Insider Espionage: Recognizing Ritualistic Behavior by Abstracting Technical Indicators from Past Cases

Research-in-Progress

Michele Maasberg
The University of Texas at San Antonio
michele.maasberg@utsa.edu

Abstract

Espionage perpetrated by insiders using information technology (IT) assets continues to vex organizations. Despite significant investment in new approaches for detection, mitigation, and prevention, the attacks continue. We contend this is largely due to a low-level, signature based approach, despite the fact that insider cases vary across perpetrators, organizations, and over time with rapidly changing technology. This paper reviews existing literature and six insider espionage cases to identify technical indicators of espionage. We then propose an espionage ritual model, derived by abstracting technical indicators to a higher-level cycle of technical objectives. This abstraction then allows for a more generalizable model, from which more robust technical detection mechanisms can be derived. The model suggests that the ritual is different for other insider threats, including sabotage, fraud and IP theft and lays the groundwork for an empirical study. This model has significant implications for supporting current research, as well as practitioners in the field challenged with insider threat detection.

Keywords:

Insider threat, espionage, detection, ritual

Introduction

Despite recent convictions (e.g., Pfc Bradley Manning, U.S. Army, and Robert Hanssen, U.S. FBI) (Band, et al. 2006; Dishneau 2014), strong legislation, and increased research, insider espionage perpetrated by insiders remains a grave concern . National security and economic consequences from an insider threat can be significant, ranging from an enormous price tag, to the actual demise of organizations (Posey et al. 2011). While all attacks on an organization's information security are problematic and can have profound consequences, insider threats are often much more challenging to detect and difficult to mitigate than external attacks, because insiders are trusted individuals who know the organizations and networks well (Nance and Marty 2011; Spitzner 2003).

In order to detect insider espionage as early as possible, the psychological, organizational, and technical aspects of the problem must be understood, as well as how the actions are coordinated over time (Band, et al. 2006). Researchers have analyzed past espionage cases for descriptive statistics and profiling purposes. For example, Herbig and Wiskoff (2002) found that most American spies have historically been white males under the age of 30; nearly half (46%) have had a high school education or less; and one-quarter (25%) were government contractors. The problem with such profiling, however, is it casts a very wide net. If used as an indication and warning mechanism, the false positive rate is inordinate. Profile-based detection mechanisms are ineffective without being coupled with other detection approaches. For example, Edward Snowden fits Herbig and Wiskoff's (2002) profile perfectly, yet he was still able to exfiltrate classified data undetected until intentional public disclosure of the compromised material (Mosk et al. 2013).

To better understand and study insiders, the Carnegie Mellon University's Software Engineering Institute CERT Division began conducting insider threat research in 2001 and developed an Insider Threat Center among other centers (Carnegie Mellon University 2014). For this study, the Insider Threat Center will be referred to as "CERT" as it is sometimes abbreviated to in insider threat research (Hanley et al. 2011).

CERT developed a more granular taxonomy of insiders, differentiating insiders by motivation and method. Specifically, CERT separated insiders into four categories: espionage, intellectual property (IP) theft, fraud, and information technology (IT) sabotage (Band, et al. 2006; Hanley et al. 2011). Espionage refers to the willful compromise of classified or proprietary information to foreign entities (Kramer et al. 2005). IP theft refers to cases where malicious insiders purposely abuse their credentials to steal confidential or proprietary information from the organization (Moore et al. 2011). Fraud is defined by an insider's malicious use of an organizational information technology system that leads to an identity crime as a result of their misuse of data for personal gain or theft (Cummings et al. 2012). Last, IT sabotage refers to individuals who inflict damage on some area of an organization targeting IT assets (Band, et al. 2006). While the four categories are related and overlap to some extent, important distinctions exist concerning their motivations, methods, and targets, as shown in Table 1. Accordingly, each category of insider should be studied and analyzed both individually and collectively, leading to the development of security controls specific to each type of insider.

Insider Threat Category	Motivation	Method	Target
Espionage	Personal crisis, patriotic disposition, civil disobedience	Information exploration and browsing; acquisitions, preparation, transfer to an external entity	Classified, sensitive, and proprietary information
IP Theft	Business advantage, financial gain, new job with competitor, disgruntlement (sense of entitlement motivates insider)	Exfiltration of data via email, removable media, remote network access	Source code, business plans, customer information, trade secrets, internal organizational information, proprietary software
Fraud	Financial gain or financial difficulty	Typically not technically sophisticated; usually committed during work hours	Personally Identifiable Information
Sabotage	Personal grudge / revenge	More technically sophisticated means including use of remote access, logic bombs, back doors, other malware	Employer's system or network

Table 1. Insider Threat Taxonomy
Adapted from (Band, et al. 2006; Cummings et al. 2012; Herbig and Wiskoff 2002; Kramer and Heuer 2007; Moore et al. 2013; Roy Sarkar 2010)

Because of the vast differences in motivations, methods, and targets between CERT's four insider threat categories, technical indicators of insider activity vary. Regarding theft of IP, Moore et al. (2013) found that 70% of insiders stole IP data within 60 days of their departure, and 50% of them stole at least some of the information within 30 days of their departure. As a result, security information and event management (SIEM) system signatures commonly define a 30-60 day departure window aperture. In contrast, espionage cases tend to exhibit much longer-term data collection and exfiltration cycles. In fact, analyses of existing cases suggest it often occurs for years until the perpetrator is caught (Herbig and Wiskoff 2002). Other technical indicators to theft of IP included use of personal and work email as well as remote network access (Hanley et al. 2011), whereas espionage cases have more frequently used other mechanisms for transferring compromised data, including document printing and removable devices (Band, et al. 2006).

Researchers studying insider fraud cases have established a fraud cycle timeline, depicted in Figure 1. Common fraud indicators include: employees not taking vacations, employee disgruntlement over lack of promotions or raises, illegal transfer of funds found by auditing, and employees using corporate credit cards for personal use, also found by auditing and monitoring (Cummings et al. 2012). In contrast, espionage cases have frequently included unexplained absences, employees subject to minimal technical access controls and monitoring, and employees having complete access to entire data stores (Band, et al. 2006). Given the overarching degree of trust often awarded to employees with access to highly classified information, and the absence of auditing and monitoring, the category of espionage is quite different from fraud. In fraud cases, there is often a higher degree of technical skill required to exploit the system, and fraud is often detected sooner than espionage (Band, et al. 2006).

Figure 1. Timeline for fraud (Cummings et al. 2012)

Sabotage is hallmarked by the creation of back door accounts and singular release of a logic bomb (Band, et al. 2006). Contrasted with espionage, where multiple accesses to a system are necessary to gather information, most acts of sabotage only occur once (Band, et al. 2006). Overall, many of the technical indicators enumerated by insider research for IP theft, fraud, and sabotage do not appear in the research for espionage and vice versa (Band et al. 2006; Cummings et al. 2012; Hanley et al. 2011).

The literature has been particularly devoid of technical indicators of espionage activity. We contend this is because the ever-changing technological implementation has been the focus, instead of higher-level, abstracted *ritual* of espionage that stays more constant over time. When cases are examined from a higher-level process and behavioral event perspective, considering espionage objectives rather than technological implementation, an abstracted ritual of espionage emerges that can be instantiated in various technologies, organizations, and methodological approaches over time. Technical indicators can then be identified more easily and accurately for specific organizations, at specific points in time, with specific technology availability, than is otherwise possible without the ritualistic view of insider espionage. We propose the idea of an espionage ritual that is agile and adaptive to changing technology, and therefore differentiating it from a detection signature.

The purpose of this study (a research-in-progress) is to conduct a cursory analysis of a small subset of espionage cases to hypothesize an espionage ritual and lay the groundwork for a more extensive empirical study that validates or adapts the espionage ritual to better detect future espionage attacks. The remainder of the paper is organized as follows. First, we present important definitions and a discussion of literature relevant to the research question. Next, we discuss examples of currently known technical indicators of espionage and highlight gaps in the research. Then, we propose a theoretical espionage ritual with a model and two levels of abstraction. Finally, we conclude with future research and conclusions.

Background

In this section, we provide background discussion and define important concepts, including: espionage, the insider, the insider threat, procedural ritual, and technical indicators. Band et al. (2006) view espionage and sabotage in the same milieu, and thus characterize espionage as malicious activity in which

the insider's primary goal is to harm the organization or an individual. Espionage is more traditionally referred to as a compromise of organizational classified or proprietary information to foreign entities (Kramer et al. 2005). Section 793 of United States Code Title 18 defines espionage as a multi-step process, which includes procuring National Defense Information (which may or may not be classified), stealing it alone or via an accomplice with access, making contact with a recipient of the information, and transferring the information to the recipient (Herbig and Wiskoff 2002). For this study, the definition of espionage is a confluence of these definitions, expands motivation beyond aid to foreign entities and includes anti-government acts of civil disobedience, and is the compromise or attempt to compromise organizational classified or proprietary information to external entities (Herbig and Wiskoff 2002; Kramer et al. 2005).

Insiders are personnel, such as permanent or temporary employees, vendors, contractors, suppliers, ex-employees, who are most capable of exploiting organizational assets (Kramer et al. 2005). Insiders operate within defined boundaries and have been granted some degree of trust and privilege within those boundaries (Chivers et al. 2013). Not only do insiders have privilege, but they have access and intimate knowledge of organizational processes that give them the ability to exploit vulnerabilities (Willison and Warkentin 2013). An insider threat occurs when an insider uses legitimate access to act in a way inconsistent with organizational security policy (Bishop and Gates 2008). It is further defined by an "insider's action that puts at risk an organization's data, processes, or resources in a disruptive or unwelcome way" (Pfleeger et al. 2010, p. 170). Insider threats can even put business viability at risk (Pfleeger and Stolfo 2009).

Previous research has investigated the psychological and organizational aspects of insider espionage, noting that this type of attack is often subtle, slow, and preceded by behavioral indicators such as organizational rule-breaking, organizational conflict, and behavioral deviance (Chivers et al. 2013). Psychological and organizational behaviors observed before and during insider sabotage and espionage include serious mental health disorders, personality problems, poor social skills and decision-making biases, and a history of rule conflicts (Band, et al. 2006). More specifically discriminating psychological and organizational indicators included disgruntlement, tardiness, truancy, arguments with coworkers, poor job performance, security violations, attack preparations, and addictions. While important, these behaviors do not clearly distinguish espionage from sabotage or the other types of insider threat (Band, et al. 2006; Herbig and Wiskoff 2002; Moore et al. 2013; Shaw et al. 1999). A comprehensive behavioral-technical profile is necessary for each type. Accordingly, this paper focuses on the technical aspect of the insider engaging in espionage.

The Capability, Motive, and Opportunity (CMO) model postulates that a perpetrator must have the capability, motive, and opportunity for a successful insider attack (Schultz 2002). The capability for espionage includes the means to collect and transfer sensitive information to foreign entities (Kramer et al. 2005). The motive for espionage occurs as a result of a complex interaction between personality characteristics and situational dynamics (Kramer et al. 2005). It is most often money or disgruntlement, but over time money usually becomes the dominant motive (Herbig and Wiskoff 2002). The opportunity for espionage consists of access to classified or proprietary information that can be exchanged for money or other benefits, and access to foreign entities interested in obtaining this information (Kramer et al. 2005). The CMO model also interleaves various situational dynamics, each partially facilitating the successful commission of espionage activity. Such situational dynamics include insider personal predispositions to committing malicious acts, stressful events contributing to the likelihood of occurrence, concerning behaviors observed before the occurrence of espionage, technical actions occurring before the espionage, organizations ignoring or failing to detect rule violations, and/or lack of physical and electronic access controls in an organization (Band, et al. 2006).

The procedural ritual refers to a recognizable and repeatable pattern of activity, or "special routines" as referred to by Carnes (2001). In the context of the insider committing espionage, ritualistic activities are those observable, repeating process-level steps that precede and/or facilitate espionage activity. They are abstracted and independent of technological advancements and implementations. For example, whereas exfiltration of sensitive data in the 1970's involved copy machines and paper documents, exfiltration in the 21st century often involves copying digital data onto removable media.

Last, technical indicators are the non-abstracted, technological implementations of the espionage ritual. For example, copying large amounts of data incident to use of removable thumb drives is a technical

indicator, whereas 'data exfiltration' is the abstracted, process-level, ritualistic artifact. This paper explores the idea that when abstracted to the process level, insider technical actions actually follow a pattern or sequence that can be determined by analyzing previous cases of insider espionage, which is supported by other modeling and simulation studies (Chivers et al. 2013).

Technical Indicator Analysis

In this section, we review relevant literature and six documented espionage cases perpetrated by trusted insiders. We illuminate technical indicators with the end goal of postulating an espionage ritual, useful for future empirical analysis.

CERT has been actively conducting case-level analyses of documented insider threat cases in all four categories. One such study published by Band et al. (2006) comparatively evaluates insider sabotage cases and insider espionage cases, in part to illuminate technical indicators of insider activity. As Figure 2 shows, their case review shows that observable technical indicators precede harmful actions on the part of the insider. Figure 2 shows what occurs when organizations fail to recognize and act upon the technical indicators preceding espionage, with the harmful actions representing the act of insider espionage in progress. The arrows and "S" and "O" notations in the model represent direction of influence (i.e., "S" represents variables move in same direction, "O" indicates a movement in opposite direction) (Band, et al. 2006). The trust trap (with CERT feedback loop reference label R2, R representative of a "reinforcing" vice "balancing" loop in their modeling system) is a reinforcing loop depicting the trust displayed by an organization to an individual over time, which research has shown to increase over time (Band, et al. 2006). Due to the increase of trust over time, organizations tend to discover fewer technical indicators and harmful actions (Band, et al. 2006).

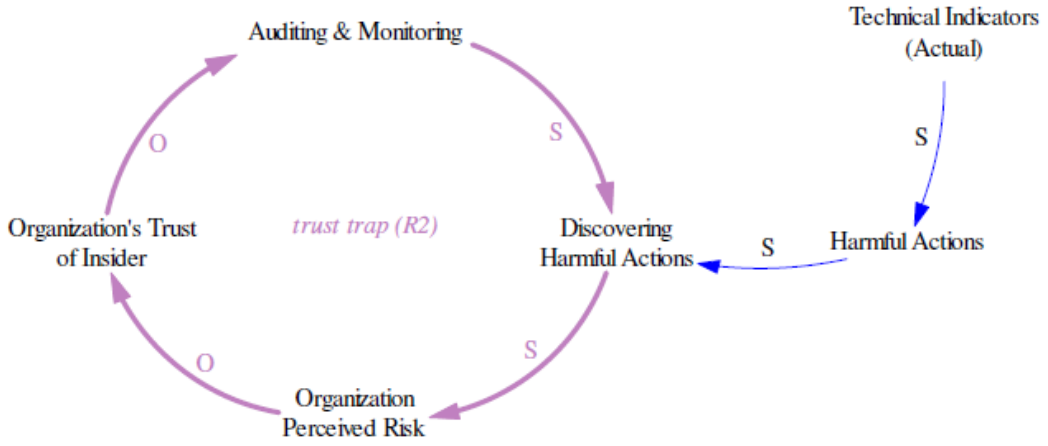

Figure 2. Insider Technological Observables Model (Band, et al. 2006).

Band et al. (2006) used system dynamics modeling to analyze nine espionage cases from the Defense Personnel Security Research Center's "Espionage Database"—a database storing information about 150 espionage cases dating back to 1940. Their review of the nine cases illuminated the fifteen (15) "technical observables" shown in Table 2.

Known Insider Espionage Technical Actions and Indicators
Access of information outside of need to know
Concealment strategies
Download and installation of malicious code and tools
Hacking
Unauthorized encryption of information
Unauthorized information transfer
Violation of acceptable use policy
Printing documents
Copying information to disks
Relabeling of disks
Violation of physical security policies and procedures
Download and use of password cracker
Unauthorized encryption of information
Compromise of supervisor's computer
Unauthorized "web surfing"

Table 2. Insider Espionage Technical Observables, Adapted from (Band, et al. 2006).

Our review of six espionage cases perpetrated by insiders disclosed several significant commonalities and differences between the cases. As expected, the commonalities emerge when the technical actions are abstracted to a higher, process level, related to technical objectives, rather than low-level technological implementations. Similarly, the differences are evidence when the cases are analyzed at the technical implementation level, wherein actions are affected by various organizational conditions and technological advancements impacted greatly by date of occurrence. Table 3 summarizes the technical actions and chronological context of the six cases reviewed.

Common to all six cases is the technological objective: *accessing information outside of need to know* (Band, et al. 2006). Master Sergeant (MSgt) Brian Patrick Reagan, a former U.S. Air Force intelligence analyst, accessed missile site information from a classified database that was authorized but outside of his need to know (Band, et al. 2006). Both Robert Hanssen, a former FBI agent, and Leandro Aragoncillo, a former military security official for the U.S. Vice President, accessed information outside of their need to know on the FBI's Automated Case Support database (Band, et al. 2006). Another commonality at the process-level is the technological objective: *unauthorized information transfer*. However, when analyzed at the technological implementation level, differences emerge. MSgt Reagan transferred the data in printed form, whereas Special Agent Hanssen used floppy-diskettes and Mr. Aragoncillo transmitted the data via email. In other words, the transport mechanism varied, but the objective (unauthorized transport) remained constant.

Espionage Agent	Date Espionage Began	Technical Action #1	Technical Action #2	Technical Action #3	Technical Action #4	Date of Discovery
Aldrich Ames (CIA)	1985	Accessed outside need to know	Unauthorized "web surfing" (searched large digitized datasets)	Printing information	Unauthorized information transfer	2/21/94
Brian Reagan (USAF)	1999	Accessed outside need to know	Unauthorized web surfing (illegal search if Intelink database)	Illegal download (illegal downloading classified information)	Unauthorized information transfer and printing (buried over 20,000 pages of classified documents, 5 CDs and 5 videotapes in rural Virginia and Maryland)	8/3/2001
Harold Nicholson (CIA)	1994	Accessed outside need to know	Unauthorized web surfing (surfing large organizational databases)	Printing information	Unauthorized information transfer	11/16/1996
Robert Hanssen (FBI)	1979	Accessed outside need to know	Unauthorized "web surfing"	Illegal download onto coded disk	Unauthorized encryption of information and unauthorized transfer (removal of data on encrypted disks)	2/18/01
Leandro Aragoncillo	2004	Accessed outside need to know	Unauthorized "web surfing" (searched FBI's Automated Case Support (ACS) database)	Illegal download and printing documents	Unauthorized information transfer (transmitted info to high level Philippine official via email)	10/5/2005
Edward Snowden (NSA)	2013	Access information outside need to know	Unauthorized "web surfing" using web crawler software	Copying information	Unauthorized information transfer	Left for Hong Kong May 20 2013; dropped documents to reporters;

Table 3. Technical Actions of Six Insider Espionage Cases, Adapted from (Band, et al. 2006; Gallu 2014; Herbig and Wiskoff 2002; Kramer et al. 2005)

Proposed Espionage Ritual

Based on the technical actions identified in the previous section and summarized in Tables 2 and 3, we propose the basic espionage ritual shown in Figure 3. Table 4 shows how the behavioral ritual can be used as a framework from which to derive technical indicators.

Figure 3. Proposed Espionage Ritual

RITUALISTIC BEHAVIOR (Technological Objective)	**Info exploration and browsing**	**Data acquisition**	**Data preparation**	**Unauthorized info transfer**
Technical Indicator (Technological Implementation)	• Hacking • Web browsing • Web crawling • Network share browsing • Database querying	• Download and installation of malware and tools • Copying data • Web scraping • Document printing	• Encryption • Compression • Stegonographic embedding • Cutting/pasting • Data organization • Archiving • Moving to alternate media • Relabeling files, data, disks	• Hand-carrying printed data off-site • Hand-carrying digital data off-site on digital media (e.g. laptops, thumb drives, CD/DVDs, hard drives) • Mailing printed data • Emailing digital data • Uploading to website, email 'drafts' folder, or other remote storage location

Table 4. Technical Indicators of Ritualistic Behavior

This espionage behavioral ritual allows for variation and iteration. In some cases, information exploration may not occur and the insider may simply acquire, prepare, and transfer the data. They may not seek out additional information in an exploratory manner, although most cases reviewed seemed to include this step. The steps may occur over varied time periods and may or may not repeat. The technological implementations may vary over time in insider threat cases where data exfiltration occurs over the course of many years, such as former FBI Agent Robert Hanssen, who was charged with spying for Russia for more than 15 years (Band, et al. 2006). In order for time periods can be calculated during an empirical study, T1-T4 are included on the model in figure 3. Further, Mr. Hanssen initially acquired only data he had technical access to, but later used a password cracker to gain unauthorized access to his supervisor's data. The frequency and timing of activity may vary widely from case to case, which is again why specific technical *signatures* are problematic and the more abstracted view of technical behavior at the ritualistic, technical objective level may be more successful.

Future Research and Concluding Comments

While the proposed espionage ritual was derived from past literature and the analysis of a small number of espionage cases, further empirical research is needed. More cases need to be analyzed to: (1) test the robustness of the proposed ritual, (2) refine the list of technical indicators for each step in the espionage ritual cycle, and (3) test the utility of the cycle in deriving technical indicators. We propose that past cases can be analyzed to identify technical actions and indicators from previous attacks of espionage and map those to the higher-level, abstracted espionage ritual. We further propose that a post-hoc, multi-case study analysis using formal modeling methodology could determine the retrospective detection probability had the espionage ritual been considered when developing and deploying insider espionage detection mechanisms. Last, we propose that the robust, refined espionage ritual can be used to predict future attacks.

Clearly, a limitation of this study is its restricted case study analysis. Empirical testing will be challenging due to: (1) accessibility of case data and (2) the volume of data for documented cases, should access be granted for the purpose of mining technical indicators. Further, the data collection procedure will require laborious content analysis techniques.

This paper presents the idea of a higher abstraction of technical espionage indicators in the form of an espionage ritual cycle. We propose that this ritual can be determined by examining previous insider espionage attacks coupled with current research on technical indicator trends for espionage. Accordingly, past literature and high-level analysis of six insider threat cases support the proposed espionage ritual cycle.

Acknowledgements

Michele Maasberg was a Kudla Fellow at the University of Texas at San Antonio while working on this paper. She thanks the Fellowship program for its support during the 2013-2014 academic year.

References

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., and Trzeciak, R. F. 2006. "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," No. CMU/SEI-2006-TR-026, Carnegie-Mellon University Software Engineering Institute Pittsburgh, PA, available online at http://www.dtic.mil/docs/citations/ADA459911

Bishop, M., and Gates, C. 2008. "Defining the insider threat," Presented at the Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, 1413158, pp. 1–3.

Carnegie Mellon University. 2014. "About Insider Threat Research: A History of Our Work," available online at https://www.cert.org/insider-threat/about.cfm

Carnes, P. 2001. *Out of the Shadows*, Center City, MN: Hazelden.

Chivers, H., Clark, J. A., Nobles, P., Shaikh, S. A., and Chen, H. 2013. "Knowing who to watch: Identifying attackers whose actions are hidden within false alarms and background noise," *Information Systems Frontiers* , pp. 1–18.

Cummings, A., Lewellen, T., McIntire, D., Moore, A., and Trzeciak, R. 2012. "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector," No. CMU/SEI-2012-SR-004, available online at http://repository.cmu.edu/sei/688

Dishneau, D. 2014, April 14. "Manning's Conviction, 35-Year Sentence Upheld," *ABC News*, available online at http://abcnews.go.com/US/wireStory/mannings-conviction-35-year-sentence-upheld-23321138

Gallu, J. 2014, February 9. "Snowden Used 'Web Crawler' to Scrape NSA: New York Times," *Bloomberg*, .

Hanley, M., Dean, T., Schroeder, W., Houy, M., Trzeciak, R. F., and Montelibano, J. 2011. "An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases," No. CMU/SEI-2011-TN-006, Carnegie-Mellon University Software Engineering Institute Pittsburgh, PA, available online at http://www.dtic.mil/get-tr-doc/pdf?AD=ADA549391

Herbig, K. L., and Wiskoff, M. F. 2002. "Espionage Against the United States by American Citizens 1947-2001," No. PERSEREC-TR-02-5, Defense Personnel Security Research Center Monterey, CA, available online at http://www.dtic.mil/get-tr-doc/pdf?AD=ADA411004

Kramer, L. A., and Heuer, R. J. 2007. "America's Increased Vulnerability to Insider Espionage," *International Journal of Intelligence and CounterIntelligence* (20:1), pp. 50–64.

Kramer, L. A., Jr, H., J, R., and Crawford, K. S. 2005. "Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage," No. PERS-TR-05-10, Defense Personnel Security Research Center Monterey, CA, available online at http://www.dtic.mil/get-tr-doc/pdf?AD=ADA433793

Moore, A., McIntire, D., Mundie, D., and Zubrow, D. 2013. "Justification of a Pattern for Detecting Intellectual Property Theft by Departing Insiders," *Software Engineering Institute*, available online at http://repository.cmu.edu/sei/732

Moore, A. P., Capelli, D. M., Caron, T. C., Shaw, E., Spooner, D., and Trzeciak, R. F. 2011. "A Preliminary Model of Insider Theft of Intellectual Property," Carnegie-Mellon University Software Engineering Institute Pittsburgh, PA, available online at http://www.dtic.mil/get-tr-doc/pdf?AD=ADA540507

Mosk, M., Meek, J. G., and Walshe, S. 2013, June 14. "Timeline: Edward Snowden's Life As We Know It," *ABC News,* available online at http://abcnews.go.com/Blotter/timeline-edward-snowdens-life/story?id=19394487

Nance, K., and Marty, R. 2011. "Identifying and visualizing the malicious insider threat using bipartite graphs," Presented at the 2011 44th Hawaii International Conference on System Sciences (HICSS), pp. 1–9.

Pfleeger, S. L., Predd, J. B., Hunker, J., and Bulford, C. 2010. "Insiders behaving badly: addressing bad actors and their actions," *Information Forensics and Security, IEEE Transactions on* (5), pp. 169–179.

Pfleeger, S. L., and Stolfo, S. J. 2009. "Addressing the Insider Threat," *Security & Privacy, IEEE* (7), pp. 10–13.

Posey, C., Bennett, R. J., and Roberts, T. L. 2011. "Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes," *Computers & Security* (30:6–7), pp. 486–497.

Roy Sarkar, K. 2010. "Assessing insider threats to information security using technical, behavioural and organisational measures," *Information Security Technical Report* Computer Crime - A 2011 Update, (15:3), pp. 112–133.

Schultz, E. E. 2002. "A framework for understanding and predicting insider attacks," *Computers & Security* (21:6), pp. 526–531.

Shaw, E. D., Post, J. M., and Ruby, K. G. 1999. "Inside the mind of the insider," *Security Management* (43), pp. 34–44.

Spitzner, L. 2003. "Honeypots: Catching the insider threat," Presented at the Computer Security Applications Conference, 2003. Proceedings. 19th Annual, pp. 170–179.

Willison, R., and Warkentin, M. 2013. "Beyond deterrence: An expanded view of employee computer abuse," *MIS Quarterly* (37:1), pp. 1–20.