furthermore, the tendency of organizations to view insider threats as a technology problem, and the stove-piped nature of their processes, has made it difficult for them to deal effectively with the socio-technical nature of the problem (INSA 2013).

The purpose of this Special Issue is to demonstrate the potential for modeling and simulation science to not only help understand the nature of the insider threat problem better, but also to help test the efficacy of mitigation controls in a safe and convenient virtual environment.

Andrew P. Moore
apm@cert.org

Kirk A. Kennedy
kirk.kennedy@ic.fbi.gov

Thomas J. Dover
thomas.dover@ic.fbi.gov

¹ CERT Program, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA
² Behavioral Analysis Unit, Federal Bureau of Investigation, Quantico, VA, USA
1.1 Definitions

Insider threat definitions include everything from malicious to unintentional and from non-violent to violent actions by trusted insiders. Shaw et al. (2009) broadly define “insider threat” as

Any activity by military, government, or private company employees whose actions or inactions, by intent or negligence, result (or could result) in the loss of critical information or valued assets.

The above definition does not include former employees and does not give different definitions that distinguish malicious insiders from unintentional insiders. There are two types of insider threats addressed in this Special Issue: malicious insider threats and unintentional, accidental, or inadvertent threats.

First, malicious insider threats that target information or information systems are defined by (Cappelli et al. 2012) as follows:

A malicious insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.

Second, unintentional, accidental or inadvertent insider threats are defined by the CERT Insider Threat Team (2013) as follows:

An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization’s network, system, or data and who, (3) through action or inaction without malicious intent, (4) causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization’s information or information systems.

1.2 Existing research

The insider threat problem is associated with an area of research that has been primarily initiated and funded by the U.S. government over the past two decades and has not had a strong emphasis in academia. Two of the largest U.S. government efforts specifically focused on insider threat are

- Defense Advanced Research Project Agency, Anomaly Detection at Multiple Scales (DARPA ADAMS): See a description of the program at http://www.darpa.mil/program/anomaly-detection-at-multiple-scales.
- Intelligence Advanced Research Projects Activity, Scientific advances to Continuous Insider Threat Evaluation (IARPA SCITE): See a description of the program at http://www.iarpa.gov/index.php/research-programs/scite.
Various workshops on the insider threat problem have also been held, such as

- Workshop on research on insider threats (WRIT)—The WRIT was held for 3 years starting in 2012 and has been associated with the IEEE Symposium on Security and Privacy. See the Security and Privacy Workshop (SPW) Proceedings link for 2012–2014 at [http://www.ieee-security.org/TC/SP-Index.html](http://www.ieee-security.org/TC/SP-Index.html) for the WRIT proceedings.

- Managing insider security threats (MIST)—The MIST workshop has been held for the last 7 years (2009–2015) and is currently associated with the ACM Conference on Communication and Computer Security. Proceedings for the 2015 MIST conference are located at [http://isyou.info/conf/mist15/](http://isyou.info/conf/mist15/).

- Schloss Dagstuhl Seminars on Insider Threat—The Dagstuhl Insider Threat Seminars at the Leibniz Center for Informatics produced a series of reports and books documenting their findings, including work that involved insider threat modeling and simulation. An overview of the seminars can be found at [http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=12501](http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=12501).

- Insider Threat Mini-Track at the Hawaii International Conference on Systems Sciences (HICSS)—For the past 5 years (2012–2016), the HICSS has had a mini-track on various aspects of the insider threat problem. For the 2016 insider threat mini-track description, see [http://www.hicss.org/#!inside-the-insider-threat/c1cck](http://www.hicss.org/#!inside-the-insider-threat/c1cck).

- CERT Resources—The Insider Threat Center in the CERT Division of the Software Engineering Institute provides a variety of regular offerings, including insider threat symposia, workshops, training, and certificates. See the insider threat web presence at [http://www.cert.org/insiderthreat](http://www.cert.org/insiderthreat) for more information about CERT insider threat offerings.

In addition, there exist publications on various insider crimes ranging from sabotage to theft, fraud, and espionage. For an overview of the research on insider theft, sabotage, and fraud, consult Cappelli et al. (2012). For a starting point in understanding insider espionage, see Herbig (2008). Another reference to consult for an introduction to espionage research is a book “Citizen Espionage” edited by Sarbin et al. (1994), which presents a wide array of information on spying and includes a discussion of models of espionage which account for person-specific variables (“P” models) and situational variables (“S” models).

Traditional insider threat research has suffered from two problems:

1. The data are limited due to the low base rates of most of the insider threat crimes. Related to this problem is the reluctance of private companies and governments to share this information with researchers.

2. Once researchers get their hands on the data, they do not typically collect data from matched control subjects from the “assumed good” population or other potential comparison groups. Thus, the validity of conclusions about the offending insider are limited in nature.
These problems can be addressed through modeling and simulation approaches. For problem #1—lack of data due to low base rates—modeling and simulation approaches can be used to generate synthetic data to consider when testing hypotheses. For problem #2—lack of comparison groups—modeling and simulation approaches can build in control and/or other comparison groups.

Modeling and simulation have been successfully used to address a number of security issues, particularly as they play out in organizational settings e.g., (Cohen 1999; Gupta et al. 2006; Liu et al. 2003). Further, there has been some attention to modeling insider threat e.g., (Duran et al. 2009; Kandias et al. 2010; Martinez-Moyano et al. 2008; Moore et al. 2015a, b). These efforts show the value of this approach, and that there are a number of modeling technologies that can support reasoning about security risks in organizational settings.

1.3 Purpose of this special issue

Given the problems associated with insider threat research, a question was posed whether modeling and simulation approaches could be used to help understand and mitigate insider threats. More specifically, how can modeling and simulation be utilized to generate useful synthetic insider threat data and to analyze underlying assumptions of traditional research in this area? Further, how can modeling and simulation be utilized alone and/or combined with other approaches, to help understand and mitigate insider threats?

These ideas were explored in an invitational meeting called “The Insider Threat Modeling and Simulation Research Meeting” sponsored by the Software Engineering Institute. This Special Issue of the Computational and Mathematical Organization Theory journal arose out of this meeting to show how the different approaches to modeling and simulation help understand the insider threat problem. The meeting objective was to understand and explain three things:

1. the role of modeling and simulation to better understand insider threat related problems and mitigation
2. how different modeling and simulation methods can be used individually and in combination
3. the role modeling and simulation methods can play toward building a scientific discipline of insider threat.

While research challenges and questions were emphasized over detailed implementation of solutions, the workshop participants made some intriguing progress on insider threat models using five methods: agent-based modeling (ABM), Bayesian belief networks (BBN), game theory (GT), system dynamics (SD), and network analysis (NA).

As we describe in the next section, these methods do not and were not meant to cover the entire space of modeling and simulation approaches that could be applied to insider threats; that would be far too ambitious for our small working meeting of 20 participants. Nevertheless, these approaches do target important aspects of the
insider threat problem, and each has had significant applications to the problems in the literature.

The 1½ day meeting, which took place on 7/31/2014 and 8/1/2014 at the Software Engineering Institute in Pittsburgh, PA, involved participants from across academia, industry, and government, including representatives from Argonne National Laboratory, Carnegie Mellon University, Human Resources Research Organization (HumRRO), MIT Lincoln Laboratory, New York University, Old Dominion University, Sandia National Laboratory, the Software Engineering Institute, and the FBI.

To the best of our knowledge, this is the first meeting with the goal of understanding how a range of modeling and simulation methods can be utilized to further our understanding of complex insider threat problems. The focus of the papers in this Special Issue are methods that involve the execution of an explicit, abstract model of an organization in contrast to the emulation of a computer system or pilot testing within an organization.

It can take a lot of time, be very expensive, disruptive, and even dangerous to pilot test controls operationally. The behaviors of malicious actors and good employees can be extremely difficult to distinguish in practice, increasing the probability that innocent employees will be implicated in malicious activities. Strong evidence of potential countermeasure effectiveness is needed before operational pilot testing commences. Using a modeling and simulation environment to rigorously test hypotheses allows confirmation, extension, and refutation of existing theory or the formulation of new theories altogether.

The experiments conducted in the virtual environment can provide a body of evidence that supports strong hypotheses that can justify subsequent pilot testing efforts. The results of our workshop confirmed the utility of these modeling and simulation methods, especially in combination, to address the complexity of the insider threat problem.

2 Modeling and simulation methods and their combination

A unique contribution of this Special Issue is to elaborate and exemplify the combination of modeling and simulation methods toward addressing aspects of the insider threat problem. The Computational and Mathematical Organization Theory journal is particularly appropriate for this topic because of the strong organizational perspective of the threat and the links to theory that the modeling and simulation enable.

Since work applying this technology to the insider threat problem is early and primarily exploratory in nature, results are not yet definitive and models are not yet predictive. Nevertheless, we believe that the papers published in this Special Issue do, in fact, strongly demonstrate the potential for modeling and simulation science to help understand the nature of the insider threat problem and test the efficacy of mitigation controls. These methods do not supplant existing research or obviate the need for other approaches, but they are underutilized in insider threat research generally.
2.1 Methods considered in this special issue

The modeling and simulation methods described in this Special Issue have a rich basis and history:

2.1.1 Agent-based modeling (ABM)

ABM is an object-oriented approach to simulate the actions and interactions of autonomous agents within a larger ecological context. Agents can represent a variety of objects from individual actors (i.e., people) to collective communities and organizations (i.e., corporations or countries) that have endogenous and frequently heterogeneous features. Ecological context provides an environment in which exogenous stimuli (produced by the environment or other agents) can influence and drive individual agent behaviors. A common goal of ABM, regardless of the scale of the agent, is to understand the emergent behavior of the larger system of which they are a part (Gilbert 2008). While the origins of ABM trace back to the late 1940s with the Von Neumann machine and the notion of cellular automaton, the first formal models were not developed until the 1970s followed by an explosion of the field in the 1990s, made possible by software platforms built on increasingly powerful computers that supported real-time visualizations (Cioffi-Revilla 2014). ABMs show that even relatively simple interaction rules can generate a broad range of complex behaviors that correspond with real-world observation (Epstein and Axtell 1996). A variant of ABMs, agent-based dynamic-network models have been successfully used to model issues of behavior adaptation and information diffusion across multiple groups—making them particularly valuable for addressing issues related to insider threat and security (Lanham 2015; Lanham et al. 2011).

2.1.2 Game theory (GT)

GT has been characterized as “the study of mathematical models of conflict and cooperation between intelligent rational decision makers” (Myerson 1991). While early discussion of two-person games goes back at least as far as the 1700s, GT did not exist as a unique field until John von Neumann’s descriptions of the foundations in his book in 1944, *Theory of Games and Economic Behavior* (Leonard 2010). The 1950s saw the field expand into the logical side of decision science by many scholars in the areas of economics, political science, psychology, computer science, and biology.

2.1.3 System dynamics (SD)

SD is a method based in continuous mathematics for modeling and analyzing the holistic and dynamic nature of problematic behavior by analyzing the underlying feedback structure of that behavior (Sterman 2000). SD was developed by Jay Forrester in the mid-1950s as a method derived from control theory to graphically portray a system of differential equations used to endogenously model soft factors, such as policy, procedural, administrative, or cultural factors along with hard,
strictly technical factors. From its beginnings as a means to help corporations improve industrial processes, its use broadened in the 1970s and 1980s to areas of urban and environmental dynamics. With the development of powerful, user-friendly simulation platforms in the 1990s, its use expanded further to both public and private sector problems involving policy analysis and design.

2.1.4 Bayesian belief network (BBN)

BBNs are probabilistic, directed acyclic graphs where the nodes represent random variables and edges represent conditional dependencies among the random variables. Efficient algorithms exist to support the automatic application of Bayes Theorem through the network to calculate the probability that a certain event will occur or condition will exist. While the foundational work by Thomas Bayes was performed in the 1700s, it was not until Judea Pearl and Richard Neapolitan’s writings in the 1980s that BBNs became a field of study (Neapolitan 1990; Pearl 1985, 1988). BBNs have been applied to modeling knowledge in computational biology, medicine, bio-monitoring, document classification, information retrieval, semantic search, image processing, data fusion, decision support systems, engineering, gaming, law, and risk analysis.

2.1.5 Network analysis (NA)

NA, a part of network science that draws on the mathematics of graph theory, considers distinct entities represented by nodes and the interconnection among those nodes represented by edges. While the study of networks was introduced in the 1700s for understanding complex relational data, its application in the area of sociology, called social network analysis, emerged in the 1930s to study interpersonal relationships (Moreno 1934). Social network analysis was formalized mathematically in the 1950s and became pervasive in the social sciences by the 1980s (Freeman 2004). Application of social network analysis to organizations grew at the end of the twentieth century, as did the methods on which they were based. A new discipline called dynamic network analysis has emerged as a means to model multiple types of nodes and links for the analysis of more complex properties of organizations over time (Carley 2003). Dynamic network analysis combines the specification of multi-dimensional networks—as in (Carley 2002; Contractor et al. 2011)—with ABM simulation to address temporal issues of network dynamics as in (Carley 2006).

2.2 Combinations of methods

As we mentioned, other modeling and simulation approaches could have been chosen for our working meeting. However, when considering problems and solutions in the insider threat domain, these five approaches complement one another in a number of ways:
2.2.1 Individual versus context

The insider threat problem requires considering attributes of both the individual and the context in which that individual acts. ABM and SD complement each other in this respect. ABM focuses on an individual level—on interaction rules among potentially heterogeneous individuals that can create complex emergent behaviors. SD, on the other hand, focuses on system features at an aggregate level and is particularly useful at analyzing how these features can drive system behaviors. Of course, what is aggregate at one level of abstraction may be considered an individual at a higher level of abstraction, so there is interplay between the two approaches that often depends entirely on scale. Some tools even directly support the development of combined ABM and SD models, for example, Anylogic (http://www.anylogic.com/), Ventity (http://vensim.com/ventity-beta/), and NetLogo (https://ccl.northwestern.edu/netlogo/). However, these tools are not a necessity. For instance, the Sokolowski et al. paper in this Special Issue uses a combination of SD and ABM in the presentation of the authors’ model without direct tool support.

2.2.2 Actor rationality

GT provides a powerful method for establishing a benchmark for beginning to understand complex decision making. Of course, the logical preferences and utility-maximized decision making of rational actors are not always representative of real-world actors with limitations of attention, memory, and information processing capability driven by emotions, reflex, and unconscious motivations. The rational actor analysis performed in GT complements (and is complimented by) the bounded rationality of actors traditionally assumed by ABM and SD modelers. SD and ABM support limiting the scope of agent decision making to information ecologically available to the agent. This limited scope promotes making decisions as real-world actors do, by considering the context in which those decisions are actually made. ABMs can also serve as a convenient means to visualize the emergent behavior of actors driven by specific GT rules of interaction. This approach is taken in the Casey et al. paper in this Special Issue.

2.2.3 Risk calculation and feedback

An important capability of insider threat programs is the ability to detect increasing levels of insider threat risk at individual and organizational levels. BBNs provide an important means for detecting increased risk and whether that risk comes from conditions in the organization, situational features of the individual, and/or the individual’s social and online behaviors. BBNs can be used to update insider risk related variables based on the probabilities of important indicators of that risk. This is true even when the probability of an insider attack is very low (Hubbard 2009, p. 227). BBNs can clearly be used to calculate initial parameter values in each of the other modeling and simulation approaches. However, the acyclic aspect of BBNs means that the values calculated do not provide feedback to previously calculated variables. Other approaches, like SD, are based directly on such feedback.
mechanisms and thus provide complimentary methods that provide an update of the prior values on which a BBN is based. This multi-method approach is taken in the Sticha and Axelrad paper in this Special Issue.

2.2.4 Execution of multi-dimensional networks

Similar to GT, NA in its most fundamental form is not executable. However, just as with GT, NA can be used in combination with ABM to provide a means to execute and visualize network behaviors over time. This approach is taken by the Carley and Morgan paper in this Special Issue. In fact, the approach taken in this paper uses a tool, called Construct, developed by the author group to conduct multi-dimensional network analysis on an evolving multi-agent network model of an organization.

Clearly there are different modes of interoperation among the various tools that support elaboration, investigation, and mitigation of the insider threat problem. Those listed above are just a few of the interactions possible. Future work could elaborate and illustrate other potential modes.

3 Papers in this special issue

The four papers in this Special Issue are

- John Sokolowski, Catherine M. Banks, and Tom J. Dover—“An Agent-Based Approach to Modeling Insider Threat”
- Kathleen M. Carley and Geoffrey P. Morgan—“Inadvertent Leak: Exploration via Agent-Based Dynamic Network Simulation”
- William A. Casey, Jose Andre Morales, Quanyan Zhu, Evan Wright, and Bud Mishra—“Compliance Signaling Games: Toward Modeling the Deterrence of Insider Threats”
- Paul J. Sticha and Elise T. Axelrad—“Using Dynamic Models to Support Inferences of Insider Threat Risk”

Table 1 illustrates our attempt to classify the computational methods described in these papers. Although this task seemed simple, it became apparent that organizing

| Special issue articles            | Game theory | Agent-based modeling | System dynamics | Bayesian belief network | Network analysis |
|-----------------------------------|-------------|----------------------|-----------------|------------------------|-----------------|
| Sokolowski, Banks, and Dover      | ✔           | ✔                    |                 |                        |                 |
| Carley and Morgan                 | ✔           |                      |                 |                        | ✔               |
| Casey, Morales, Wright, Zhu, and  | ✔           | ✔                    |                 |                        |                 |
| Mishra                            |             |                      |                 |                        |                 |
| Sticha and Axelrad                |             |                      |                 |                        | ✔               |

Table 1 Primary modeling and simulation methodologies described by articles in this special issue

© Springer
these papers into categories was not only difficult but also possibly counter-
productive and subject to debate. There were, of course, obvious categorizations. For instance, several of the papers involve well-defined characteristics of agent-
based modeling. Yet, upon closer examination of the respective agents in those models, we begin to find that the macro-behaviors being described are the outcomes of generative models of decision making that transverse the other categories. Other papers emphasize the application of hybrid methodologies or the use of one method to inform the other.

Ultimately, the specific method(s) of implementation in each of these articles may not be as important as the overall understanding that there are diverse ways to approach the same problems that have vexed the non-computational research community. This realization is not a surprise to computational modelers, but it may be an epiphany to researchers who sense that the current methods of research into hard problems, like insider threat, are limited when applied to intractable issues.

Modeling and simulation is critical for understanding complex domains. Complexity in the natural cognitive and social environment is the source of the difficulty associated with mitigating the insider threat. The complexity of insider threat related behaviors, compounded with low base rates and relatively hidden processes and populations, highlights the dangerous voids in our theories and practical knowledge.

The articles in this Special Issue offer a diversity of perspectives on the hard problem of insider threat and its many features. While the tendency might be to view each of these computational methods as distinct, it is also our intention to present them as part of a larger mosaic of methodological tools. The overlap among methods, in some cases, will be obvious; in other cases the overlap will be more nuanced. The point is, however, that these tools each offer an opportunity to gain a new perspective on the multi-faceted insider threat problem.

Acknowledgments This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Compliance with ethical standards

Conflict of Interest The authors declare that they have no conflict of interest.

References

Cappelli DM, Moore AP, Trzeciak RF (2012) The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley, Boston
Carley KM (2002) Smart agents and organizations of the future. Handb New Media 12:206–220
Carley KM (2003) Dynamic network analysis. Dynamic social network modeling and analysis: workshop summary and papers. Committee on Human Factors, National Research Council, Washington, pp 133–145
Carley KM (2006) A dynamic network approach to the assessment of terrorist groups and the impact of alternative courses of action. DTIC Document
CERT Insider Threat Team (2013) Unintentional insider threats: a foundational study. Technical Report CMU/SEI-2013-TN-022, Software Engineering Institute, Pittsburgh

© Springer
Cioffi-Revilla C (2014) Introduction to computational social science: principles and applications. Springer, London and Heidelberg
Cohen F (1999) Simulating cyber attacks, defences, and consequences. Comput Secur 18(6):479–518
Contractor NS, Monge PR, Leonardi PM (2011) Multidimensional networks and the dynamics of sociomateriality: bringing technology inside the network. Int J Commun 5:682–720
Duran F, Conrad SH, Conrad GN, Duggan DP, Held EB (2009) Building a system for insider security. IEEE Secur Priv 6:30–38
Epstein JM, Axtell R (1996) Growing artificial societies: social science from the bottom up. Brookings Institution Press, Washington
Freeman LC (2004) The development of social network analysis: a study in the sociology of science. Empirical Press, Vancouver
Gilbert N (2008) Agent-based models. SAGE Publications Inc, New York
Gupta M, Rees J, Chaturvedi A, Chi J (2006) Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach. Decis Support Syst 41(3):592–603
Herbig KL (2008) Changes in Espionage by Americans, 1947–2007 (PERSEREC Technical Report No. 08-05). Defense Personnel and Security Research Center (PERSEREC). Retrieved from https://www.scribd.com/doc/192035027/Katherine-L-Herbig-Changes-in-Espionage-by-Americans-1947-2007-Technical-Report-08-05-Northrop-Grumman-March-2008
Hubbard DW (2009) The failure of risk management. Wiley, Hoboken
INSa (2013) A preliminary examination of insider threat programs in the U.S. Private Sector. Intelligence and national security alliance. Retrieved from http://www.insaonline.org/id/a/b/InsiderThreat_embed.aspx
Kandias M, Mylonas A, Virvilis N, Theoharidou M, Gritzalis D (2010) An insider threat prediction model. In: Katsikas S, Lopez J, Soriano M (eds) Trust, privacy and security in digital business. Springer, Berlin Heidelberg, p 26–37 Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-15152-1_3
Lanham MJ (2015) Rapid mission assurance assessment via sociotechnical modeling and simulation. Dissertations. Paper 536
Lanham MJ, Morgan GP, Carley KM (2011) Data-driven diffusion modeling to examine deterrence. In: IEEE presented at the network science workshop (NSW), 2011, p 1–8
Leonard R (2010) Von Neumann, Morgenstern, and the creation of game theory. Cambridge University Press, New York
Liu L, Yu E, Mylopoulos J (2003) Security and privacy requirements analysis within a social setting. In: Proceedings of the 11th IEEE international presented at the requirements engineering conference, p 151–161
Martinez-Moyano JJ, Rich E, Conrad S, Andersen DF, Stewart TR (2008) A behavioral theory of insider-threat risks: a system dynamics approach. ACM Trans Model Comput Simul 18(2):7:1–7:27. doi:10.1145/1346325.1346328
Moore AP, Carley KM, Collins ML, Altman NW (2015) Social network dynamics of insider threats: a preliminary model. In: Proceedings of the international conference of the system dynamics society. System Dynamics Society, Boston
Moore AP, Novak WE, Collins ML, Trzeciak RF, Theis MC (2015b) Effective insider threat programs: understanding and avoiding potential pitfalls. Software Engineering Institute White Paper, Pittsburgh
Moreno J (1934) Who shall survive? A new approach to the problem of human interrelations. Nervous and Mental Disease Publishing Co., Beacon House
Myerson RB (1991) Game theory: analysis of conflict. Harvard University Press, Cambridge
Neapolitan RE (1990) Probabilistic reasoning in expert systems: theory and algorithms. Wiley, New York Office of the Press Secretary (2011) Executive Order 13587—Structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information. The White House. https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified
Pearl J (1985) Bayesian networks; a model of self-activated memory for evidential reasoning. In: Proceedings of the 7th Conference of the Cognitive Science Society, University of California, Irvine, p 329–334
Pearl J (1988) Probabilistic reasoning in intelligent systems. Morgan Kaufman, San Francisco
Sarbin TR, Carney RM, Eoyang C (1994) Citizen Espionage: studies in trust and betrayal. Praeger, Westport
Shaw ED, Fischer LF, Rose AE (2009) Insider risk evaluation and audit (No. Technical Report 09-02).
Defense Personnel Security Research Center, Monterey
Sterman J (2000) Business dynamics: systems thinking and modeling for a complex world. Irwin/
McGraw-Hill, New York
U.S. GAO (2015) Insider threats: DOD should strengthen management and guidance to protect classified
systems (No. GAO-15-544). United States Government Accountability Office

Andrew P. Moore is a Lead Researcher in the CERT Insider Threat Center and Senior Member of the
Technical Staff at Carnegie Mellon University’s Software Engineering Institute. Andy works with teams
across the SEI applying modeling and simulation techniques to cyber security, and system and software
engineering problems. Before joining the SEI in 2000, he worked for the Naval Research Laboratory
(NRL) investigating high-assurance system development methods for the Navy. He has over 25 years of
experience developing and applying mission-critical system analysis methods and tools, leading to the
transfer of critical technology to both industry and the government. Andy has co-published a book on
insider threat, two book chapters, and a wide variety of technical journal and conference papers. Andy
received a MA in Computer Science from Duke University, a BA in Mathematics from the College of
Wooster, and a Graduate Certificate in System Dynamics from Worcester Polytechnic Institute.

Kirk Kennedy, Ph.D is a Licensed Clinical Psychologist with over 25 years of operational experience in
applying psychological principles in various agencies within the federal government including the
military, Department of Defense, as well as NSA, CIA and FBI. Dr. Kennedy has expertise in the areas of
psychological assessment and selection programs; risk assessment and threat management; program
design and implementation of effective consultation, research, and training programs. Currently, Dr.
Kennedy is working with the FBI Behavioral Analysis Units to provide case consultation, training and
research. Also, he teaches the “Psychology of Intelligence Collection and Analysis” course offered as an
elective for intelligence analysts enrolled in the Intelligence Community Advanced Analyst Program
(ICAAP).

Thomas J. Dover is a Crime Analyst with the Behavioral Analysis Unit-5 in the FBI’s National Center
for the Analysis of Violent Crime, an instructor in crime analytic theory and applications for the National
Academy at Quantico, Virginia, and a Doctoral Candidate in Computational Social Science at George
Mason University in Fairfax, Virginia.